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.

- **[PDF] Corporate Governance Policy**

Corporate Governance Structure (as of June 23, 2025)

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 23, 2025, the Board of Directors consists of nine members in total, comprising three Executive Directors and six Non-Executive Directors (including five External Directors).

In FY2024, the Company held 15 Board of Directors meetings (including three 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, convening extraordinary meetings as necessary in addition to monthly regular meetings. The Board identified the following five themes as the themes that it should focus on based on the business environment surrounding Fujitsu Group: 1) progress in the Medium-Term Management Plan, which the Board had approved; 2)

mechanisms to)ink Materiality to business; 3) development and operation of internal control systems and oversight of risk management; 4)
monitoring of important M&As and reorganization cases; and 5) succession planning of Directors and others.
The Board had discussions with focus on these themes and continued monitoring them.)

Furthermore, the Board discussed agenda items such as shareholder returns, examinations of strategic shareholdings, and feedback on dialogues with shareholders and investors. It also received timely reports from the Risk Management & Compliance Committee that oversees risk management of the entire Group. The reports included monthly updates on the execution status of its tasks and the actions taken regarding individual risks that materialized in FY2024. The Board continued implementing oversight based on these reports. The Company carries out an evaluation of the effectiveness of the Board of Directors every year to improve corporate value by raising the Board's effectiveness. In FY2024, as in FY2023, we conducted a questionnaire for all directors and corporate auditors and individual interviews with each officer based on the answers to the questionnaire, analyzed and evaluated the results, and discussed specific measures at the Board of Directors. As a solution to the issues identified through these efforts, the Company has made efforts to further improve the effectiveness of the Board of Directors by implementing measures such as (1) The Company created a new framework of intensive discussions to confirm the progress of the Medium-Term Management Plan resolved by the Board of Directors and to intensively discuss important management themes, (2) For efficient operation of the Board of Directors meeting, we offered videos explaining agenda items that are suitable for video-based explanation and conducted the meetings on the premise that the participants watched the video in advance using video recordings as an effort to operate the Board of Directors efficiently.

＜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.
The Audit & Supervisory Board has five members, comprising two full-time Audit & Supervisory Board Members and three Independent External Audit & Supervisory Board Members.

In FY2024, the Company held 9 Audit & Supervisory Board meetings, mainly to develop and resolve its audit policy and audit plans, confirm the audit plan and method of Accounting Auditors, examine the appropriateness of their audit results and key audit matters and heard reports from the internal audit section. In addition, the full-time Audit & Supervisory Board Members reported and discussed on important items to External Audit & Supervisory Board Members.

In FY2024, Audit & Supervisory Board Members conducted the following audit 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 FY2024.

＜Independent Directors &Auditors Council＞
The Company has Independent Directors and 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 establish 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 FY2024, the Company held 12 Independent Directors and Auditors Council meetings. The members continuously discussed important management matters such as progress in management policies and business restructuring of the Company and the Fujitsu Group including mergers and acquisitions and shared information and exchanged viewpoints. In addition, in cases of setting prior explanation of important matters that required resolutions at meetings of the Board of Directors as an agenda, a new framework was set up in which a body was structured as a meeting for prior explanation, and full-time Audit & Supervisory Board Members attended as observers. The meeting was held twice during the period under review.

＜Executive Nomination Committee and 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.

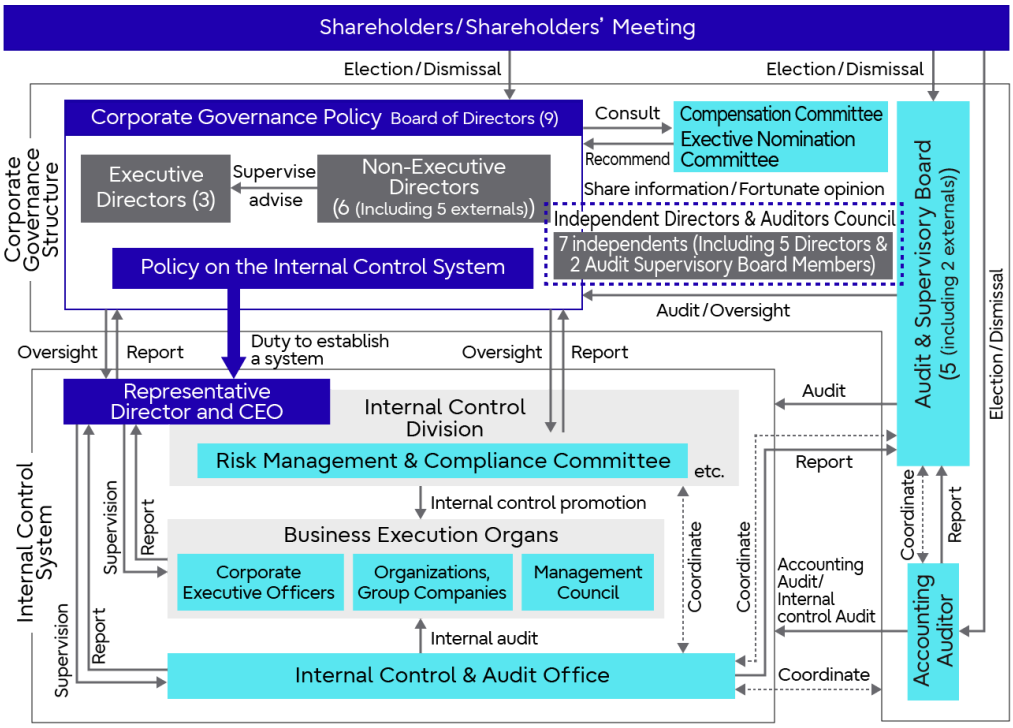
The Executive Nomination Committee deliberates on the candidates for Director and Audit & Supervisory Board Member positions in accordance with the Framework of Corporate Governance Structure and the Procedures and Policy for the nomination and dismissal of Directors and Auditors stipulated in the Policy, 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 performance-based compensation to the Board of Directors in accordance with the Procedures and Policy of Determining Directors and Auditors Compensation, as stipulated in the Policy. Executive Nomination Committee consists of three Non-Executive Directors (including two Independent Directors) and Compensation Committee consists of three Independent Directors. The Members of the 2 committees appointed in June 2025 are as follows. Additionally, the secretariats of both committees are operated by the Company's HR and legal departments. The committee shall consist of Non-Executive Directors and Auditors, more than half of whom shall be Independent Directors. The Chair of the committee shall be an Independent Director.

- Executive Nomination Committee
  Chairperson: Yoshiko Kojo (Independent Director)
  Members: Kenichiro Sasae (Independent Director), Hidenori Furuta (Non-Executive Director)
- Compensation Committee
  Chairperson: Byron Gill (Independent Director)
  Members: Takuya Hirano(Independent Director), Izumi Kobayashi(Independent Director)

In FY2024, the Executive Nomination Committee met ten times and the Compensation Committee met six 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 Chairperson of the Board of Directors, etc. The Compensation Committee discussed the level of compensation of Directors and evaluation indicators for the performance-related compensation for the 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 skills matrix, the succession planning 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 disclosure scope of executive compensation.

The diagram below illustrates the Company's corporate governance structure. (As of June 23, 2025).



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.

Basic Approach to the Internal Control System

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.

- **[PDF] 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.

- **[PDF] Matters Subject to Measures for Electronic Provision (Matters Excluded from Paper-based Documents Delivered Upon Request) at the Time of Notice of the 125rd Annual Shareholders' Meeting**

Disclosures Relating to Corporate Governance

Board of Directors (as of June 23, 2025)

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

- **[PDF] Board of Directors (as of June 23, 2025)**

FY2024 Attendance at Meetings of the Board of Directors or Audit & Supervisory Board

Meeting	Number of Meetings	Attendance Rate
Board of Directors	15	100%
Audit & Supervisory Board	9	97.8%

- [PDF] FY2024 Attendance at Meetings of the Board of Directors or Audit & Supervisory Board

Skills of directors and auditors

As a global company making the world more sustainable by building trust in society through innovation, our company has identified requisite qualities including diversity and the necessary skills for Directors and Audit & Supervisory Board Members to execute operations and provide appropriate advice and supervision in their respective roles.The table indicates skills that the Board of Directors highly expected of, among the skills that each Directors and Audit & Supervisory Board Members possesses.

Directors (as of June 23, 2025)

	Name	Independent	Diversity		Skill Matrix				
			Gender	Nationality	Corporate Management	Finance and Investment	Global	Technology	ESG, Academia and Policy
Non-Executive Chairman, Member of the	Hidenori Furuta		Male	JP	x		x	x	
Representative Director, CEO	Takahito Tokita		Male	JP	x		x	x	
Representative Director, CFO	Takeshi Isobe		Male	JP	x	x	x		
Director and Corporate Executive Officer, CHRO	Hiroki Hiramatsu		Male	JP	x		x		x
Director	Yoshiko Kojo	x	Female	JP			x		x
Director	Kenichiro Sasae	x	Male	JP			x		x
Director	Byron Gill	x	Male	US		x	x		
Director	Takuya Hirano	x	Male	JP	x		x	x	
Director	Izumi Kobayashi	x	Female	JP		x	x		x

- [PDF] Skill Matrix (Directors)

Auditors (As of June 23, 2025)

	Name	Independent	Diversity		Skill Matrix		
			Gender	Nationality	Legal Affairs and Compliance	Finance and Accounting	Operating Process
Full-time Audit & Supervisory Board Member	Yuuichi Koseki		Male	JP		x	x
Full-time Audit & Supervisory Board Member	Kazuo Yuasa		Male	JP		x	x
Audit & Supervisory Board Member	Koji Hatsukawa	x	Male	JP		x	x
Audit & Supervisory Board Member	Hideo Makuta	x	Male	JP	x	x	
Audit & Supervisory Board Member	Catherine O'Connell	x	Female	NZ	x		

- [PDF] Skill Matrix (Auditors)

Definitions of skill matrix categories

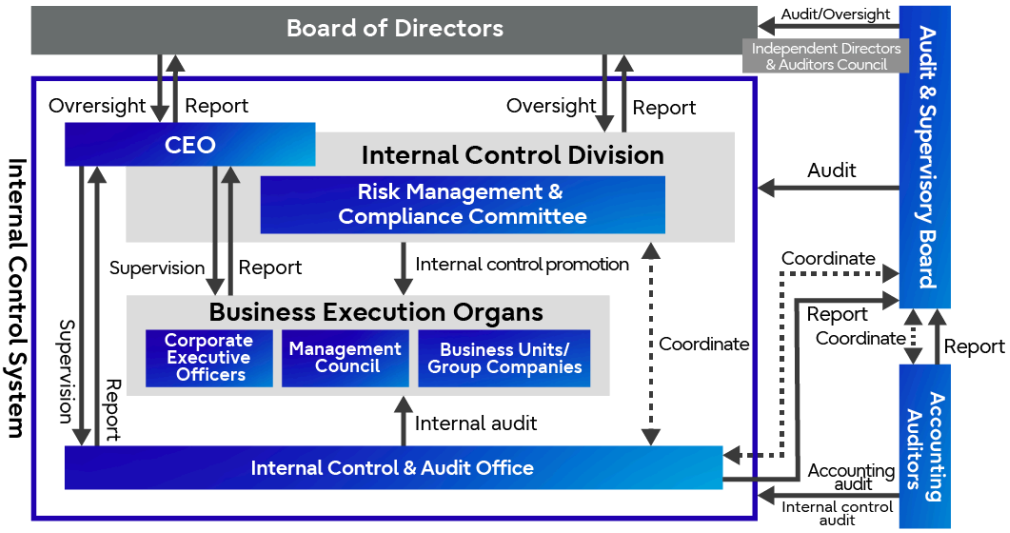
	Categories	Definitions
Director	Corporate Management	Experience in corporate management gained as a top executive or senior management
	Finance and Investment	Experience in formulating and executing financial, capital, or investment strategies at a company, or experience in the financial sector or investment operations
	Global	Experience managing international business operations ,managing in overseas countries , working for foreign companies, or leading activities at international organizations
	Technology	Experience in developing technology strategies or conducting R&D at technology-related companies or organizations, or experience in advanced scientific or technological fields
	ESG, Academia and Policy	Experience as a representative or researcher at government agencies, industry organizations, universities, or research institutes, or experience in external engagement on ESG, academic, or policy-related matters
Audit & Supervisory Board Member	Legal Affairs and Compliance	Experience as a legal professional, legal scholar, or as a corporate legal or compliance officer
	Finance and Accounting	Professional certification as a public accountant or tax accountant, or experience in accounting or finance in general
	Operating Process	Experience in managing overall business processes within a company

- [PDF] Definitions of skill matrix categories

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 (including the Independent Directors and Auditors Council) 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, and ensuring thorough risk management under the CEO's direction. As well it 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 and internal audits by audit departments (Third line).



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

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 Fujitsu 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.
- 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. By plotting to four quadrants on a risk map, important risks are evaluated at four levels (avoid/transfer/reduce/hold). From these evaluation results and status of materialized risks, importance is evaluated and high priority risks are determined.
- Risk Management & Compliance Committee Report
  Analyses are conducted based on the evaluation findings, and mitigation policies are discussed and determined to address high priority risks and 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 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.

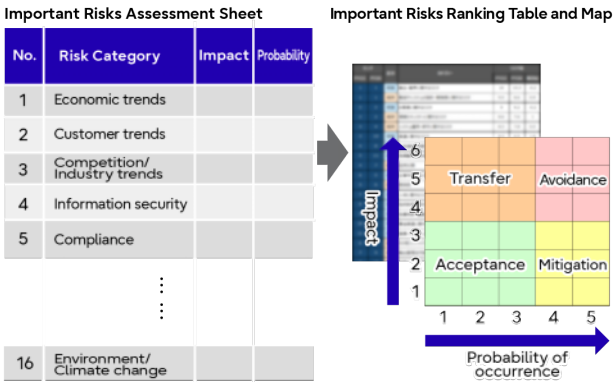
By cycling through this risk management process and having the risk management departments monitor it regularly throughout the year, we aim to reduce risks across the Fujitsu Group and to minimize the impact when risks emerge.

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 Fujitsu Group's business strategies and goals. Consequently, we have identified the following two important risks as high priority for FY2025:

- Security risks
- Deficiencies or flaws in products and services

Risk management process



Visualization of important risks

Important risks of the Group (*1)

- 1. Security risks (Pure risk)
- 2. Risks of natural disasters and unforeseen Incidents (Pure risk)
- 3. Human rights risks (Pure risk)
- 4. Compliance risks (Pure risk)
- 5. Financial risks (Management risk)
- 6. Risks related to environment and climate change (Pure risk)
- 7. Risks related to the Fujitsu Group facilities and systems (Pure risk)
- 8. Risks related to competitors and industries (Management risk)
- 9. Deficiencies or flaws in products and services (Pure risk)
- 10. Risks related to economic and financial market trends (Management risk)
- 11. Intellectual property risks (Management risk)
- 12. Customer risks (Management risk)
- 13. Risks related to suppliers, alliances, etc (Management risk)
- 14. Risks related to investment decisions and business restructuring (Management risk)
- 15. Risks related to public regulation, public policy and tax matters (Management risk)
- 16. Risks related to human resources (Management risk)

*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"**

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 "FY2024 Performance" section for information on education outcomes for FY2024.

Group-Wide Disaster Management

The basic policy of Fujitsu and its group companies in and outside 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 FY2024 refer to the "FY2024 Performance" section.

- **[PDF] 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 both in and outside Japan 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.
In its response to disasters and infectious diseases, the Fujitsu Group placed the highest priority on maintaining the health and safety of its customers, suppliers and employees, and their families . It also promoted initiatives to sustain the supply of products and services to customers and to help resolve the many societal issues that arise due to disasters and infectious diseases.
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 FY2024 refer to the “FY2024 Performance” section.

- **[PDF] BCM activities, infectious disease countermeasures, supply chain BCM**

FY2024 Performance

Risk Management Education

Fujitsu Group new executive training: 38 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.

Fujitsu Group new manager training: 1,012 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: 357 people

These forums are targeted at Fujitsu Group staff responsible for disaster management and business continuity, and all employees 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

Serious incident response exercise (Europe region, April 2024: 143 people; Uvance, January 2025: 88 people): 231 people in total

To strengthen the response to a serious incident (including initial measures, cause investigation, cooperation between the site or region and head office, customer response, response to personal information leakage, and media response), we verified the incident response process through training run on two levels, to the site units, and to management in the form of an incident response meeting. Incident response capabilities and inter-organizational cooperation in overseas regions will be enhanced by identifying issues through training and making continuous improvements.

Disaster Management & BCM Training

Joint disaster response drills: FY2024 Drill - Earthquake in the Chugoku/Shikoku area

These annual 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 the “Tokyo Metropolitan Area Earthquake” and the “Nankai Trough Megaquake”.)

Training exercise involving a hypothetical pandemic scenario to check BCP

An awareness training exercise centered on a hypothetical scenario involving the loss of human resources in a crisis situation was implemented for all our employees around the globe. The objective was to raise the awareness of every employee involved in business continuity, and measure the business continuity capabilities of the organization as a whole. In addition, a simulation of operations and inter-organizational coordination as outlined in each organization’s BCP was used to identify issues and improve the Fujitsu Group BCP.

Information Security

Policy

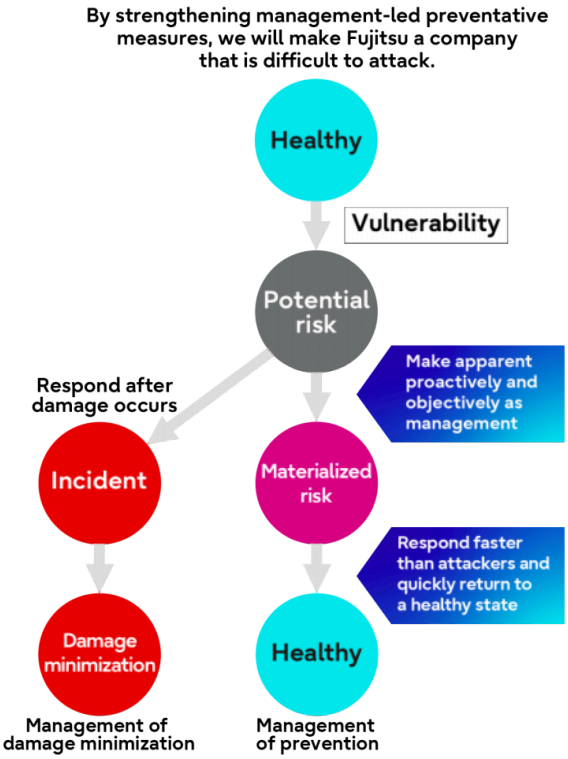
The world is facing more frequent and severe cyberattacks than ever before, which result in a wide range of damages. With advancements in technology that enable the discovery of internet-facing system, it has become easy for any attacker to identify vulnerabilities and launch attacks. Meanwhile, the threats and methods of attack—which we must now be prepared for—are becoming increasingly sophisticated, including exploitation of unknown vulnerabilities and attacks launched within days from public disclosure of vulnerability.
Given this environment, the Fujitsu Group conducts its activities based on Our Purpose which is to "make the world more sustainable by building trust in society through innovation." Fujitsu works with many customers to create value for society. We recognize that if Fujitsu were to encounter a cyber incident, the impact would not be limited to our company alone but could extend to our customers and society as a whole. As such, cybersecurity is positioned as a critical management issue. From top executives to the field organization, the entire organization is united in addressing this challenge. To achieve our information security goals, we have established a "Company-Wide Security Risk Management Scheme."

Approach to Security Management

Since 2021, Fujitsu has experienced multiple serious security incidents, and those in the field organization who are responding to them have faced various internal issues. Addressing these issues, we recognized the need to become—and remain—an organization that is attack-resilient. Being "attack-resilient" means creating a situation where attackers perceive that attacking our organization is not easy and that the likelihood of a successful attack is low.
To become an organization that is attack-resilient, we are thoroughly eliminating security risks that could serve as potential entry points for external attacks, such as vulnerabilities in internet-facing assets. By doing so, we aim to create a state where it is extremely difficult for attackers to even identify potential entry points, and even if one is found, executing an attack becomes highly challenging.

Security Risk Management as an Attack-Resilient Company

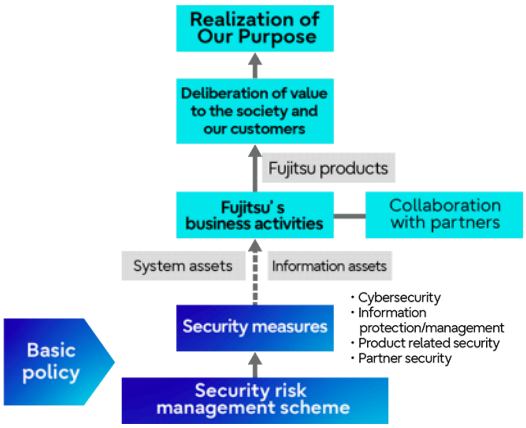
Fujitsu's conventional approach to security risk management was rooted in standard risk management practices, with an emphasis on minimizing damages through post-incident response. As a result, potential risks that went unrecognized by field organization gradually enlarged, and the severity of those risks only became apparent after an incident had occurred.
In light of this, we believe it is necessary to proactively identify and materialize potential risks from attackers perspective, and to implement countermeasures in advance. This approach is essential to minimizing the impact of cyber threats. Given the increasingly short window between risk discovery and actual attacks in today's threat landscape, it is imperative to adopt a management framework that enables early risk detection and swift response.



Risk Management through Materializing Potential Risk

Scope of Security Measures

To support the realization of Our Purpose, Fujitsu is implementing security measures based on the assumption that cyber attackers may target not only Fujitsu itself but also our partners and SaaS offerings on our cloud infrastructure. These measures are designed to safeguard customer information across the entire supply chain, both domestically and internationally. Our efforts span cybersecurity for systems that deliver value to our customers (business systems) and those that support internal operations (corporate systems). In addition, we focus on robust information management to ensure proper handling and protection of data and extend our security initiatives to the products we provide as well as to partner companies that form part of our supply chain.



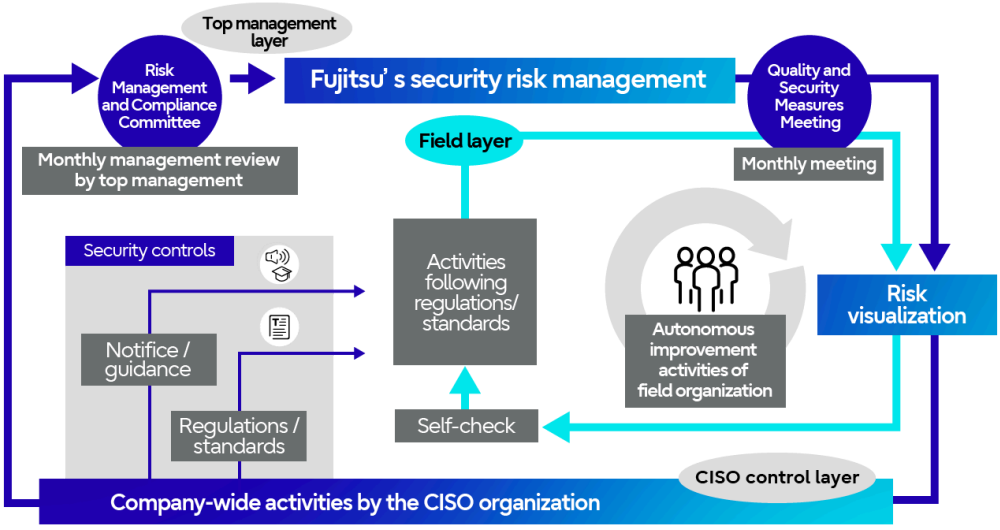
Security Risk Management to Realize Purpose

Company-wide Security Risk Management Scheme

Through our experience responding to past incidents and analyzing those events, we have come to recognize that a security incident occurring within a single department can have impacts that extend beyond our organization, affecting customers and society at large. We have also recognized that enhancing the ability of field organization to proactively identify potential risks and respond swiftly requires direct involvement from senior management. Based on this understanding, we have established a company-wide security risk management scheme that enables senior management layer, field organization layer, and the CISO organization (controlling layer) to work together as one, treating security as a core business issue.

Scheme Overview

This scheme is designed to enable company-wide implementation of security measures, involving senior management, field organization and the CISO, as visualizing risks and building a shared understanding of them are key to driving coordinated efforts across all organizational levels.
The CISO plays a pivotal role in communicating security risks to senior management and fostering a shared understanding between leadership and field organization. This alignment enables effective top-down governance (the outer loop) while encouraging bottom-up improvements (the inner loop). The CISO also defines policies and standards to guide autonomous improvement initiatives at the operational level. In cases where critical and time-sensitive vulnerabilities emerge, the organization exercises direct security oversight of field organization. Through these coordinated efforts, Fujitsu Group advances company-wide security via comprehensive and consistent initiatives across the organization.
The role of the senior management is to make decisions based on information on visualized risks. When risk mitigation measures are implemented at the operational level, field organization sometimes face competing demands—such as increasing business efficiency, reducing costs, and meeting customer expectations. These pressures can at times conflict with security measures and impact the speed of response to such security measures. To address this challenge, management makes decisions based on visualized risks and improves the environment that the field organization cannot resolve conflict or cannot implement the measures even if they want to.
At the operational level, field organization conduct their activities in accordance with company-wide policies and standards set by the CISO organization during normal time. In the event of a security incident due to materialized risk, provisional measures are taken within the respective departments, while formal responses are implemented in line with directions and guidance from the CISO organization. Additionally, teams proactively work to improve their own operations based on visualized risks.



Dual-Loop Company-Wide Security Risk Management Scheme

- Outer loop (dark blue arrow)
  This loop enhances senior management involvement through visualization of security risks and empowers the CISO organization to drive effective risk governance.
- Inner loop (light blue arrow)
  The inner loop serves as an autonomous loop to promote self-driven risk assessment and risk response based on information of visualized risks.

<Company-Wide Security Risk Management in Accordance with the Scheme>

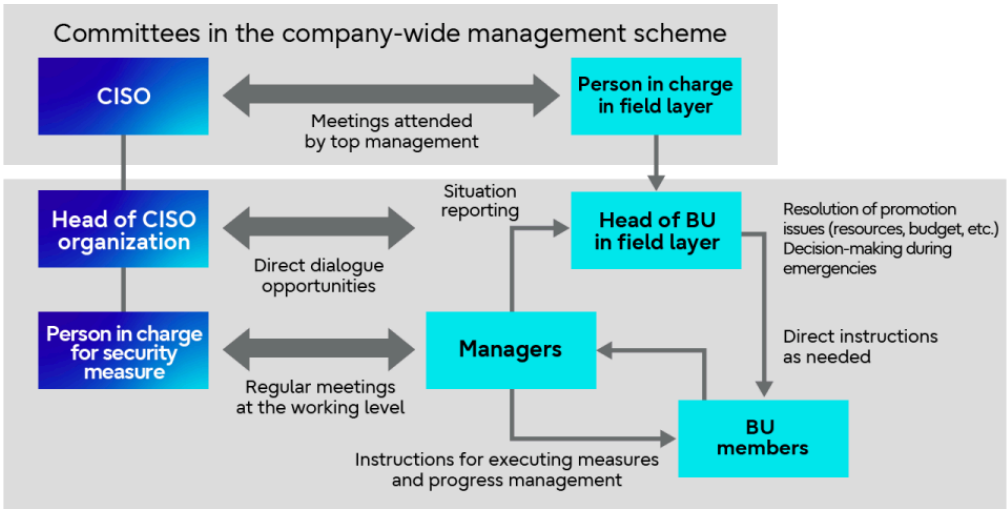
This scheme promotes company-wide security by fostering a shared understanding of risk status and the progress of security measures through two key meetings: the Risk Management and Compliance Committee, chaired by the CEO of the Fujitsu Group, and Regular Meetings on Quality and Security Measures, which includes the CEO, CRMO, CISO, CQO, and heads of each field organization. These meetings bridge communication between management, control, and operational layers of the organization.
For example, it was decided through these meetings that responsibility for implementing security measures would be included in the duties of field organization heads. In addition, departments that were slow to address critical vulnerabilities were identified for the CISO to step in as necessary to prompt the responsible department heads to take action through a top-down approach. This communication approach encourages department heads to not leave security matters solely to their staff, but to take an active leadership role in driving security improvements themselves.
The status of risks and the implementation of security measures are continuously monitored, enabling both management and operational layers to quantitatively assess the response of their respective departments. This monitoring fosters a sense of urgency and risk awareness when responses are delayed. In instances where the implementation of security measures is delayed or deemed insufficient, the CISO may intervene with direct oversight. This has reinforced accountability among operational-level managers, fostering a heightened awareness of their critical role in advancing security initiatives and ensuring more robust execution at the operational level.

Structure and Communication of Security Measures during Implementation

A governance framework has also been established to permeate the CISO organization's policies, standards, and security measures at the operational level. Based on directives from the CISO organization, each of Fujitsu's headquarters, under the authority of its organization head, has appointed three key roles including a System Security Manager, Information Manager, and PSIRT (Product Security Incident Response Team) Manager*1, to promote autonomous security practices within the field organization. The CISO organization engages in structured communication at both the head of Business Unit and security managers in the field organization by pairing head of Unit and persons in charge of initiatives in CISO organization. Specifically, one-on-one discussions are conducted with each division head to convey the current realities facing Fujitsu, including specific incidents, as well as the actual risk landscape within their organization. These conversations aim to foster a shared sense of urgency and encourage division heads to actively engage in their division's security response. Additionally, regular leadership meetings and subcommittees led by persons in charge of implementing security measures provide a forum for dialogue between the CISO organization's initiative leaders and security managers in the field organization. Through these discussions, company-wide policies, standards, and security measures are effectively embedded into day-to-day operations. These efforts strengthen the leadership role of division heads in promoting security initiatives and ensure that responsible officers are executing them effectively at the field organization. For global operations, where alignment between corporate policy and local security requirements is essential, a regional CISO framework has been established to coordinate and oversee efforts by region.

*1: System Security Manager: Person responsible for overseeing the maintenance and management of information systems security.

Information Manager: Person responsible for overseeing information management and protection.
PSIRT Manager: Person responsible for overseeing the management of product related vulnerabilities.



Communication between the Governance Structure and each Layer

<Policies/Standards>

Fujitsu has established a Risk Management Framework grounded in the global standards of NIST's (*2) SP800-37 (*3), to define its approach to security risk management across the Group. This framework outlines a structured set of processes for identifying and systematically managing security risks related to both organizational operations and information systems. It institutionalizes regular risk management activities across all organizational units and embeds these practices as formal rules throughout the development and operational phases of information systems. By integrating these processes into business workflows, Fujitsu ensures widespread awareness and adoption of risk management practices across the Group.
In addition, the Fujitsu Group Standards for Information Security Measures have been formulated with reference to NIST's CSF (*4), SP800-53 (*5), and ISO/IEC 27002 for standardized application across the Group. This standards consists of 165 management measures, which defines how each management measure should be applied based on the importance of the information systems involved. Materials such as manuals and guidelines are also available to support the effective company-wide implementation of these measures.

*2: NIST: National Institute of Standards and Technology
*3: SP800-37: NIST SP800-37 Rev.2 Risk Management Framework
*4: CSF: Cybersecurity Framework
*5: SP800-53: NIST SP800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations

Visualization of Security Risks

Fujitsu has developed various dashboards, such as the Risk Monitor and Information Management Dashboard, for the digital (mechanic) visualization of risks, including status of remaining vulnerability on information systems or improper information management.
The Risk Monitor provides a comprehensive view of each department at Fujitsu headquarters and Group companies and visualizes numerical values of risks. With regard to the risks detected through the above mentioned vulnerability scanning and other measures, the remaining number of corrective actions by severity level is displayed in a heatmap or graph, and it is possible to prioritize the most important risks.

The Information Management Dashboard is a digitized information management ledger that maintains inventory of confidential information, including names of administrators, storage locations and disclosure restrictions in digital form. The system checks for consistencies with the actual status of information management (e.g., audit logs for storage services) and alerts the management department if any deficiencies are detected, thereby enabling an immediate response.
These dashboards are utilized across the management, control, and operational layers, functioning both as governance tools for monitoring field organization and as practical tools for those departments to evaluate their performance and foster autonomous improvement efforts.

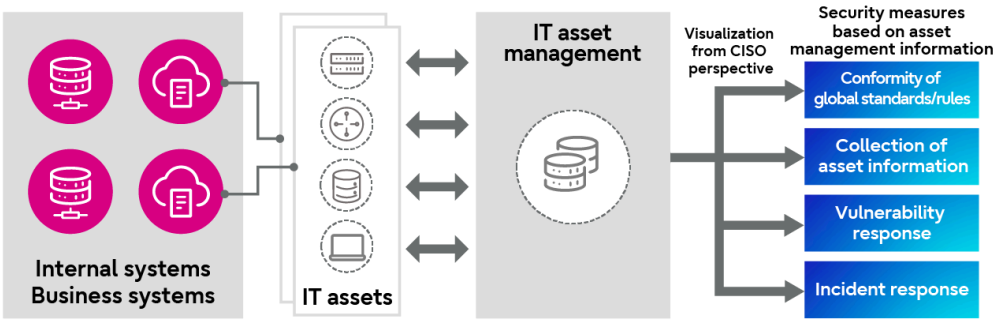
Cyber Security Measures

Fujitsu implements a multi-layered cybersecurity framework. As part of its preventative measures against unauthorized access, the company manages vulnerabilities based on IT asset management data across its systems. In addition, comprehensive monitoring is conducted to detect and respond swiftly in the event of a breach. To further mitigate risk, sensitive information is encrypted to ensure data protection, even in the unlikely event of information exfiltration.

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 data of the IT systems (business 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 remediation.

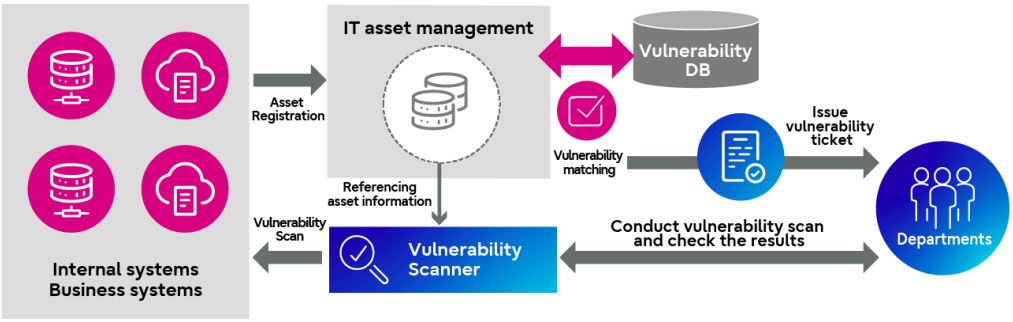


Global IT Asset Management

<Vulnerability Detection and Remediation>

By establising vulnerability scanning process for systems 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.
Even systems that are not directly accessible from the internet may be compromised through lateral movement originating

from internet-facing systems, potentially resulting in broader impact . To address this risk, we regularly update IT asset management information and match with vulnerability database to detect and remediate the vulnerability of systems. This initiative has been rolled out across the entire Fujitsu Group, ensuring proactive management of vulnerabilities in managed assets. As a result, the number of new externally exposed vulnerabilities detected has significantly declined. In particular, detections of high-risk vulnerabilities, such as open ports, have been reduced to just a few cases.



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.

<Establishment of an Emergency Vulnerability Response Process>

It is essential to establish a system that enables swift response to vulnerabilities not only during emergencies but also in normal operations. As such, the following measures have been implemented in Japan: appointment of designated personnel authorized to make service suspension decisions and establishment of comprehensive procedures for emergency vulnerability response.
Today, cyberattacks targeting software vulnerabilities are launched in increasingly shorter intervals following their discovery, while the speed of such threats continues to accelerate. Given these circumstances, as Fujitsu prioritizes the protection of customer data and the delivery of stable services, we may proactively suspend services at our own discretion if a critical vulnerability arises. This action is taken only when rapid intervention, including service suspension, is essential to protect the information assets of both customers and the company. Such decisions are made with the belief that they not only mitigate security risks but also minimize potential business impacts.

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.

Protection of Important Information

At Fujitsu, it is our policy that activities involving the handling of confidential information, such as development and operations tied to customer contracts, are conducted using the Fujitsu Developers Platform. This approach aims to enhance information security and ensure system quality.
The Fujitsu Developers Platform is equipped with features that fundamentally improve information management. These include restricted sharing functions that prevent data mixing across multiple projects by limiting access to designated project members and enforced access deadlines to deter improper data retention after project completion. Additionally, it supports confidentiality-aware information management by issuing alerts when files labeled with sensitivity levels are stored in inappropriate folders. Furthermore, it monitors activities such as downloads to promptly detect and contain potential data leaks in the event of unauthorized access.
Encryption of critical information on the Fujitsu Developers Platform is mandatory. Any unencrypted data is flagged on dashboards to prompt remedial action. Through these measures, we safeguard valuable information assets across diverse business operations and support secure, reliable business continuity.

Response to Incidents

While proactive measures are in place to prevent security incidents, it is equally important to ensure a prompt response in the event an incident does occur, in order to minimize potential impacts. For this reason, we have preemptively established 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.

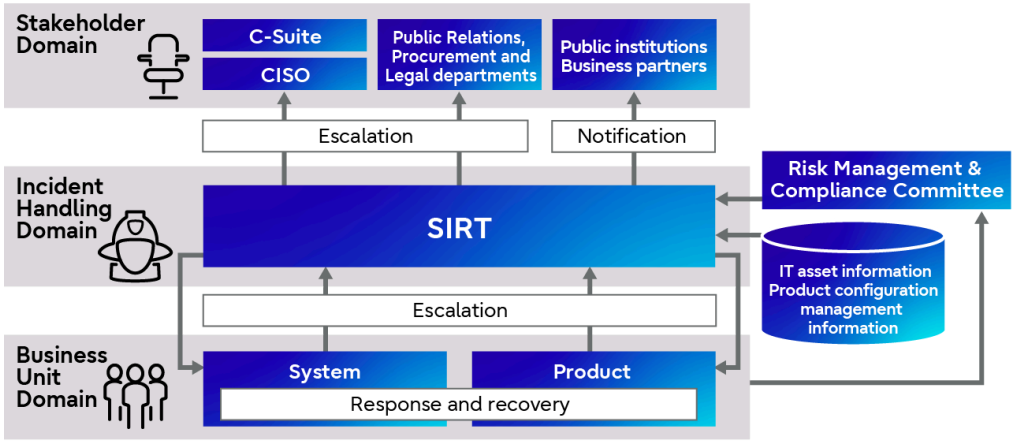
(1) Escalation
When a security incident is confirmed to have caused damage to the system managed by a department or to a personal terminal, the incident and the extent of the damage are assessed according to preestablished procedures, and immediate emergency measures to be carried out, while also escalating the incident to the appropriate level. After escalation, a specialized team 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 procedures has been developed and deployed at Fujitsu Headquarters and Group companies in Japan. In addition, for international group companies, alignment is being carried out to accommodate country-specific requirements.



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>

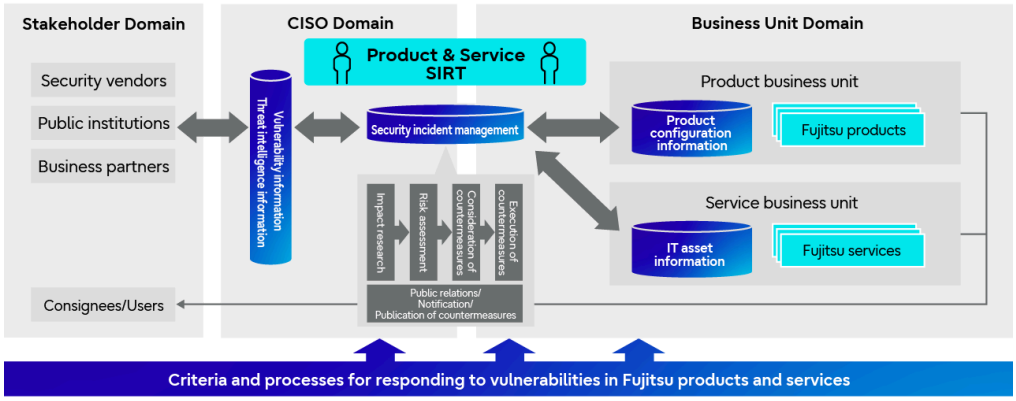
To protect customers who use Fujitsu's products and services, we centrally manage product configuration information, IT asset information, and threat intelligence information, which includes vulnerability information. In addition, to enable prompt and proactive response to risks arising from vulnerabilities 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.

<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. In addition, we 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 has been able to avoid damage from information exploitation based on its prompt identification of the affected system and appropriate remedial action taken.

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



Vulnerability Response Framework in Fujitsu Products and Services

Information Management

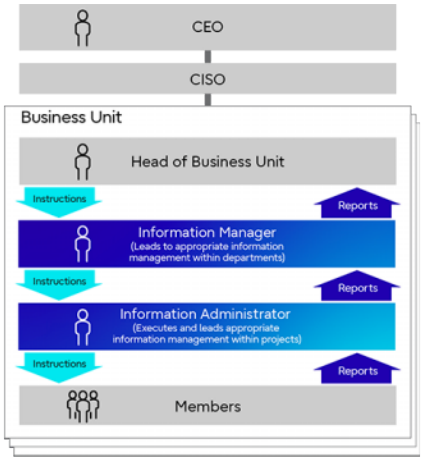
Fujitsu and its Group companies in Japan implemented the Information Protection Management System in order to appropriately protect confidential information (including personal information) of the Group and third parties. We also apply a PDCA cycle that covers from the "(1) Roles & Responsibilities" 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

Information Protection Management Systems (7 Points)

unifying the classification of information on a global scale. Furthermore, we utilize various support tools such as information management dashboards to support appropriate information management, while also making improvements as necessary to realize effective and secure operations. In addition, a number of internal departments have obtained ISMS certification.
The main activities of the Information Protection Management System are described below.

<Information Protection Management System>

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



Information Management System and Roles

(2) Policies & Regulations
In order to handle confidential and personal information appropriately, necessary rules (such as policies on information management, handling of third party confidential information and personal information management), 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 at least once annually for all employees including executives. Information management training materials are also available to employees at any time.

*8: Number of participants in 2024: 37,234

(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 and Audit 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.

Information Security Course 2024-2025

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.

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. The Information Management Promotion and Audit Division conducts third-party reviews of each division's information management practices, providing guidance and recommendations for remedial actions and improvements as needed. Internal audits were conducted in all departments in FY2024.

*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.

In FY2024, 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 Security/ Information System Certification

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

- **[PDF] Third-party evaluation/certification audit results (link)**

Initiative to Promote Autonomous Improvement at the Operational Level

Aligned with the Company-Wide Security Risk Management Scheme, we are driving initiatives that are primarily led by the control layer to enhance organizational resilience against cyberattacks as an attack-resilient company. However, if response efforts at the field organization level are initiated only upon receiving notifications or guidance from the control layer, there is a risk of lagging behind the speed at which attackers operate. To address this, it is imperative that each organizational unit proactively complies with security standards and independently executes timely countermeasures. This self-directed approach is essential to identifying and mitigating risks before they can be exploited.

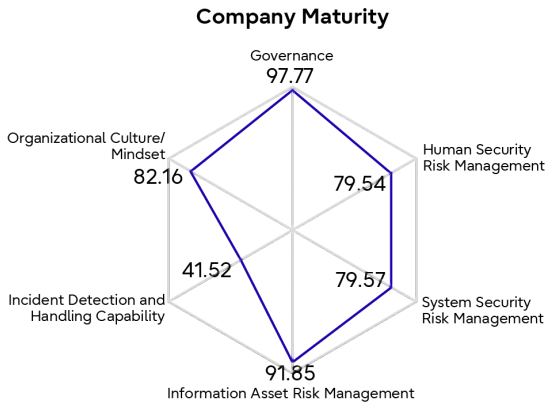
Visualization of Organizational Maturity

<Maturity Monitor>

At Fujitsu, we digitally score factors such as the occurrence of vulnerabilities within organizations and the speed at which they are remediated, and visualize them as indicators of organizational maturity.
By visualizing the maturity level of each department at Fujitsu headquarters and Group companies on a monthly basis, we aim to foster a culture of autonomous implementation of specific solutions and remedial actions based on an understanding of current circumstances and gaps from targets.
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, we aim to strengthen our cybersecurity incident response capabilities by using external security rating services to continuously check Fujitsu's security scoring, which is objective from a third-party perspective.

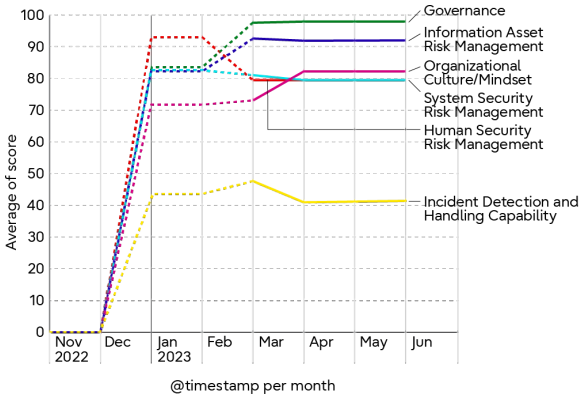
*11: C2M2：Cybersecurity Capability Maturity Model
*12: SIM3：Security Incident Management Maturity Model

Visualized Security Maturity Level



Organizational Maturity

Maturity Score Trends (Entire Company)



Maturity Score Trends

Third-party Assessments

As a global provider of IT services, the Fujitsu Group places great importance on the continuous implementation of security measures and our accountability to stakeholders regarding the soundness of our security status. As part of these efforts, we have adopted the services of third-party security ratings companies SecurityScorecard and Bitsight, which provide objective assessments of our security posture. These services assess risks from an attacker perspective and incorporate publicly disclosed security incidents into an overall score reflecting the soundness of our security status. By utilizing these security rating services to guide our security initiatives, we have achieved and maintained high ratings from both SecurityScorecard and Bitsight.

SecurityScorecard	A Rating
Bitsight	Advanced Rating

(As of May 2025)

The Fujitsu Group is committed to continuously enhancing its security measures based on objective assessments provided through security rating services. Through these efforts, we aim to further strengthen stakeholder trust and contribute to positive business outcomes, including garnering deeper partnerships and expanding the customer base.

Security-Related Human Resource Development

To foster greater autonomy at the field organization, we deliver security education and training that covers the latest threat landscape, as well as incorporates real-world lessons learned from recent incidents that have occurred within Fujitsu.

Through these efforts, we are committed to developing a strong security mindset and strengthening the skills of all executives and employees.

<Security Education and Training>

In addition to providing basic education on cyber-security and information management, we thoroughly disseminate the latest trends, as well as current status and lessons learned from response to incidents occurred at Fujitsu . We work to improve the skills of our professional personnel by issuing guidelines on system monitoring for system managers. Moreover, 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 sales personnel 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 across the Group. 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 FY2024: 1 time company-wide training sessions, 2 times 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 across the Fujitsu Group, and security measures are taken through security managers assigned to each department.
In 2023, the Fujitsu Group redefined the profile of its ideal security personnel and revised the Professional Certification System. In addition to clearly outlining the expected competencies of personnel contributing to security enhancement across the organization, we also launched training programs and aligned compensation schemes to reflect such professional expertise.
Through these initiatives, we are expanding skilled security personnel and reinforcing security frameworks across all departments.

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 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.

Fujitsu Global Quality Policy / Quality Standards System

For example, in Japan, we have established the Fujitsu Group Quality Charter and five 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

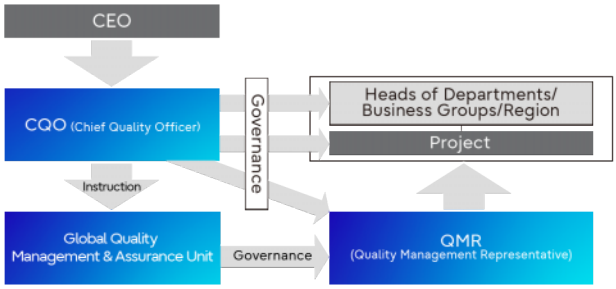
The Fujitsu Group recognizes its social responsibility to contribute to building a safe and secure society. The Fujitsu Group always considers and endeavors to improve the safety of products and services in every aspect of the group's business activities.

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) and have built a quality management system for our products/services across the entire Group. Specifically, under the leadership of the CQO, the Global Quality Management & Assurance Unit, as the company headquarters, promote and implement quality management activities for Fujitsu's entire Group by formulating a company-wide quality policy and strategy, and evaluating its implementation status from independent view point, then executing further improvement actions. Furthermore, Fujitsu established Quality Management Representatives (QMRs) in each department, business group and region to implement quality management in their own organization as our means of governing Groupwide quality management

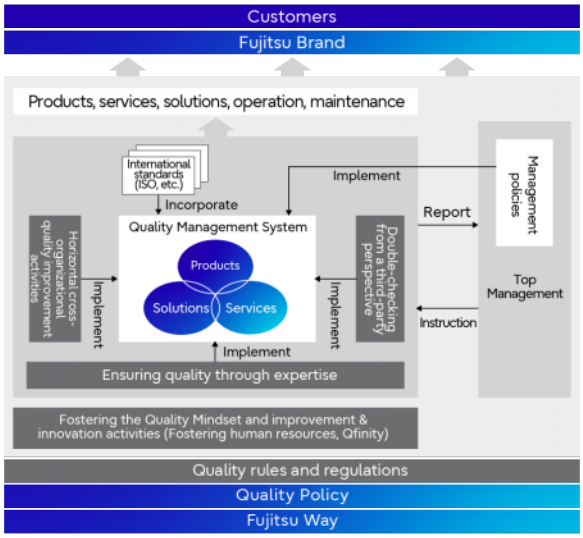
Towards the goal of thorough quality governance, the CQO, QMR, and Global Quality Management & Assurance Unit have established a steering body that regularly discusses issues, countermeasures, and implementation status in the field, as we perform field-oriented quality activities in an effort to provide products/services with consistent and optimal quality for our customers.



Our Quality Management Structure

Our Quality Support Framework

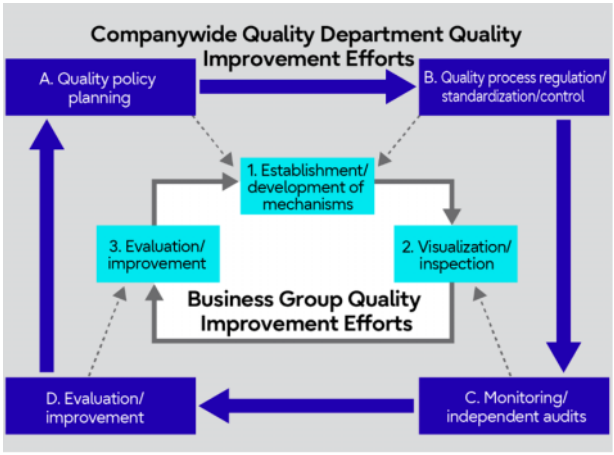
In order to provide a level of quality for our products and services which meets the needs and expectations of our customers in a consistent way, it is essential for us to coordinate with various organizations inside and outside Fujitsu—including business units, common business units, and business partners—from 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 (*1) activity, good/best practices are commended and shared across the entire Fujitsu Group to increase the level of quality throughout the Group.

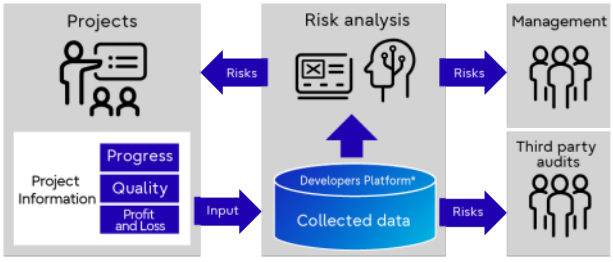
*1: Qfinity
Qfinity, an internal branding term which combines the words "quality" and "infinity," represents the DNA of the Fujitsu Group: the "infinite pursuit of quality by each and every employee." Qfinity is an improvement and innovation activity launched throughout the Fujitsu Group in FY 2001 to 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, while also encouraging the extraction and sharing of key knowledge, as we 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.

< Design/Operation Platform Supporting Quality Governance and Risk Monitoring >

We 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 analyzing this accumulated data with AI to identify potential future risks and urging the teams to plan and implement countermeasures, we aim to improve project success rate.
Additionally, extraction and visualization of risks from quality data obtained in daily activities leads to self-directed



*Developers Platform: A newly introduced standardized development platform that enables delivery transformation throughout the Fujitsu Group

Mechanism for Objectively Assessing Field Decisions

improvements, as project members in the field notice risks by themselves.

< Quality Assurance Processes That Support Service Delivery >

To provide customers with higher value than ever before and ensure stable system operation, we have moved 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.
Through the "One Delivery Quality Assurance Process," the entire Fujitsu Group provides higher quality services with greater stability.

One Delivery Quality Assurance Process

FY2024 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: Conformance error in labeling requirements for the importer (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 in third-party certification: 1 incident (Falsified certification documentation (corrected))

ISO9001 / ISO20000 Certification Status

Fujitsu is continuously working to improve processes under the QMS (items below as of September 2024).

- ISO9001: 20 divisions certified
- ISO20000: 9 divisions certified

Working With Our Customers

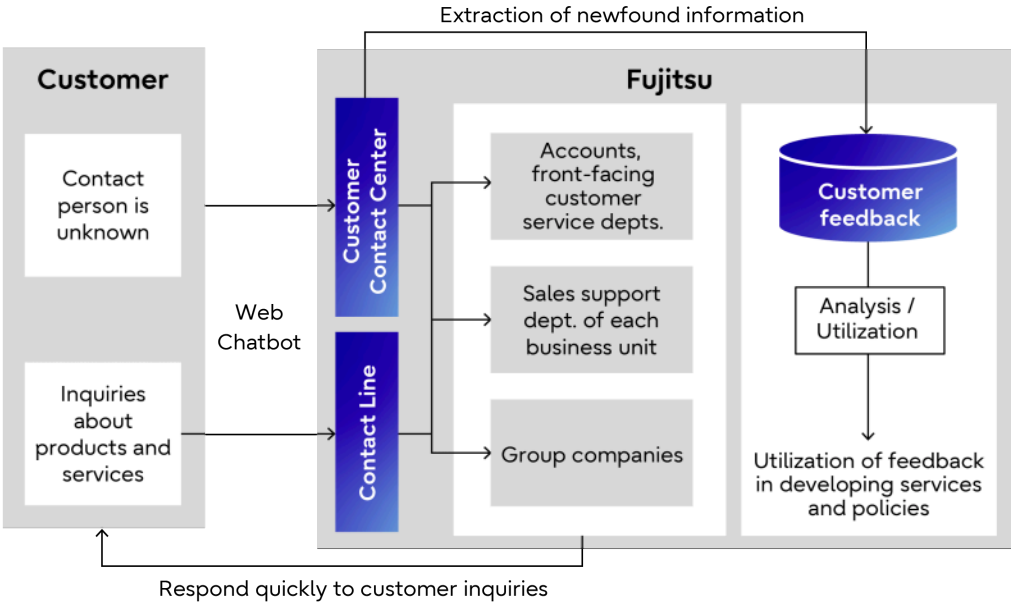
Improving Customer Satisfaction

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.

- **Customer Contact Center / Fujitsu Contact Line (Japanese only)**



Operating Framework

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 FY2025, we will engender the trust of society through innovation, and promote Fujitsu's initiatives under our purpose 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.

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)**