



Governance

Corporate Governance

Basic Approach to Corporate Governance

Through a decision by the Board of Directors in December 2015, Fujitsu formulated a basic policy that sets out its approach to corporate governance (the "Corporate Governance Policy").

We updated the policy in September 2023 and, adopting the stance that the aim of corporate governance is to ensure better management, we constantly review the policy to ensure that it does not become rigid or lose its relevance. We also discuss it with the Board of Directors as appropriate, and strive to maintain the best corporate governance system at all times.

- [Corporate Governance Policy](#) 

Corporate Governance Structure (as of June 24, 2024)

In accordance with its Corporate Governance Policy, the company outlines the following rules to ensure effective oversight and advice, given from the diverse perspectives of Non-Executive Directors (hereinafter, the term used for a combination of Independent Directors and Non- Executive Directors appointed from within the company), to Executive Directors on their business execution as part of the Board of Directors function while taking advantage of the company through the Audit & Supervisory Board system.

<Board of Directors>

The Company has a Board of Directors to serve as a body for making important decisions and overseeing management. The Board of Directors delegates the decision-making authority over business execution to the Representative Directors and subordinate Corporate Executive Officers to the broadest extent that is permitted by law and the Articles of Incorporation of the company and is considered to be reasonable and will mainly perform as oversight and advisory function. Moreover, the Board of Directors has been formed with Non-Executive Directors at its core so as to enable correction and remediation of errors, insufficiencies, and recklessness in business execution. And by ensuring that External Directors, who are highly independent and hold diverse perspectives, constitute the majority of the members of the Board of Directors, the oversight and advisory function of the Board of Directors is strengthened. Furthermore, in order to better define the management responsibility of the Directors, their terms were reduced from two years to one year in accordance with a resolution at the June 23, 2006 Annual Shareholders' Meeting. As of June 24, 2024, the Board of Directors consists of nine members in total, comprising three Executive Directors and six Non-Executive Directors (including five External Directors).

In FY2023, the Company held 18 Board of Directors meetings (including six extraordinary meetings) to

flexibly resolve and report on the matters that come under the Board's province pursuant to the Companies Act and the Regulations of the Board of Directors of the Company. The Board identified the following six themes as the themes that it should focus on based on the business environment surrounding Fujitsu Group: 1) new medium term management plan; 2) business portfolio transformation; 3) profitability improvement in international business; 4) quality and security issues; 5) succession planning of Directors and others; and 6) efficient monitoring methods of these themes. The Board had intensive discussions on these themes and continued monitoring them.

Furthermore, as its agenda items, the Board discussed and heard reports on shareholder returns, examinations of strategic shareholdings, the organization and operation status of internal control systems, and feedback on dialogues with shareholders and investors. For the evaluation of the effectiveness of the overall Board, the Board's Secretariat introduced individual interviews based on questionnaire responses from FY2023 and analyzed and evaluated the interviews. This allowed the Board to discuss accurate improvement measures based on the correct understanding of responses and led to efforts to improve information sharing with outside officers and to further raise the effectiveness of the Board. The Risk Management & Compliance Committee that oversees risk management of the entire Group began holding a monthly meeting from FY2023 to ensure the speediness and effectiveness of each measure. The Board of Directors received a report on the implementation status of the Committee's tasks at every Board meeting and discussed and monitored actions taken, including preventative actions of individual quality and security issues.

<Audit & Supervisory Board>

The Company has an Audit & Supervisory Board that performs the auditing and oversight functions. The auditing and oversight functions are carried out by Audit & Supervisory Board Members, who review the Board of Directors as well as business execution functions and attend important meetings, including meetings of the Board of Directors. As of June 24, 2024, the Audit & Supervisory Board has five members, comprising two full-time Audit & Supervisory Board Members and three External Audit & Supervisory Board Members.

In FY2023, the Company held 11 Audit & Supervisory Board meetings (including two extraordinary meetings), mainly to develop and resolve its audit policy and audit plans, confirm the audit plan and method of Accounting Auditors, and examine the appropriateness of their audit results and key audit matters. In addition, the Audit & Supervisory Board heard reports from the internal audit section and heard and discussed the reports on important items made by full time Audit & Supervisory Board Members to External Audit & Supervisory Board Members. Except for one meeting where one member was absent, all Audit & Supervisory Board Members attended all Audit & Supervisory Board meetings.

In FY2023, Audit & Supervisory Board Members conducted the following activities with a focus on the building and operation of internal control systems and responses to management challenges in accordance with the approved audit policy and plans:

- Attending and expressing opinions at the Board of Directors meetings, meetings of Independent Officers, and other important meetings
- Reading important approval documents
- Exchanging opinions with Representative Directors
- Interviewing each business line at the Head Office and subsidiaries on their operations
- Hearing reports from statutory auditors of subsidiaries
- Hearing reports from Accounting Auditors
- Hearing the audit status and results from the internal audit section
- Hearing the status of whistleblowing from the compliance section
- Hearing the status of risk management and quality control

The discussion topics were potential risks of material misstatements in the consolidated financial statements and impacts of, and developments in, material events, etc. that occurred in FY2023

<Independent Directors & Auditors Council>

In response to the requirements of Japan's Corporate Governance Code, which facilitates the activities of Independent Directors and Auditors, and in order to invigorate discussions on the medium- to long-term direction of the Company at its Board of Directors Meetings, the Company believes it essential to establish a system that enables Independent Directors and Auditors, who maintain a certain degree of separation from the execution of business activities, to consistently gain a deeper understanding of the Company's business. Based on this recognition, the Company established the Independent Directors and Auditors Council, which consists of all Independent Directors and Auditors (five Independent Directors and three Independent Auditors), and discusses the medium- to long-term direction of the Company, shares information, and exchanges viewpoints so that each can formulate their own opinions.

In FY2023, the Company held 8 Independent Directors and Auditors Council meetings. The members continuously discussed the Company's management direction and on important management matters that were associated with business restructuring including mergers and acquisitions by the Company and the Fujitsu Group, and shared information and exchanged viewpoints.

<Executive Nomination Committee & Compensation Committee>

The Company has established the Executive Nomination Committee and the Compensation Committee as advisory bodies for its Board of Directors for the process of nominating Directors and Audit & Supervisory Board Members, for ensuring the transparency and objectivity of its process for determining executive compensation, to enable efficient and substantial discussions, as well as to ensure the fairness in the structure and level of executive compensation.

The Executive Nomination Committee deliberates on the candidates for Director and Audit & Supervisory Board Member positions in accordance with the Framework of Corporate Governance Structure and the Procedures and Policy for the nomination and dismissal of Directors and Auditors stipulated in the Policy, and it provides its recommendations or proposal to the Board of Directors.

In addition, the Compensation Committee provides its recommendations or proposal on the level of base compensation and the method for calculating performancebased compensation to the Board of Directors in accordance with the Procedures and Policy of Determining Directors and Auditors Compensation, as stipulated in the Policy.

The Executive Nomination Committee consists of three Non-Executive Directors (including two Independent Directors) and the Compensation Committee consists of three Independent Directors. The members appointed to the two committees in June, 2024 are as follows. Additionally, the secretariats of both committees are operated by the Company's HR and legal departments.

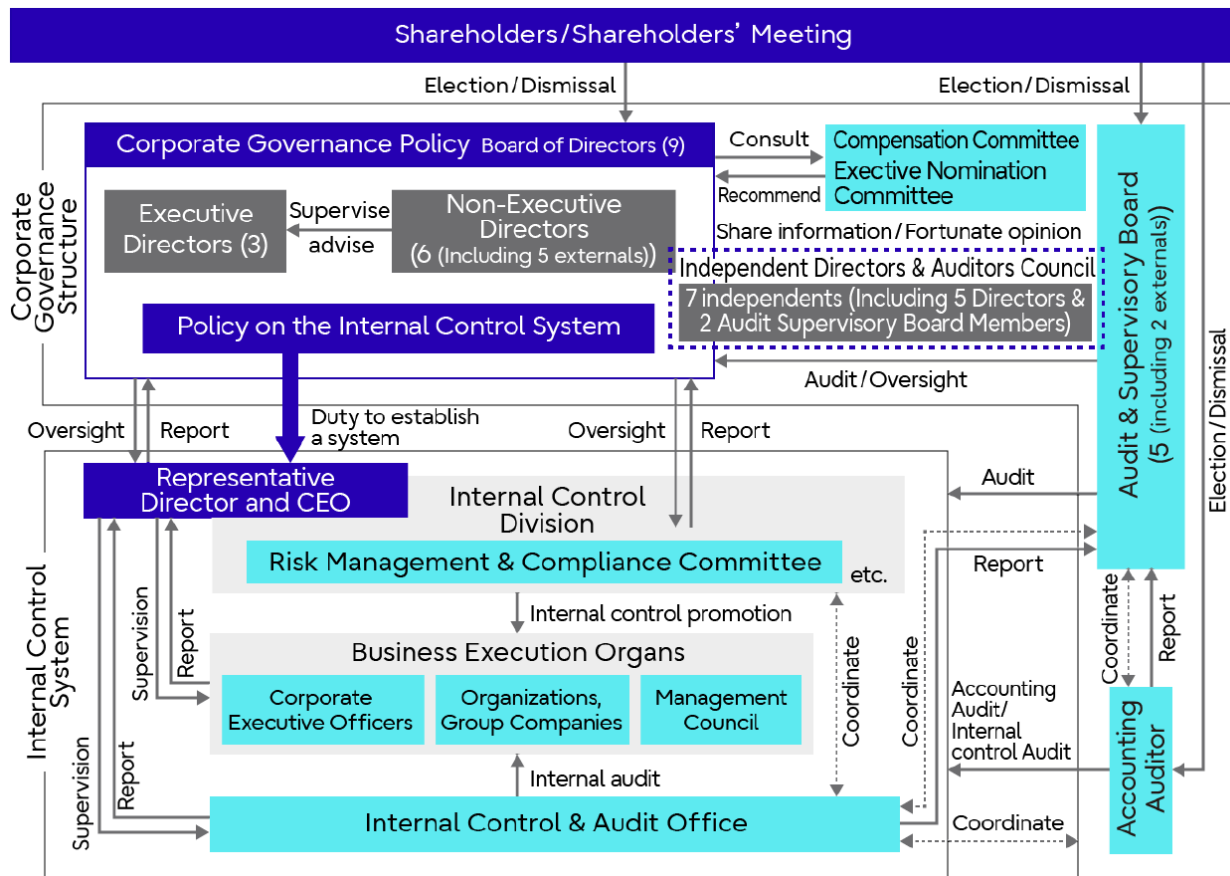
- Executive Nomination Committee
Chairperson: Chiaki Mukai (Independent Director)
Members: Yoshiko Kojo (Independent Director), Hidenori Furuta (Non-Executive Chairman, Board of Directors)
- Compensation Committee
Chairperson: Byron Gill (Independent Director)
Members: Kenichiro Sasae (Independent Director), Takuya Hirano (Independent Director)

In FY2023, the Executive Nomination Committee met nine times and the Compensation Committee met seven times. The Executive Nomination Committee considered a proposal for the election of Representative Directors, including the CEO, and proposals for the election of candidates for Directors, Audit & Supervisory Board Members, and the Chairman of the Board of Directors, etc. The Compensation Committee discussed the revision to the level of compensation of Directors, revision to the performance related compensation for the Executive Directors and the introduction of share based compensation for the Non-Executive Directors.

And each Committee provided its findings to the Board of Directors by the end of the period under review.

The Executive Nomination Committee also considered the succession plan for the CEO, etc. and the selection of candidates for External Directors and Audit & Supervisory Board Members, and conducted a peer review of Non-Executive Directors, while the Compensation Committee discussed the amount of compensation paid to each Executive Director for the period under review.

The diagram below illustrates the Company's corporate governance structure.(As of June 24, 2024).



Corporate Governance Structure

*Number inside parenthesis refers to number of Directors and /or Audit & Supervisory Board Members

Reasons for Adoption of Current Corporate Governance System


We believe that both direct oversight to business execution by the Non-Executive Directors and the oversight by Audit & Supervisory Board Members that stays distant from the decision making and operation of business execution should work jointly to ensure highly effective oversight performance. The company adopts “the company with Audit & Supervisory Board system” that establishes the Audit & Supervisory Board, which is composed of the Audit & Supervisory Board Members appointed as an independent agent.

Moreover, the Board of Directors has been formed with Non-Executive Directors at its core so as to enable correction and remediation of errors, insufficiencies, and recklessness in business execution. And External Directors constitute the majority of the members of the Board of Directors. The core of Non-Executive Directors shall be External Directors with a high degree of independence and diverse perspectives. Moreover, at least one Non-Executive Director is appointed from within the Company to

complement the External Directors' knowledge in the business fields and the culture of the Company, so that the efficiency of oversight and advice performance by the Non-Executive Directors is enhanced.

Policy for Determining Executive Compensation


The compensation of Directors and Auditors is determined based on the "Basic Policy on Executive Compensation," which sets out the details of individual compensation for Directors, and was decided by the Board of Directors in response to a recommendation from the Compensation Committee.

- [Corporate Governance Report](#)
[\[Incentive Policies for Directors \(page 21\); Policy on Determining Remuneration Amounts and Calculation Methods \(Page 23, 24\)\]](#) 

Basic Approach to the Internal Control System

To continuously increase the corporate value of the Fujitsu Group, it is necessary to pursue management efficiency and control risks arising from business activities. Recognizing this, the Board of Directors have formulated the "Policy on the Internal Control System", which provides guidelines on: a) how to practice and promote the Fujitsu Way, the principles that underlie the Fujitsu Group's conduct; and b) what systems and rules are used to pursue management efficiency and control the risks arising from the Company's business activities.

See below for the full text of the Policy on the Internal Control System and an overview of the operating status of the systems tasked with ensuring appropriate business practices.

- [Matters Subject to Measures for Electronic Provision \(Matters Excluded from Paper-based Documents Delivered Upon Request\) at the Time of Notice of the 124rd Annual Shareholders' Meeting](#) 

Disclosures Relating to Corporate Governance

Board of Directors (as of June 24, 2024)

| | Name | Position and Responsibilities | Representation Authority | Independent Officer |
|-------------------|------------------|---|--------------------------|---------------------|
| Business executed | Takahito Tokita | CEO, Chairman of the Risk Management & Compliance Committee | ○ | |
| | Takeshi Isobe | Representative Director, Corporate Vice President, CFO* | ○ | |
| | Hiroki Hiramatsu | Corporate Executive Officer, SEVP, CHRO | | |
| Nonexecutive | Hidenori Furuta | Non-Executive Chairman, Member of the Board | | |
| | Chiaki Mukai | | | ○ |
| | Yoshiko Kojo | Chairman of the Board of Directors | | ○ |
| | Kenichiro Sasae | | | ○ |
| | Byron Gill | | | ○ |
| | Takuya Hirano | | | ○ |

FY2023 Attendance at Meetings of the Board of Directors or Audit & Supervisory Board

| Meeting | Number of Meetings | Attendance Rate |
|---------------------------|--------------------|-----------------|
| Board of Directors | 18 | 97.5% |
| Audit & Supervisory Board | 11 | 98.2% |

Skills of directors and auditors

As a global company that brings trust to society through innovation and makes the world more sustainable, our company identifies the diversity and skills required for directors and corporate auditors to effectively exercise their advisory and supervisory functions and discloses them in a Skills Matrix.

Directors (as of June 24, 2024)

| | Name | Independent | Diversity | | Skills Matrix | | | | |
|---|------------------|-------------|-----------|-------------|----------------------|------------------------|--------|------------|---------------------------|
| | | | Gender | Nationality | Corporate management | Finance and investment | Global | Technology | ESG, academia, and policy |
| Representative Director, CEO | Takahito Tokita | | Male | JP | ○ | | ○ | ○ | |
| Representative Director, CFO | Takeshi Isobe | | Male | JP | ○ | ○ | ○ | | |
| Director and Corporate Executive Officer | Hiroki Hiramatsu | | Male | JP | ○ | | ○ | | ○ |
| Non-Executive Chairman, Member of the Board | Hidenori Furuta | | Male | JP | ○ | | ○ | ○ | |
| Director | Chiaki Mukai | ○ | Female | JP | | | ○ | ○ | ○ |
| Director | Yoshiko Kojo | ○ | Female | JP | | | ○ | | ○ |
| Director | Kenichiro Sasae | ○ | Male | JP | | | ○ | | ○ |
| Director | Byron Gill | ○ | Male | US | | ○ | ○ | | |
| Director | Takuya Hirano | ○ | Male | JP | ○ | | ○ | ○ | |

Auditors (As of June 24, 2024)

| | Name | Independent | Diversity | | Skills Matrix | | |
|--|---------------------|-------------|-----------|-------------|-----------------------------|------------------------|-------------------|
| | | | Gender | Nationality | Legalaffairs and compliance | Finance and accounting | Operating process |
| Full-time Audit & Supervisory Board Member | Youichi Hirose | | Male | JP | | ○ | ○ |
| Full-time Audit & Supervisory Board Member | Yuuichi Koseki | | Male | JP | | ○ | ○ |
| Audit & Supervisory Board Member | Koji Hatsukawa | ○ | Male | JP | | ○ | ○ |
| Audit & Supervisory Board Member | Hideo Makuta | ○ | Male | JP | ○ | ○ | |
| Audit & Supervisory Board Member | Catherine O'Connell | ○ | Female | NZ | ○ | | |

Risk Management

Guidelines & Structure

The Fujitsu Group aims to achieve business continuity, enhanced corporate value, and the sustainable development of corporate activities. Uncertainties that might affect the achievement of these objectives are considered to be risks. To address these risks, the Fujitsu Group established a Risk Management & Compliance Committee based on the Policy on the Internal Control System determined by the Board of Directors.

The Committee reports directly to the Board of Directors and oversees risk management and compliance for the entire Fujitsu Group.

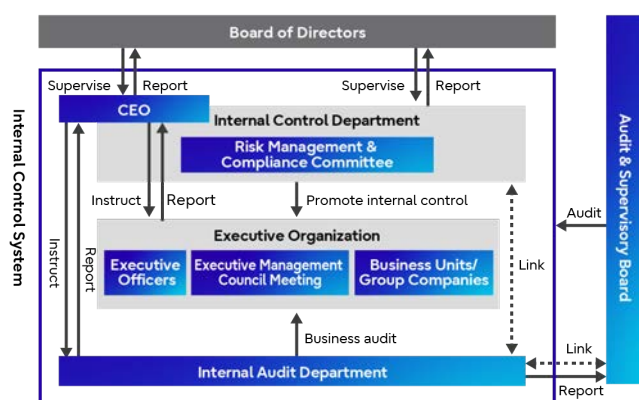
The Risk Management & Compliance Committee is chaired by the CEO and is composed of Board Members. Its primary function is to continually assess and verify risks that could potentially lead to losses for the Fujitsu Group. The Committee proactively implements measures to control risks identified during the course of business operations (potential risk management). Additionally, the Committee regularly analyzes realized risks to minimize losses, reporting them to the Board of Directors and working to prevent their recurrence (materialized risk management).

The Risk Management & Compliance Committee has established Regional Risk Management & Compliance Committees in each region that forms part of the global, region-based business execution structure. These regional committees operate as subcommittees. The Risk Management & Compliance Committee has deployed Risk Management & Compliance Officers to Business units (First line), as well as to Group companies and regions, both in Japan and overseas. Together, these entities collaborate to build a structure that promotes risk management and compliance throughout the Group.

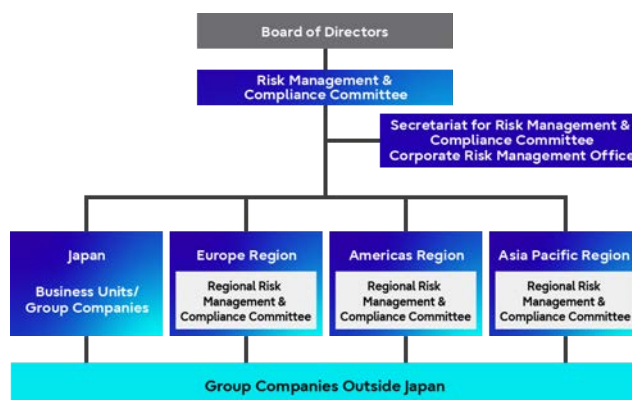
To further strengthen the Group's risk management capabilities, the company has established the Corporate Risk Management Office (Second line), a department which reports directly to the CEO and is independent of the business divisions. The Committee's secretariat function is provided by the Corporate Risk Management Office and is supervised by the Chief Risk Management Officer (CRMO).

The Secretariat monitors overall risk information, providing rapid and appropriate responses. In June 2023, the company appointed a Chief Quality Officer (CQO) to ensure prompt implementation of corporate policies and support for information security and system quality, as well as thorough risk management under the CEO's direction. The CQO convenes a monthly meeting of the Risk Management & Compliance Committee to ensure the swift and effective implementation of corporate policies.

To check that the risk management and compliance system is functioning properly, the company conducts annual audits by corporate auditors, internal audits by audit departments (Third line), and external audits by an auditing firm.



Positioning of the Risk Management & Compliance Committee in the Internal Control System



Risk Management & Compliance Structure

Processes

Potential Risk Management Process

- Identification and review of important risks of the Fujitsu Group
The Risk Management & Compliance Committee Secretariat (Corporate Risk Management Office, Second line) identifies and reviews the 16 important risks considered important to the Group, taking into account environmental changes affecting the Group. Risk scenarios are defined for each important risk, and they are classified into pure risk and management risk.
- Appointment of risk management departments (Second line)
A risk management department is assigned to each important risk, and is responsible for maintaining control over that specific risk.
- Evaluation of risks to the Fujitsu Group
Risk management departments, Business units, and Group companies evaluate the impact of each important risk, the likelihood of its occurrence, and the status of mitigation measures.
We select the risks that must be actively taken to achieve the Group's business strategies and goals, and those that must be actively avoided.
- Ranking and mapping of important risks
Based on the evaluation results of the Group, we rank important risks and create risk maps to visualize their importance. High priority risks are determined based on their importance.
- Risk Management & Compliance Committee Report
Analyses are conducted based on the evaluation findings, and mitigation policies are discussed and determined to address important risks to the Group.
- Issuing of corrective instructions to Business units and Group companies
Based on the evaluation results, feedback is provided to Business units and Group companies, advising them on improvements.
- Risk monitoring within Business units divisions and Group companies
Regular risk monitoring is implemented within Business units and Group companies to assess the status of mitigation measures and reduce risk exposure.

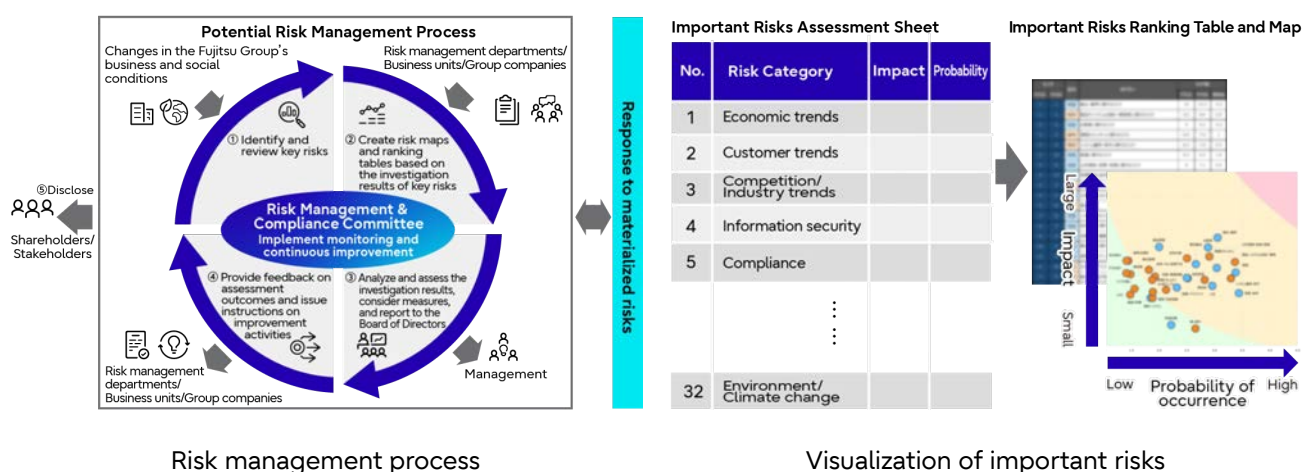
Addressing Materialized Risks

- Risk management regulations mandate rules (such as prompt escalation to the Risk Management & Compliance Committee) and require employees to be informed accordingly.
- Establish escalation rules for Business units and Group companies, and deploy promptly, based on risk management standards and rules for escalating risks to the Risk Management & Compliance Committee.
- Analyze risks and deploy mitigation measures, and report to the Board of Directors as necessary, to prevent recurrence. By cycling through this risk management process and having the risk management departments check it every six months, we aim to reduce risks across the Fujitsu Group and to minimize the impact when risks emerge.

High Priority Risks

Considering the findings from evaluations conducted in the Potential Risk Management Process and the status of materialized risks, we have chosen to focus on high priority risks based on their impact on achieving the Group's business strategies and goals. Consequently, we have identified the following two important risks as high priority for FY2023 and FY2024:

- Security risks
- Deficiencies or flaws in products and services



Important risks of the Group *1

| No. | Classification | Risk Category |
|-----|-----------------|--|
| 1 | Pure risk | <u>Security risks</u> |
| 2 | Pure risk | <u>Risks of natural disasters and unforeseen Incidents</u> |
| 3 | Pure risk | <u>Compliance risks</u> |
| 4 | Management risk | <u>Financial risks</u> |
| 5 | Management risk | <u>Intellectual property risks</u> |
| 6 | Pure risk | <u>Risks related to environment and climate change</u> |
| 7 | Management risk | <u>Risks related to suppliers, alliances, etc</u> |
| 8 | Management risk | <u>Customer risks</u> |
| 9 | Management risk | <u>Risks related to competitors and industries</u> |
| 10 | Pure risk | <u>Deficiencies or flaws in products and services</u> |
| 11 | Management risk | <u>Risks related to public regulation, public policy and tax matters</u> |
| 12 | Management risk | <u>Risks related to human resources</u> |
| 13 | Pure risk | <u>Human rights risks</u> |
| 14 | Management risk | <u>Risks related to economic and financial market trends</u> |
| 15 | Management risk | <u>Risks related to investment decisions and business restructuring</u> |
| 16 | Pure risk | <u>Risks related to the Fujitsu Group facilities and systems</u> |

*1 These are just some examples of the risks associated with doing business. More detailed risk-related information can be found in our securities and other reports.

<https://pr.fujitsu.com/jp/ir/secreports/>

Please refer to the web page below for detailed risk information in accordance with our Task Force on Climate-related Financial Disclosures (TCFD) declaration.

"Response to Environmental Risks"

<https://www.fujitsu.com/global/about/environment/risk/>

Risk Management Education, etc.

To enforce risk management across the entire Fujitsu Group, we conduct education and training at every level.

These programs are targeted at newly appointed executives and managers, as well as others, to educate them on our basic approach to risk management and our rules for promptly escalating issues to the Risk Management & Compliance Committee. The programs present specific instances relating to products, services, and information security, with the aim of continually improving participants' awareness of risk management and enhancing their capacity to respond to risks.

Furthermore, by incorporating risk management into employee evaluation indicators, the risk management departments aim to not only link evaluations to financial incentives, but also enhance the organization's risk responsiveness by improving its risk management skills.

Refer to the "FY2023 Performance" section for information on education outcomes for FY2023.

Group-Wide Disaster Management

The basic policy of Fujitsu and its group companies in Japan is to ensure the safety of staff and facilities when disasters occur, to minimize harm and to prevent secondary disasters. We also aim to ensure that business operations resume quickly, and that we can assist in disaster recovery for our customers and suppliers. To this end, we are building robust collaborative structures in our internal organizations and strengthening our business continuity capabilities. In addition to supporting our customers through the management structure in each business unit and group company, the Fujitsu Group is building 'area-based disaster management systems' in each region for working in cooperation with and responding to customers.

To verify the efficacy of our disaster management systems and enhance our response capabilities, we conduct drills tailored to every level, from the entire company through to task forces, workplaces, and employees. We also implement voluntary inspections and verification activities to prevent accidents and minimize the level of harm in each of our facilities. These efforts enable us to accurately identify existing issues and review and implement measures to address those issues, thereby allowing us to work toward continually improving our capacity to prepare for disasters and sustain our business operations.

For more information on our Group-wide disaster management, joint disaster response drills and verification activities, please refer to the PDF listed below, and for activity outcomes for FY2023 refer to the “FY2023 Performance” section.


- [Group-wide disaster management, joint disaster response drills, verification activities](#) 

Business Continuity Management

Recent years have seen a myriad of risks that threaten continued economic and social activity. Such events include earthquakes, floods and other large-scale natural disasters, disruptive incidents and accidents, and pandemics involving infectious diseases. To ensure that Fujitsu and its group companies can continue to provide a stable supply of products and services offering the high levels of performance and quality that customers require, even when such unforeseen circumstances occur, we have formulated a Business Continuity Plan (BCP). We are also promoting Business Continuity Management (BCM) as a way of continually reviewing and improving our BCP.

Regarding the COVID-19 pandemic, to maintain the safety of its customers, suppliers and employees, and their families, the Fujitsu Group placed the highest priority on preventing the spread of the infection. It is also promoted initiatives to sustain the supply of products and services to customers and to help resolve the many societal issues that arose due to the spread of the infection.

For more information on our BCM activities, infectious disease countermeasures and BCM in our supply chain, please refer to the PDF listed below, and for activity outcomes for FY2023 refer to the “FY2023 Performance” section.

- [BCM activities, infectious disease countermeasures, supply chain BCM](#) 

FY2023 Performance

Risk Management Education

— Fujitsu Group new executive training: 45 people

Uses specific examples to illustrate key points that new executives need to take note of, including internal regulatory systems and issues relating to risk management and compliance.

— Training for Board of Directors: 9 (including 6 non-executive directors)

Providing e-learning in various fields, including risk management, for non-executive and executive directors. In addition, individual sessions on risk management for non-executive directors were held by executive officers in charge.

— Fujitsu Group new manager training: 1,033 people

An e-Learning course that covers areas such as the basic approach to risk management and the role of managers regarding risk management.

— Risk management education program: Fujitsu Group 120,000 people

Implemented e-Learning on risk management in general (information security, compliance, etc.)

— Disaster Management Forum: 314 people

These forums are targeted at Fujitsu Group staff responsible for disaster management and business continuity in Japan. They offer an opportunity for participants to share knowledge with the aim of improving our on-site responses to large-scale disasters.

Serious Incident Response Training

— Information security incident response exercise in overseas regions (Asia Pacific: 90; Americas: 75): 165 people in total

Implement the flow of initial response when an information security incident occurs by connecting Japan and overseas regions in real time, and confirm and verify the incident response process including cooperation/information sharing within the region and with the head office, customer response, response to personal information leakage, and media response. Strengthen incident response capabilities and inter-organizational cooperation in overseas regions by identifying issues through training and making continuous improvements.

Disaster Management & BCM Training

— Joint disaster response drills: The FY2023 Near-field earthquake in the Tokyo Metropolitan area

These drills are used to ensure and to verify that Fujitsu and its group companies in Japan are fully versed in the essentials of dealing collaboratively with major disasters. (Proposed scenarios include “Tokyo Inland Earthquake” and “Nankai Trough Megathrust Earthquake”.)

— **Training exercise involving a hypothetical pandemic scenario to check BCP**

A remote work-from-home training exercise centered on a hypothetical pandemic scenario was implemented for all our employees around the globe. The objective was to raise the awareness of each employee involved in business continuity, and measure the business continuity capabilities of the organization as a whole. In addition, the feedback on the findings of the BCP survey that was conducted will help improve the Fujitsu Group's BCP.

Information Security

Policy

The Fujitsu Group has appointed a dedicated Chief Information Security Officer (CISO) to strengthen our information security management regime, while at the same time developing globally consistent security policies and measures to ensure the information security of the entire Group and to ensure and improve information security for customers through our products and services.

Management Structure

<Top Management-led Information Security Control>

With the rapid increase in more complex and sophisticated cyber attacks, strengthening information security has become a top priority for national economic security and corporate business activities. In order to further strengthen and ensure the effectiveness of information security policies, we believe it is necessary more than ever before to take prompt and appropriate actions under the leadership of top management. Therefore, we have enhanced the structure and functions of the Risk Management and Compliance Committee, chaired by the CEO of the Fujitsu Group, where critical risks and compliance issues in Fujitsu Group are discussed, to enable a continuous, company-wide cyber security controls.

In parallel with the security controls by the Risk Management and Compliance Committee, monthly Regular Meetings on Quality and Security Measures have been established as a venue for discussing countermeasures involving the CEO, CISO, CRMO (Chief Risk Management Officer), CQO (Chief Quality Officer), and the heads of each business group to share the status of information security and strengthen measures according to the given status, thereby ensuring CEO-led risk management.

<Enhanced CISO Governance Structure>

CISO governance structure includes regional CISOs in Japan and three international regions (Americas, Europe, and Asia Pacific) to strengthen information security through a globally integrated structure by aligning headquarters policies with the security requirements specific to each country.

For Fujitsu headquarters and group companies in Japan and international regions, information security managers have been assigned to strengthen autonomous information security in each department, and a system has been established to reinforce the leadership by the CISO.

Specifically, our security manager system ensures that each department has an “Information Manager,” who oversees the management and protection of information; an “System Security Manager,” who supervises the maintenance and management of information security system; and a “Product Security Incident Response Team (PSIRT^{*1}) Manager,” who leads product vulnerability management., so that they can promote various information security measures in cooperation with the CISO.

^{*1} Product Security Incident Response Team (PSIRT): An organization that is responsible for incident resolution involving products offered by the company



Information Security Management System Run by CISO and Information Security Managers

Information Security Initiatives

Our Goals for Information Security

Our goal is to achieve information security to provide secure services to our customers through appropriate risk control by planning/executing proactive security strategies and initiatives based on security lifecycle management.

In order to achieve this goal, we are committed to “respond to cyber attacks with ever-evolving advanced information security” and to “improve the awareness of each employee and reform our organizational culture,” which are the keys to success. The entire Fujitsu Group is united in the efforts to develop processes, rules, and methods to promote cybersecurity practices, and to strengthen information security for the entire Fujitsu Group and while ensuring a safe environment for our customers and partner companies.

Company-wide Security Risk Management Scheme

To achieve our information security goals, we have established a “Company-Wide Security Risk Management Scheme” which focuses on highly objective security risk identification, visualization, and their precise remediation.

The Company-Wide Security Risk Management Scheme forms a dual-loop structure as shown in the figure below. Under the scheme, a combination of security measures is implemented to address each issue identified by visualizing security risks, and senior management, departments, and the CISO organization collaborate on a response through organic activities.

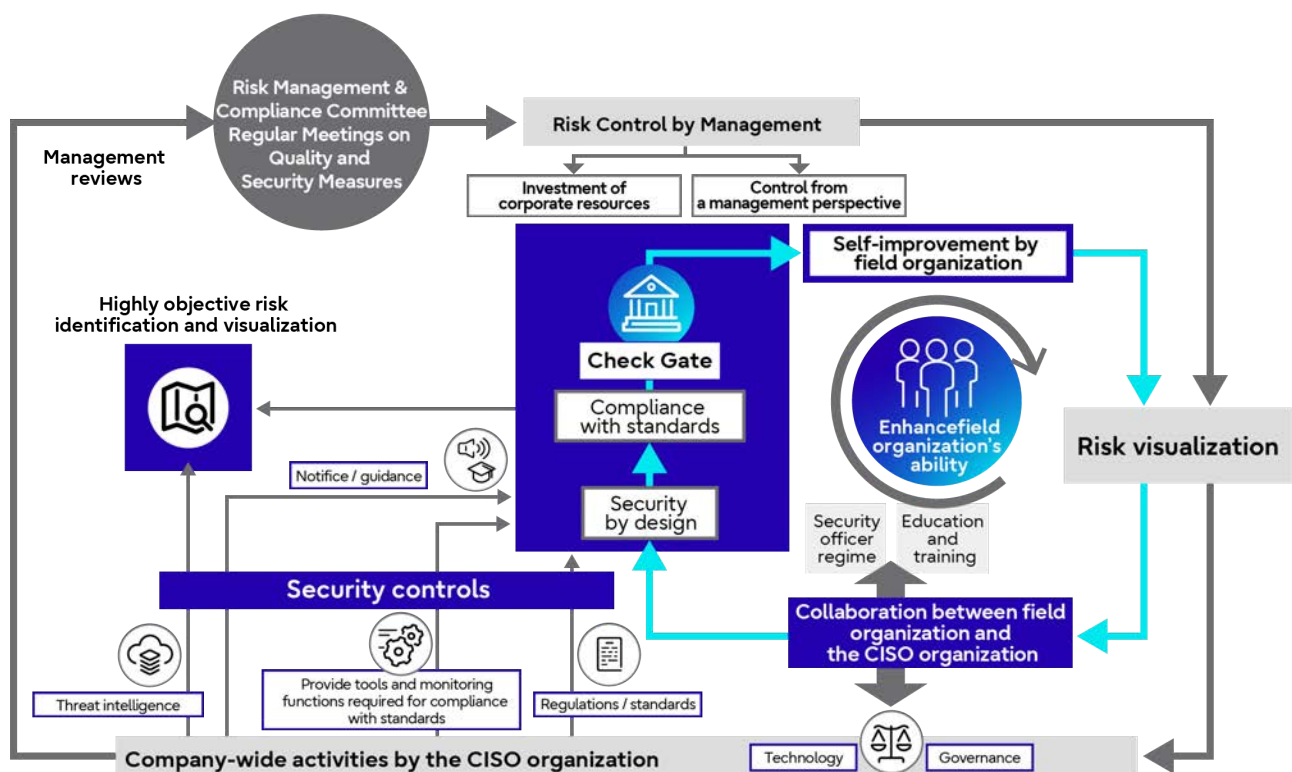
This dual-loop includes, monitoring by senior managements through monthly reviews conducted during the Risk Management and Compliance Committee and Regular Meetings on Quality and Security Measures where senior management is directly involved. This enables security measures under the responsibility of the CISO to be considered as part of the business priorities and can be pursued with the same perspective as the senior management, thereby realizing a company-wide risk management cycle.

- **Outer loop (gray arrow)**

Control loop consist of a role to strengthen senior management involvement by making visualized risks available to senior management, and a role of risk management with security governance by the CISO organization.

- **Inner loop (blue arrow)**

Autonomous loop to promote self-improvement (autonomous corrective activities based on principles) in each department to ensure correct understanding of the situation in their own department through highly objective risk visualization.



Dual-Loop Company-Wide Security Risk Management Scheme

<What Can be Realized through the "Company-Wide Security Risk Management Scheme">

In the dual-loop of the Company-wide Security Risk Management Scheme, "Risk visualization" serves as a common checkpoint between the outer loop and the inner loop. By rotating the dual-loops starting from this checkpoint enables information security to be continuously maintained, improved, and enhanced. By continuing this cycle, the scheme becomes firmly established thus realizing a reform of the organizational culture.

<Visualization of Security Risks Using Technology>

"Visualization of security risks," is enabled by introduction of CMDB*2 and Information Management Dashboards*3 to digitally (mechanically) visualize risks such as the residual vulnerabilities of information systems and inappropriate information management practices. For example, if a vulnerability is detected through a process of matching the information system configuration information registered in the CMDB with the Vulnerability Database*4, the system management department is instructed to mitigate the vulnerability by issuing a remediation task ticket. The status after the remediation instruction is also visualized in the remaining vulnerability status dashboard to ensure successful completion of the remediation.

If a particularly hazardous risk is detected through risk visualization, a timely and appropriate remedial solution will be implemented under the control of the management and the CISO.

***2 CMDB: Configuration Management Database**

A database for collecting and consolidating configuration information on information systems, including hardware, software and network. The collected configuration information is used for security inspections/audits, vulnerability mitigation and security incident resolution.

***3 Information Management Dashboard: A digitized information management ledger**

Fujitsu Group manages and utilizes an information management ledger that maintains inventory of confidential information, including name of administrators, storage locations and disclosure restrictions, in digital form. The system checks for consistency with the actual status of information management (e.g., audit logs for storage services) and alerts the managing department if any deficiencies are detected, thereby enabling an immediate response.

***4 Vulnerability Database:**

A database that collects and consolidates known product vulnerabilities.

Similarly, each department is also working to foster an organizational culture that encourages self-improvement based on risk visualization. The first step is to visualize and share the state of the organization's and individual employees' information management literacy (internal factors) as well as the actual state of cyber risks (external factors). (Visualization)

Then, by having each employee correctly understand the visualized risks and take them personally (taking ownership), autonomous information security practices will be facilitated (taking the initiative). Repeatedly reinforcing this process while making improvements, will nurture an organizational culture with effective self-improvement.

Initiatives

In the following chapters, the key initiatives implemented within the "Company-wide Security Risk Management Scheme" are introduced by the following three themes.

- **Cyber security**

Introduction of measures related to information system security (ensuring and maintaining the safety and reliability of information systems and networks), as well as security maintenance activities for Fujitsu products and services

- **Information management**

Introduction of measures to maintain and manage the confidentiality, integrity, and availability of the information itself, including critical information (e.g., confidential information and personal information)

- **Governance enhancement**

Introduction of governance enhancement measures to strengthen the security of the entire organization by disseminating and instilling the security practices.



Three Themes for Information Security Initiatives

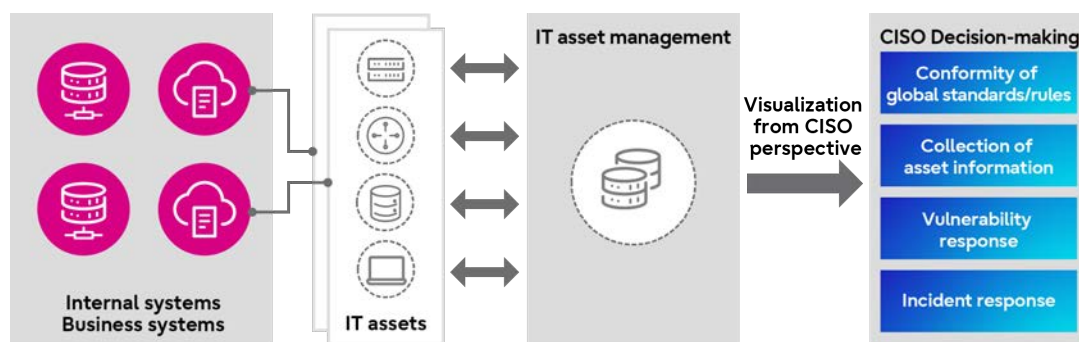
Cyber Security

Based on the IT asset management information of Fujitsu's systems, we will strengthen cyber security practices to prevent security breaches by providing perimeter defense and zero-trust security not only to block any unauthorized access by an attacker, but also to detect and take defensive actions in the event of such intrusion.

Measures Linked to Centralized IT Asset Management

<Autonomous Risk Remediation Through Centralized and Visualized IT Asset Management>

To support our customers' safe, secure, and sustainable business activities, we have centralized and visualized the IT asset management of the IT systems for our globally operating customers, as well as internal IT systems. This helps us promptly identify and remediate any security risks throughout the Fujitsu Group. We have been strengthening routine risk management, visualizing risk audits conducted by the CISO organization and their result, and promoting an appropriate understanding of the actual situation in each departments and their autonomous correction.



Global IT Asset Management

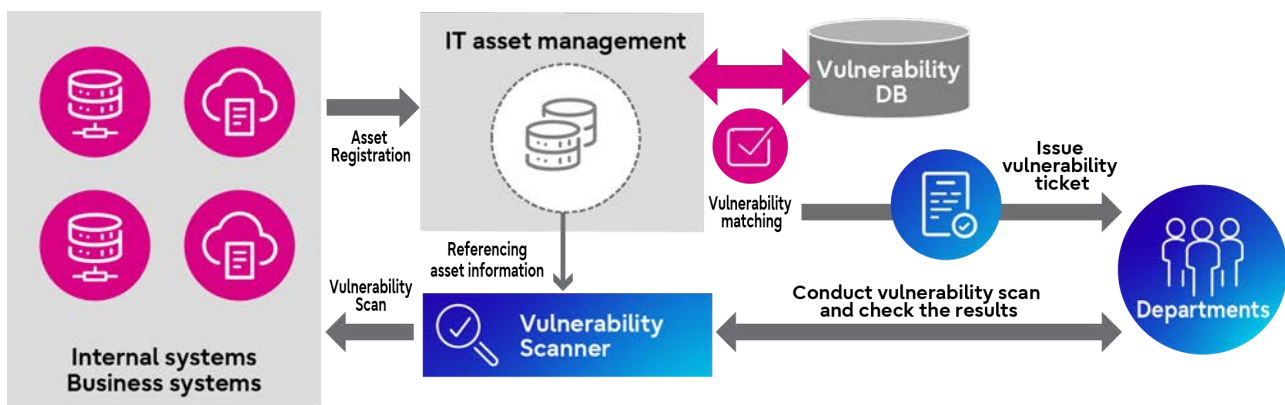
<Vulnerability Detection and Remediation>

By providing vulnerability scanning process for systems (assets) directly accessible from the Internet using IT asset management information, each department that manages the system can autonomously conduct periodic scanning and implement remedial solutions triggered by vulnerability detection. Annual inspection using this process are conducted to ensure that vulnerability remediation practices are in place, and when high-risk vulnerabilities are detected, reliable solution will be implemented in a timely manner with the involvement of the CISO organization.

In addition, by maintaining IT asset management information up to date on a regular basis and matching it with a vulnerability database, any vulnerabilities detected are reported to the relevant department via issued remediation task ticket, ensuring that all vulnerabilities are fully addressed. This process also makes it possible to detect vulnerabilities in systems (assets) that are not directly accessible from the Internet. As of the end of FY2023, we have completed implementing solutions to address the high-priority vulnerabilities^{*5} detected through this initiative for the systems in Japan. For international regions, remedial solutions are scheduled to be implemented by the end of FY2024.

*5 High-priority vulnerabilities:

High-risk vulnerabilities that remain in systems (assets) that are directly accessible from the Internet and that hold sensitive information such as personal data.



Vulnerability Detection and Remediation

<Utilization of Threat Intelligence and Attack Surface Management>

We are proactively utilizing threat intelligence to speed up the detection of, and response to, vulnerabilities in systems exposed to the Internet. Threat intelligence enables us to collect information in the early stage of an actual attack from an attacker's perspective, such as information on global threat trends and vulnerabilities as well as vulnerability information in Fujitsu Group's systems exposed to the Internet. The obtained threat intelligence allows impact analysis and prompt remedial action.

Moreover, in combination with vulnerability scanning of Internet-exposed systems based on IT asset management information, we also implement attack surface management, which monitors system vulnerabilities from an attacker's perspective.

Thorough Monitoring

The cyber security environment is constantly changing, and attack methods are becoming more complex and sophisticated. Under such circumstances, the Fujitsu Group takes a zero-trust approach, based on the concept that 100% prevention of intrusion by cyber-attack is impossible, to reinforce security monitoring. We have established internal guidelines for security monitoring and conduct periodic system inspections to assess and visualize the current situation. We are also working to ensure a sound monitoring to enhance detection capabilities and enable timely response to cyber-attacks. Furthermore, we ensure that critical systems are thoroughly monitored through third-party inspections conducted by the CISO organization. As of the end of FY2023, we have completed enhancing and improving capabilities for detecting cyber attacks against critical systems in Japan. For international regions, formulation of a improvement plan was completed at the end of FY2023, and actual improvement is scheduled to be completed in accordance with the plan during FY2024.

Response to Incidents

As a company that supports the safe and secure business activities of our customers, we need to be able to respond immediately to increasingly advanced and sophisticated cyber attacks. For this reason, we have preemptively established an incident response policy, scheme, and procedures based on the assumption that security incidents may occur during normal times. This allows us to quickly implement a series of procedures in the event of an incident, including escalation, response, recovery, and notification

(1) Escalation

When a security incident is confirmed to have caused damage to the system managed by a department or to a personal terminal, the incident and the extent of the damage are assessed in according to preestablished procedures, and immediate emergency measures to be carried out, while also escalating the incident to the appropriate level. After escalation, support staff will be assigned by the Security Control Organization to assist with incident response, allowing them to work together to resolve the incident.

(2) Incident response

The Security Control Organization and the department managing the affected system cooperate to prevent the spread of damage by shutting down the affected system and/or disabling specific functions. The cause of the incident is investigated and eradicated thereafter. (e.g., application of patches).

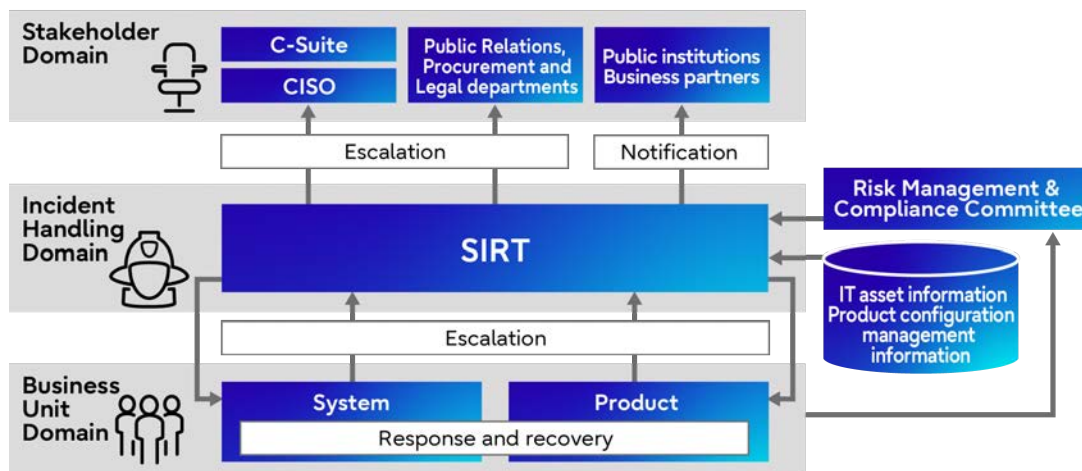
(3) Recovery

After eradicating the cause of the incident, system and business-related data are restored to resume the system and business operations to a normal state.

(4) Notification

Incident details is shared and reported to fulfill our accountability to stakeholders, including public authorities, affected customers, and business partners.

The Incident Response Handbook & Guidelines, which defines the above incident response policies and procedures has been developed and deployed in Japan by FY2023. Versions for international regions will be released and deployed by FY2024 after making alignment with the specific requirements of each country.



Incident Response Procedure

<Sophistication of Incident Response>

Responding to a security incident requires an accurate understanding of the event from a technical perspective through log analysis, malware analysis, disk forensics, and other methods. A quick and fitting response also requires determining an overall policy and collaborating with parties involved inside and outside the company.

At Fujitsu, technical experts and members who take the lead on the path to the solution work together to respond to security incidents, following several processes, including the escalation process.

We have been accumulating data on attacker's tools, processes, and access methods and improving technical knowledge and skills of our response team members through continuous training. We also conduct reviews of the result of past incidents we have handled with our global group companies to continuously improve our incident response capabilities, including upgrading our structure, rule and processes and accumulating know-how, to enable immediate responses and minimize the impact of incidents.

Risk Prevention in Our Products and Services

<xSIRT Regime>

To protect customers who use Fujitsu's products and services, we centrally manage product configuration information, IT asset information, and threat intelligence information, which includes vulnerability information. In addition, to enable prompt and proactive response to risks arising from vulnerabilities in products and services, we have established an xSIRT^{*6} regime by assigning PSIRT managers and System Security Managers, who are responsible for managing vulnerabilities in their departments.

*6 xSIRT: Security Incident Response Team

An organization or regime that handles incidents that affect products and services offered by Fujitsu. It plays a similar role to PSIRT, while xSIRT covers wider range of cases.

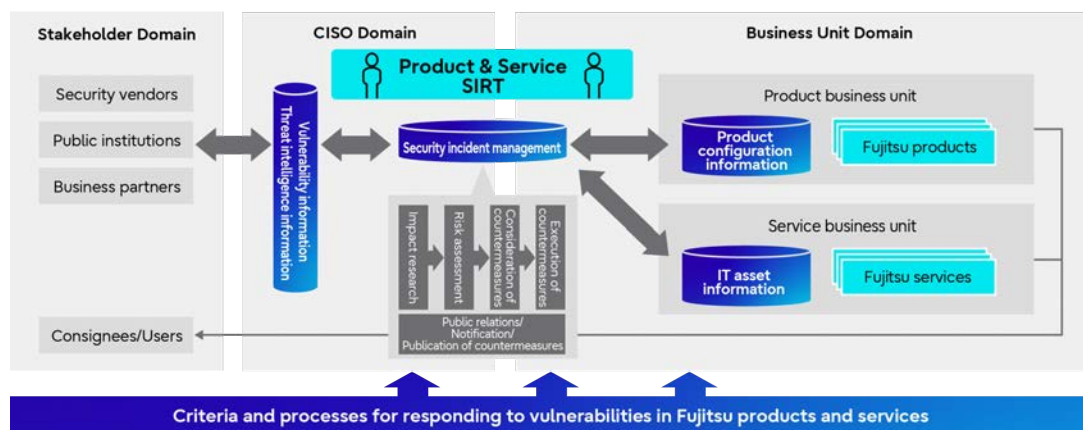
<Process Formulation>

In order to estimate risks to products and services, and to promptly consider and execute countermeasures against vulnerabilities based on risks to products and services, we have established criteria and processes for addressing risks associated with vulnerabilities, and are continuously improving these processes based on statistical analysis and our past incident response results.

With these regime and processes in place, we ensure prompt remediation of vulnerabilities in order to shorten the vulnerability response time and resolve them in a timely manner, thereby preventing secondary damage to our customers and minimizing the impact on their business continuity.

As an example of the successful achievements of implementing this solution, at the time when a vulnerability-induced cyber attack occurred in the past, which caused significant damage and had an impact worldwide and resulted in a major risk warning from CISA*7, Fujitsu was able to quickly identify the affected system and took appropriate remedial action to avoid damage from information exploitation.

*7 CISA: The U.S. Cybersecurity and Infrastructure Security Agency



Vulnerability Response Framework in Fujitsu Products and Services

Information Management

Fujitsu Group in Japan implemented the Information Protection Management System in order to appropriately protect third-party confidential information (including personal information) and our confidential information. We also apply a PDCA cycle that covers from the “(1) Roles & Responsibilities” to “(7) Review”. In order to clarify information assets that must be protected, we establish appropriate management according to the status of our customers and suppliers, and take initiatives for protecting information. These steps are taken for the autonomous information protection activities (regulations by industry, business type, etc.) conducted by each division while unifying the classification of information on a global scale.

Furthermore, we utilize various automation support tools such as information management dashboards to support appropriate information management, while also making improvements as necessary to realize effective and secure operations.

The main activities of the Information Protection Management System are described below.



Information Protection Management Systems (7 Points)

<Information Protection Management System>

(1) Roles & Responsibilities

Under the CEO, we are building a system to manage and protect information through a global network that is centered on the CISO and overseen by the CEO. We appoint management staff for each department, clarify roles, and promote the appropriate handling of information.

(2) Policies & Regulations

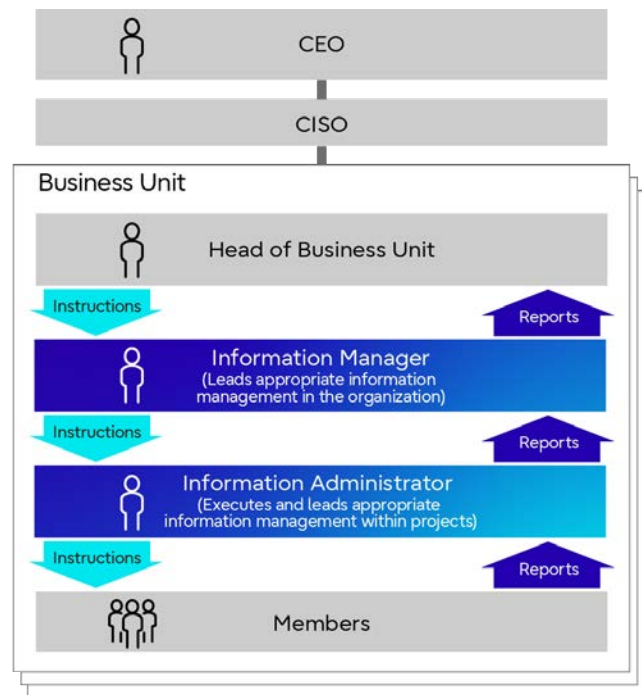
In order to handle information appropriately, necessary rules, procedures, and an annual activity plan have been formulated. Policies and rules are updated on a regular basis, along with changes to the law.

(3) Training & Cultivation of Awareness

In order to improve the information security awareness and skills of each employee, we provide relevant information according to employees' positions and roles. We also provide various training sessions and information in response to changes in the work environment, such as working from home.

Information management training (e-Learning)*8 is provided annually for all employees including executives. Information management training materials are also available to employees at any time.

*8 Number of participants in 2023: 38,603



Information Protection Management System and Roles



Information Security Course 2023-2024

(4) Self-Inspection

Inventory is conducted regularly to identify and classify and perform risk analysis on the information assets retained by each department.

(5) Incident Response

Scheme, escalation routes, procedures are being developed on a global basis to ensure that incidents are addressed appropriately in a timely manner.

(6) Audit

The Information Management Promotion Division confirms the status of information management in each division from a third-party perspective and provide instructions and suggestions for corrections and improvements.

(7) Review/Modification

The Information Protection Management System is reviewed and modified in consideration of external opinions, including audit results, incidents, and complaints, as well as legal revisions, and changes in the environment.

Protection of Personal Information

Fujitsu has established a global Personal Information Protection System to strengthen the protection of personal data. Under the leadership of the CISO organization and the Legal Division, we work with each region and Group company to comply with the laws and regulations of each country, including the GDPR^{*9}. In regard to the handling of personal information, we post and announce privacy policies on public websites in each country.



^{*9} GDPR: General Data Protection Regulation

A European regulation that was put into effect on May 25, 2018 and that requires companies, organizations, and groups to protect personal data. Includes rules on the transfer of personal data outside the European Economic Area (EEA) and the obligation to report within 72 hours of a data leakage at cybersecurity incidents.

The PrivacyMark

In Japan, with the objective of protecting personal information, Fujitsu Group obtained certification for the PrivacyMark^{*10} by the Japan Information Processing and Development Center (JIPDEC) in August 2007 and we are continually working to strengthen our Personal Information Protection System. Group companies also obtain the PrivacyMark as necessary to ensure thorough management of personal information. Internal audits were conducted in all departments in FY2023.

^{*10} The PrivacyMark

The PrivacyMark is granted to businesses that handle personal information appropriately under a personal information protection management system that conforms to JIS Q 15001:2017.

In FY2023, Fujitsu Customer Service Center Personal Information Protection Desk did not receive any consultations or complaints regarding customers' privacy. No customer information was provided to government or administrative agencies in accordance with the Act on the Protection of Personal Information.

Acquisition of Information System Certification

Fujitsu Group is actively promoting the acquisition of third-party evaluation and certification in our information security efforts.

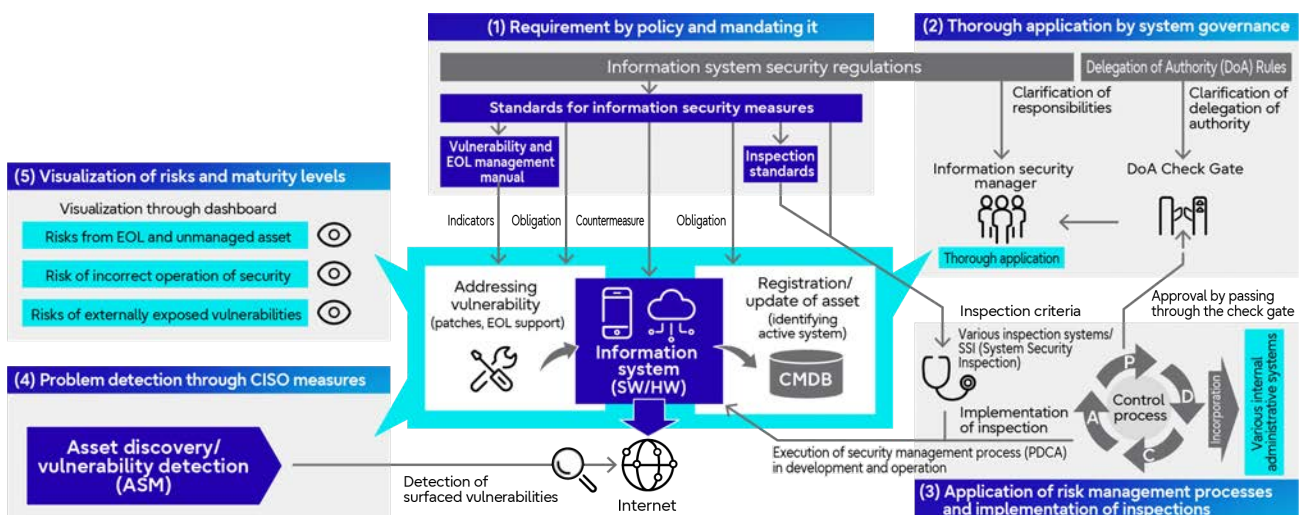
- [Third-party evaluation/certification audit results \(link\)](#) 

Governance Enhancement

We are working to minimize security risks through a multifaceted approach to enhance global security governance.

To ensure common governance in the global group, we clarify what must be done by “(1) making policy requirements mandatory,” and make sure “(2) thorough governance” under the Information Security Management Structure. By organically combining these with “(3) execution of inspections and audits,” mentioned earlier, and “(4) issue detection through ASM,” we realize reliable security measures that each department can carry out autonomously.

In addition, by “(5) visualizing risks and maturity levels” along with metering of security maturity levels, we foster a culture of taking security measures autonomously and thus promote self-improvement effect of cyber-security measures.



Overall Picture of Governance Enhancement Measures

Metering of Security Maturity Levels

Fujitsu leverages the Security Risk and Maturity Monitor to monitor the status of various security measures as a method to facilitate smooth promotion of strengthening organizational governance (common interface of the dual-loop) through the Company-wide Security Risk Management Scheme. Two functions of the monitor are; a Risk Monitor to visualize risks, and a Maturity Monitor to visualize maturity levels. This enables both management and each department to identify risks and check maturity levels using the same yardstick.

<Risk Monitor>

The Risk Monitor provides a comprehensive view of each department at Fujitsu headquarters and Group companies and visualizes numerical values of risks. For risks detected by the aforementioned vulnerability scanning, the number of cases still requiring remediation is displayed on a heat map and graph according to their criticality, allowing for prioritizing and mitigating risks with high severity.

<Maturity Monitor>

The Maturity Monitor digitally scores factors such as the occurrence of vulnerabilities and the speed with which vulnerabilities are remediated. By visualizing the maturity level of each department at Fujitsu headquarters and Group companies on a monthly basis, we foster a culture of autonomous implementation of specific solutions and corrective actions based on an understanding of current circumstances and gaps from targets, and promote self-improvement for cybersecurity practices in each department.

Inspired by the C2M2^{*11}, or Cybersecurity Capability Maturity Model, and SIM3^{*12}, or Security Incident Management Maturity Model, both of which have been proven globally, our security maturity level evaluation indicators incorporate a unique method of scoring maturity mechanically from data taken from our security measures. The maturity levels are scored on six axes: governance, human security risk management, system security risk management, information asset risk management, incident detection and response capabilities, and organizational culture and mindset.

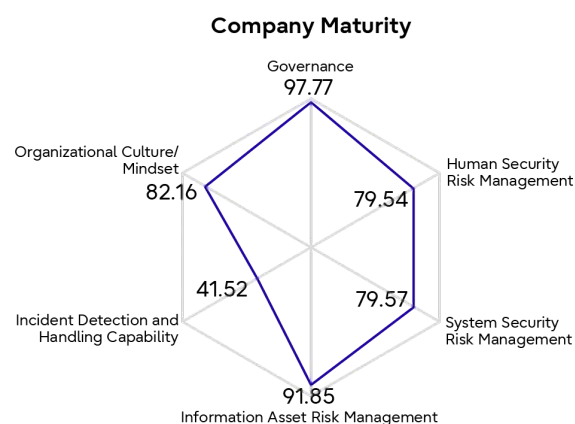
In addition to Fujitsu's internal metering described above, we aim to strengthen our cybersecurity incident response capabilities by using external security rating services to continuously check Fujitsu's security scoring, which is highly objective from a third-party perspective.

*11 C2M2 : Cybersecurity Capability Maturity Model

*12 SIM3 : Security Incident Management Maturity Model

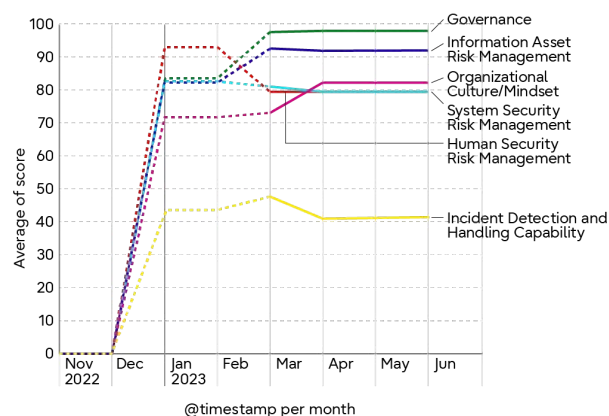
The following is an example image from the Maturity Monitor.

Visualized Security Maturity Level



Company Maturity

Maturity Score Trends (Entire Company)



Maturity Score Trends (Entire Company)

Visualized Graph of Security Maturity Levels (sample)

Ensuring Awareness and Understanding of Frameworks, Rules and Processes

Fujitsu is implementing mainly two initiatives to unify and raise the level of information security measures on a global basis.

<Fujitsu Group Standards for Information Security Measures>

The first is the formulation of “Fujitsu Group Standards for Information Security Measures” which set the standard security measures in the group. Consisting of 165 management measures based on the global standards NIST’s ^{*13} CSF ^{*14}, SP800-53 ^{*15} and ISO/IEC27002, the application of management measures according to the importance of information systems and other factors is standardized. Materials such as manuals and guidelines to support the application of such management measures are also available.

<Risk Management Framework>

The second is the development of “Risk Management Framework,” a framework for security risk management in the group. Based on the global standards NIST’s SP800-37^{*16}, the framework defines a set of processes to identify and manage security risks of each organization and information system in a systematic and appropriate manner. Within this set of processes, periodic risk management in each organization and risk management in the development and operation phases of each information system are being standardized. We incorporate these set of processes into the Fujitsu Group’s various business processes to ensure that they are well understood and widely accepted. In Japan, this “Risk Management Framework” has been in operation since FY2023, and we plan to expand its operation to international regions in FY2024.

By sharing these two initiatives within the Fujitsu Group and executing a series of processes of “Risk Management Framework,” management measures based on the “Fujitsu Group Standards for Information Security Measures” are applied to each organization and information system, while running a continuous improvement process. This contribute with our pursuit for effective implementation of security measures and realization of “security by design.”

*13 NIST : National Institute of Standards and Technology

*14 CSF : Cybersecurity Framework

*15 SP800-53 : NIST SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations

*16 SP800-37 : NIST SP800-37 Rev.2 Risk Management Framework

Security Training, Development of Mindset, Human Resource Development and Maturity of Responsible Personnel

As one of the measures to support the improvement of security maturity levels, mentioned above, we are engaged in promoting security education and training. Particularly, we focus on preventing the recurrence of recent incidents. For example, our company-wide mandatory information security education program shares the latest trends of security threats and incident cases and informs trainees of the lessons learned from the past incident responses and the measures that were supposed to be taken, in order to develop a security mindset and strengthen skills of each employee.

<Security Education and Training>

In addition to providing basic education on information management and cyber-security, we thoroughly disseminate the lessons learned from the latest trends and incident responses. We also work to improve the skills of our professional personnel by issuing guidelines on system monitoring for system managers. As incidents cannot be 100% prevented, we have shifted our approach from “efforts to prevent contingencies”, to “efforts based on the premise that contingencies will occur”, thereby strengthening our company-wide incident response capabilities. As part of this effort, the Fujitsu Group conducts company-wide training for executives and employees every six months. Specifically, with the aim of responding quickly and minimizing the impact of incidents that have a social impact, we conduct incident drills in which executives and personnel from various departments participate. We also provide practical training scenarios for SEs and business producers who are involved in external business and internal operations. Insights gained from these training sessions are reflected as appropriate in the Incident Response Handbook & Guidelines described in the "Incident Response" section, and are shared with each department. In addition, targeted e-mail drills are conducted on an ongoing basis to foster a security mindset among each employee.

*Number of training sessions conducted in FY2023: 2 times company-wide training sessions, 1 time targeted e-mail training session

<Strengthening Information Security Structure and Human Resource Development>

In an effort to change employees' mindsets and behavior regarding information security within the Fujitsu Group, the CISO and the CISO organization regularly disseminate information internally, and security measures are taken through security managers assigned to each department.

In 2023, we revised the Professional Certification System to redefine our image of the ideal security personnel, especially security managers assigned in each department. After clarifying security managers' roles and responsibilities and revising their compensation and other aspects, we have been reinforcing security structures in organizations in Japan ahead of international regions since January 2023.

In addition to sharing the actual status of each organization through visualization using the aforementioned "security maturity metering," we are working with each department to improve their security maturity level through regular communication within the security managers' community and through security managers' meetings and subcommittee meetings.

Quality Initiatives

Our Policy

The Fujitsu Group has the important responsibility of supporting businesses and lifestyles of our diverse customer base, beyond developing better society, through providing a wide range of products and services. In order to contribute to the creation of a trusted society, the entire Fujitsu Group utilizes technology to ensure stable operation and improve the quality of our customers' systems.

To that end, the Fujitsu Group has established the Fujitsu Global Quality Policy to put the Fujitsu Way's cherished value of trust into practice. This policy recognizes quality as a foundational part of our business and shows how we will continue to provide safe and secure products/services worldwide.



In line with the Fujitsu Way and the Fujitsu Global

Fujitsu Global Quality Policy / Quality Standards System

Quality Policy, we have established Quality Policy (Standard Policy for Quality Management) and Global Quality Rules under the Fujitsu Group Global Policy which outlines the rules that the entire group adheres to. Under the Fujitsu Group Global Policy, we have established regulations and standards tailored to the characteristics of the countries where we do business, our products/services, customer requests, and applicable laws and restrictions.

For example, in Japan, we have established the Fujitsu Group Quality Charter and .ive Quality Assurance Regulations (including Shipment, Registration, Release, and Safety Promotion Regulations).

All of our measures, from planning to design to verification, production, sales, and even follow-up support, are based on this charter and these regulations. This ensures that we continue to provide products/services that stay one step ahead of our customers and any changes in their business landscapes.

Implementation Policy for the Safety of Our Products and Services

The Fujitsu Group recognizes its social responsibility to contribute to building a safe and secure society. The Fujitsu Group always considers and endeavors to improve the safety of products and services in every aspect of the group's business activities.

1. Observation of laws and regulations

We observe laws and regulations concerning product and service safety.

2. Efforts to secure safety

We try to ensure that products and services are safe in a variety of use situations and take measures as necessary to secure the safety of the products and services. In addition to legally specified safety standards, we develop and observe voluntary safety standards in our endeavors to improve products and services continuously.

3. Prevention of incidents caused by improper use, etc.

For the safe use of products and services by customers, we properly display notices and warnings in handbooks or on the body of the products in order to prevent incidents caused by improper use or carelessness.

4. Collection of incident information, etc.

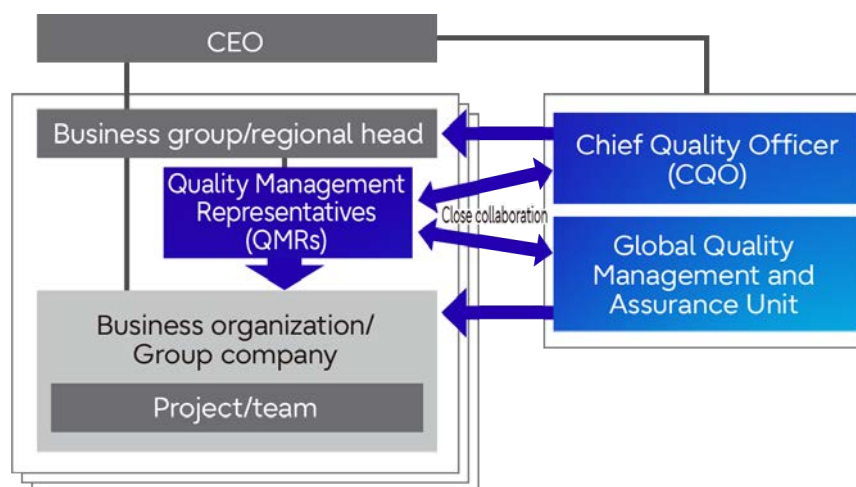
We actively collect safety-related information from customers, including information on product and service incidents and what might lead to such an incident.

5. Handling of incidents

We immediately check the facts of any occurring incident related to a product or service, investigate the cause, and handle it properly. If the product or service has a safety problem, we provide that information to customers and take proper measures, such as product recall, service recovery, and prevention of further damage and other damage from occurring. We quickly report the occurrence of major product incidents to the proper authorities in accordance with laws.

Our Quality Management Structure

The Fujitsu Group appointed a Chief Quality Officer (CQO) in June 2023 in an effort to enhance the quality of our products/services across the entire Group. Furthermore, Fujitsu established Quality Management



Representatives (QMRs) in

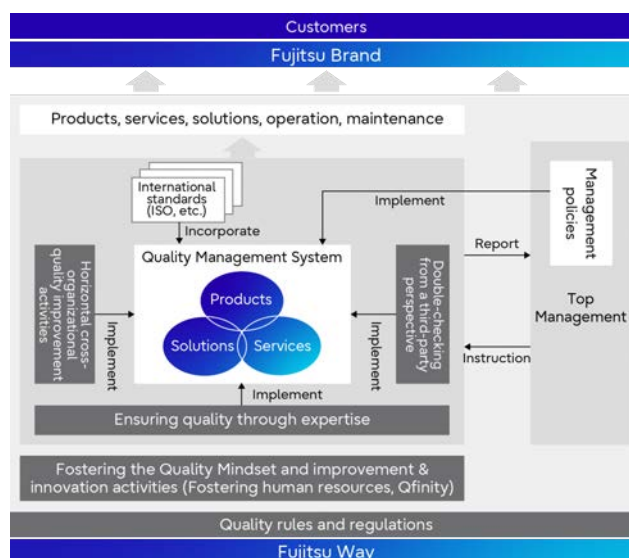
Our Quality Management Structure

each business group and Group company to govern Groupwide quality management under the leadership of the CQO. Following the decision and direction of the CQO, the Global Quality Management & Assurance Unit formulates common policies, standardization, and quality improvement measures as the headquarters of quality. By deploying these common measures through QMRs with close collaboration, we strive toward more field-oriented implementation and application, and perform quality management in an effort to provide products/services with consistent and optimal quality for our customers.

Our Quality Support Framework

In order to provide a level of quality for our products and services which meets the needs and expectations of our customers in a consistent way, it is essential for us to coordinate with various organizations inside and outside Fujitsu—including business units, common business units, and business partners—from planning and design through development, manufacturing, testing, sales, operations, and up until maintenance. Frameworks and mechanisms to integrate these organizations are essential as a foundation for our efforts.

This is why we built our Quality Management System (QMS): to coordinate among these business units as appropriate for the product or service. Our QMS periodically verifies the progress in light of international certification standards such as the ISO in the aim of achieving process improvements to realize even higher quality.



Our Quality Support Framework

Companywide Quality Improvement Cycle

The Fujitsu Group's quality improvement efforts consist of activities based on the Quality Policy by our Companywide Quality Department (Companywide Quality Department Quality Improvement Efforts in the diagram below) and activities to develop and implement quality management systems for each business group (Business Group Quality Improvement Efforts sections of the Companywide Quality Improvement Cycle diagram). These elements turn the cycle, with the entire Group working collaboratively and strategically to improve quality.



Companywide Quality Improvement Cycle

A. Quality policy planning

Quality objectives are set and reviewed, and quality strategies and policies for achieving them are planned and rolled out across the entire Fujitsu Group. In addition, we monitor and manage activities to ensure they are conducted in accordance with our Quality Policy.

B. Quality process regulation/standardization/control

Based on our Quality Policy, we are making progress with the standardization of specific processes and techniques in key areas targeted for improvement. We implement and control these standards at the locations where we operate. Additionally, also in line with our Quality Policy, we promote activities to improve quality across our business groups.

Furthermore, in addition to developing and disseminating quality-related standards, we also share best practices derived from successful projects, so that they can be widely utilized. Further, we promote the sharing of knowledge and project standardization through lessons learned from unsuccessful projects in a manner readily accessible to anyone.

C. Monitoring/independent audits

We monitor the projects of each business group, identify risks to quality at an early stage, escalate issues found, and implement countermeasures as needed. Any concerns regarding quality are addressed by a third party, who audits / conducts an inspection of the items involved, whereby we carry out corrections and improvements.

<In the event of a serious quality issue with any product/service we provide our customers>
Following the Risk Management Regulations, the matter is immediately reported from the field to the Risk Management & Compliance Committee at the Fujitsu Headquarters. Under the direction of the Committee, the relevant departments address the incident jointly and consider ways to prevent recurrence. The recurrence prevention measures are shared with other departments through QMR in an effort to prevent the same incident from occurring at other Fujitsu Group companies.

D. Evaluation/improvement

We regularly examine and analyze our approach to quality and consider additional measures if necessary, directing the QMR to make improvements based on the business characteristics of each organization.

After reporting updates to executive management on a regular basis, action is taken following their decision making and instructions.

Additionally, through Qfinity ([Note 1](#)) activity, good/best practices are commended and shared across the entire Fujitsu Group to increase the level of quality throughout the Group.

Note 1: Qfinity

Qfinity, an internal branding term which combines the words “quality” and “infinity,” represents the DNA of the Fujitsu Group: the “infinite pursuit of quality by each and every employee.” Qfinity is an improvement and innovation activity launched throughout the Fujitsu Group in FY 2001 to continuously improve the quality of products and services, with each and every employee taking a central role. Through Qfinity, we promote quality improvement activities in each workplace and engage in quality improvement of products and services.

Quality Governance

Under the CQO, we are working to strengthen quality governance across the Fujitsu Group as well as prevent major incidents from reoccurring and enhancing the quality of products/services.

The process of strengthening quality governance involves rolling out a common platform to assess quality risk and the quality assurance process that supports service delivery within the Fujitsu Group to correctly assess risks and take thorough action against it.

As the number of challenges in new area of business increases and information systems become more complex, we use these mechanisms as a base to make swift and appropriate decisions and prepare for a variety of risks.

Strengthening the Design/Operation Platform Supporting Quality Governance and Risk Monitoring

We will consolidate quality-related information that we obtain in the development field, such as progress of development projects, test density, and defect detection rate, onto our common platform, Fujitsu Developers Platform. By combining this information with Earned Value Management (EVM) and quality indicators and conducting timely analysis, we will build a mechanism for assessing the quality and delivery decisions in the development field in a more objective manner.



Mechanism for Objectively Assessing Field Decisions

Quality Assurance Processes That Support Service Delivery

To provide customers with higher value than ever before and ensure stable system operation, we are moving to the “One Delivery” project structure—a new type of service delivery that is not organization-dependent. One Delivery manages projects in accordance with the shared “One Delivery Quality Assurance Process” to enable centralized risk management.

The One Delivery Quality Assurance Process embodies four key steps based on past quality issue trends. First, “Resource management” aims to prevent skills mismatch and similar problems. Next, the “GOGI Approval system” determines the promotion of business opportunities and projects from an objective and multifaceted perspective. “Technology control” then aims to improve technological appropriateness and feasibility. Finally, through “business opportunity and quality monitoring”, we detect at an early stage those projects with potential troubles.

We are working to apply and improve the One Delivery Quality Assurance Process, enabling the entire Group to provide higher-quality, more stable services.

Value creation for customers and stable system operation



One Delivery Quality Assurance Process

FY 2023 Performance

Violation of Laws and Regulations Concerning Product Safety

- Violation of laws and regulations concerning product safety: 1 incident (Electrical Appliance and Material Safety Law: Non-compliance with safety design requirements (corrected))

Disclosure of Information Related to Product Safety

- Number of disclosed issues: 0 major product incidents
- Important notices concerning product safety
- Prevention Measures for Laptop Battery Ignition Incidents
 On three previous occasions, Fujitsu has asked customers to exchange and return battery packs in order to prevent the spread of ignition incidents due to the possibility that foreign matter had contaminated the interior of the battery during the battery pack manufacturing process.
 At the same time, however, although extremely rare, there have been cases of ignition occurring in battery packs outside those covered by the returns and exchanges.
 It has been found that limiting the phenomena that increase the internal pressure of batteries is an effective measure in preventing these types of ignition incidents.
 Since February 9, 2017, Fujitsu has been offering a "Battery Charging Control Update Tool" through its website for its laptop PCs launched between 2010 and 2016. In addition, since November 2018, Fujitsu has been distributing the Battery Charging Control Update Tool via Microsoft's Windows Update service to the laptop PCs of all those affected in order to ensure all customers using the affected laptop PCs apply the update.

Non-legal compliance violations related to product safety and information/labeling violations

- Product information and labeling violations: 0
- Violation of the Foreign Exchange and Foreign Trade Act: 1 incident (Documentation errors at the time of compliance evaluation (corrected))

ISO9001 / ISO20000 Certification Status

Fujitsu is continuously working to improve processes under the QMS (items below as of September 2023).

- ISO9001: 21 divisions certified
- ISO20000: 5 divisions certified

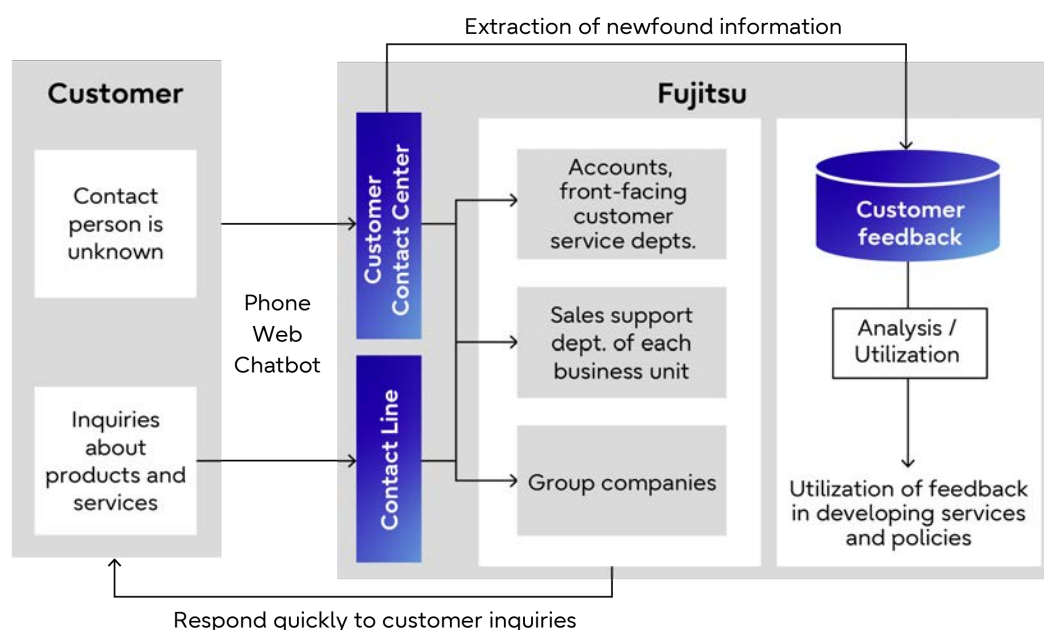
Working With Our Customers

Improving Customer Satisfaction

Our current era is characterized by dizzying levels of social and economic change, and it seems impossible to predict what will come about in the future. In this kind of landscape, it is vital that we maintain an accurate understanding of our customers' various needs and adapt quickly to changes as they arise. In order to accomplish this, we must think and behave from the customer perspective, and engage continuously in reform.

The Fujitsu Customer Contact Center and Fujitsu Contact Line

To be able to address customer inquiries quickly and accurately, the Fujitsu Customer Contact Center and the Fujitsu Contact Line collaborate with multiple departments and utilize AI and chatbots to respond. Furthermore, they also act as a form of surveillance, helping prevent missed and late responses. Not only do they increase customer satisfaction by facilitating quick answers, but they also allow us to analyze information about customer inquiries so that we can improve the development and quality of our products and services.



Operating Framework

- Customer Contact Center / Fujitsu Contact Line (Japanese only)
<https://www.fujitsu.com/jp/about/resources/contact/others/customer/>

Advertising and Promotion Policy

At Fujitsu, we work to make sure that our advertising makes use of fair and appropriate language and symbols, and are in adherence to laws and internal regulations. In FY 2024, we will engender the trust of society through innovation, and promote our initiatives to make the world a more sustainable place, so that those efforts will be more widely recognized. We also set goals (KPIs) and monitor these indices via the PDCA cycle to see if they have been achieved, in order to determine whether our advertising policies have been effective and cost-effective.

Due to changes in the Fujitsu business model, we have also not had products and/or services that would fall under the regulation of the Act Against Unjustifiable Premiums and Misleading Representations.

Fujitsu offer contact lines where the general public can voice their opinions about our advertisements. We take all of these opinions to heart, respond in a measured way with regard to matters that require a response, and do our best to engage in further communication.

- Advertising and Promotion (Japanese only)
<https://jad.fujitsu.com/>