Governance

Corporate Governance

Basic Approach to Corporate Governance

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

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

- Corporate Governance Policy

Corporate Governance Structure (as of June 26, 2023)

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 26, 2023, the Board of Directors consists of nine members in total, comprising three Executive Directors and six Non-Executive Directors (including five External Directors).

The Company held 13 Board of Directors meetings in FY2022 (including one extraordinary Board of Directors meeting) to discuss matters including formulation of the Management Direction and measures for its implementation, as well as to decide a new management system based on the recommendations of the Executive Nomination Committee.

Audit & Supervisory Board

The Company has an Audit & Supervisory Board that performs the auditing and oversight functions. The auditing and oversight functions are carried out by Audit & Supervisory Board Members, who review the Board of Directors as well as business execution functions and attend important meetings, including meetings of the Board of Directors. As of June 26, 2023, the Audit & Supervisory Board has five members, comprising two full-time Audit & Supervisory Board Members and three External Audit & Supervisory Board Members. The Company held ten Audit & Supervisory Board meetings in FY2022 (including one extraordinary Audit & Supervisory Board meeting), mainly to discuss audit policy and plans, the audit method of Accounting Auditors and the appropriateness of the audit results, and the Key Audit Matters. Internal Audit Departments made reports and full-time members of the Audit & Supervisory Board reported matters of importance to External Audit & Supervisory Board Members, which were discussed at Audit & Supervisory Board meetings.

All meetings were attended by the full Audit & Supervisory Board.

Independent Directors & Auditors Council

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

In FY2022, the Independent Directors and Auditors Council met 12 times. The members shared information and exchanged views on important management matters arising from business restructuring in Fujitsu and the Fujitsu Group, including the Company's management direction and mergers and acquisitions.

Executive Nomination Committee & Compensation Committee

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

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

The Executive Nomination Committee consists of three Non-Executive Directors (including two Independent Directors) and the Compensation Committee consists of three Independent Directors. The members appointed to the two committees in June, 2023 are as follows. Additionally, the secretariats of both committees are operated by the Company's HR and legal departments.

- Executive Nomination Committee
  Chairperson: Atsushi Abe (Independent Director)
  Members: Yoshiko Kojo (Independent Director), Masami Yamamoto (Director and Senior Advisor)

- Compensation Committee
  Chairperson: Chiaki Mukai (Independent Director)
  Members: Kenichiro Sasae (Independent Directors), Byron Gill (Independent Directors)

In FY2022, the Executive Nomination Committee met eight times to discuss the election of Representative Directors including the CEO, the nomination of candidates for Director, and the skill matrix of Directors and Auditors, etc. and provided its recommendations to the Board of Directors. The Compensation Committee met six times to discuss the revision of executive compensation details and changes to the process for determining individual compensation, and provided its recommendations to the Board of Directors.

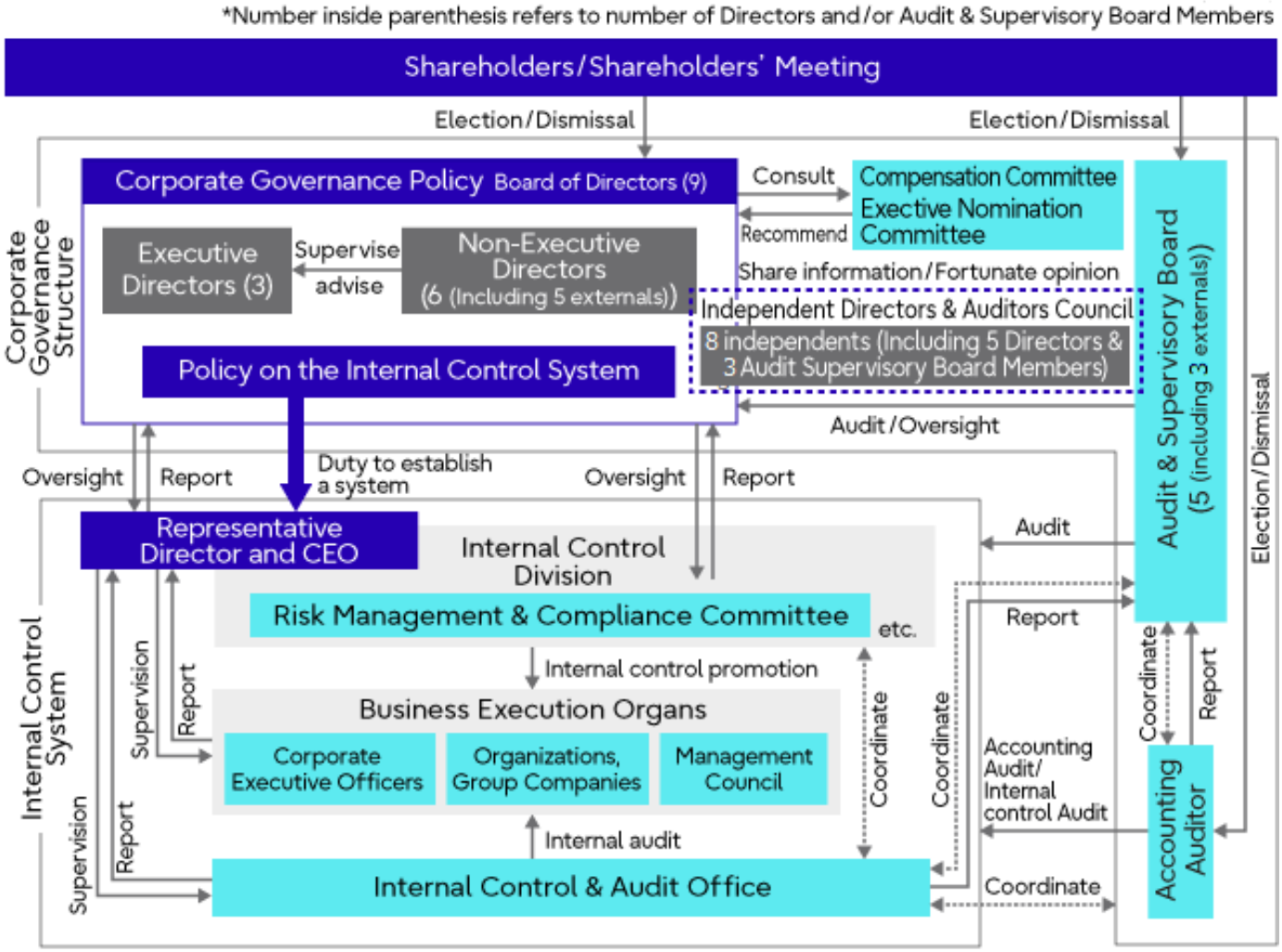
The Executive Nomination Committee discussed CEO succession and mutual evaluations of Non-Executive Directors, and the Compensation Committee discussed the introduction of the stock compensation plan for External Directors.

› Corporate Governance Report

Matters on Functions such as Business Execution, Auditing, Oversight, Nomination and Compensation Decisions (Overview of Current Corporate Governance System)

The diagram below illustrates the Company's corporate governance structure.(As of June 26, 2023)

Corporate Governance Structure



Reasons for Adoption of Current Corporate Governance System

We believe that both direct oversight of business execution by the Non-Executive Directors and 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", which establishes an Audit & Supervisory Board composed of Audit & Supervisory Board Members appointed as independent agents.

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. External Directors also 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 performance by the Non-Executive Directors is enhanced.

Policy for Determining Executive Compensation

Compensation paid to Directors and members of the Audit & Supervisory Board is determined based on the policy on the determination of the details of compensation, etc. for individual Directors established by the Board of Directors, subject to approval by the Compensation Committee.

- Corporate Governance Report

Incentive Policies for Directors (page 19); Policy on Determining Remuneration Amounts and Calculation Methods (Page 21)

Basic Approach to the Internal Control System

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

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

- Matters Subject to Measures for Electronic Provision (Matters Excluded from Paper-based Documents Delivered Upon Request) at the Time of Notice of the 123rd Annual Shareholders' Meeting

Disclosures Relating to Corporate Governance

Board of Directors (as of June 26, 2023)

	Name	Position and Responsibilities	Representation Authority	Independent Director
Business executed	Takahito Tokita	CEO, Chairman of the Risk Management & Compliance Committee	✓	
	Hidenori Furuta	COO	✓	
	Takeshi Isobe	Corporate Executive Officer, SEVP, CFO		
Non-executive	Masami Yamamoto	Senior Advisor		
	Chiaki Mukai			✓
	Atsushi Abe	Chairman of the Board of Directors		✓
	Yoshiko Kojo			✓
	Kenichiro Sasae			✓
	Byron Gill			✓

FY2022 Attendance at Meetings of the Board of Directors or Audit & Supervisory Board

Meeting	Number of Meetings	Attendance Rate
Board of Directors	13	99.1%*
Audit & Supervisory Board	10	100%

* Of the nine members of the Board of Directors, eight attended every meeting, with only Kenichiro Sasae missing one of the 13 meetings.

Skills of directors and auditors

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

Directors (as of June 26, 2023)

	Name	External	Diversity		Skills Matrix				
			Gender	Nationality	Corporate management	Finance and investment	Global	Technology	ESG, academia, and policy
CEO	Takahito Tokita		Male	JP	✓		✓	✓	
COO	Hidenori Furuta		Male	JP	✓		✓	✓	
CFO	Takeshi Isobe		Male	JP	✓	✓	✓		
Senior Advisor	Masami Yamamoto		Male	JP	✓		✓	✓	
Independent Director	Chiaki Mukai	✓	Female	JP			✓	✓	✓
Independent Director	Atsushi Abe	✓	Male	JP		✓	✓	✓	
Independent Director	Yoshiko Kojo	✓	Female	JP			✓		✓
Independent Director	Kenichiro Sasae	✓	Male	JP			✓		✓
Independent Director	Byron Gill	✓	Male	US		✓	✓		

Auditors (as of June 26, 2023)

	Name	External	Diversity		Skills Matrix		
			Gender	Nationality	Legal affairs and compliance	Finance and accounting	Operating process
Full-time Independent Audit & Supervisory Board Member	Youichi Hirose		Male	JP		✓	✓
Full-time Independent Audit & Supervisory Board Member	Megumi Yamamuro		Male	JP	✓	✓	
Independent Audit & Supervisory Board Member	Koji Hatsukawa	✓	Male	JP		✓	✓
Independent Audit & Supervisory Board Member	Hideo Makuta	✓	Male	JP	✓	✓	
Independent Audit & Supervisory Board Member	Catherine O'Connell	✓	Female	NZ	✓		

Among the non-executive directors, Senior Advisor Yamamoto and Director Abe, who have business experience at companies, have expertise in risk management.

Risk Management

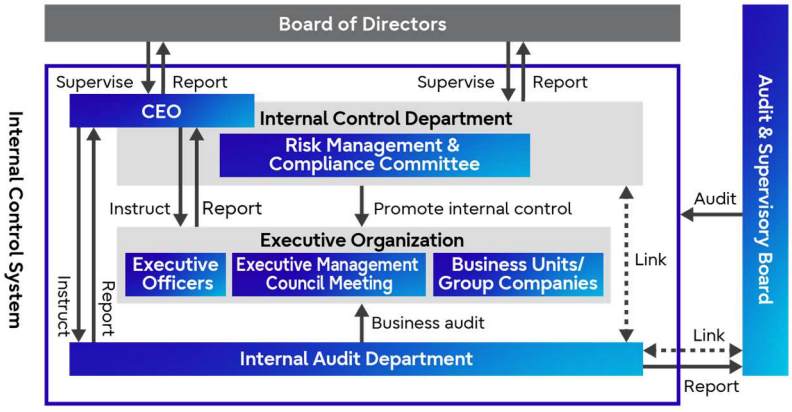
Guidelines & Structure

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

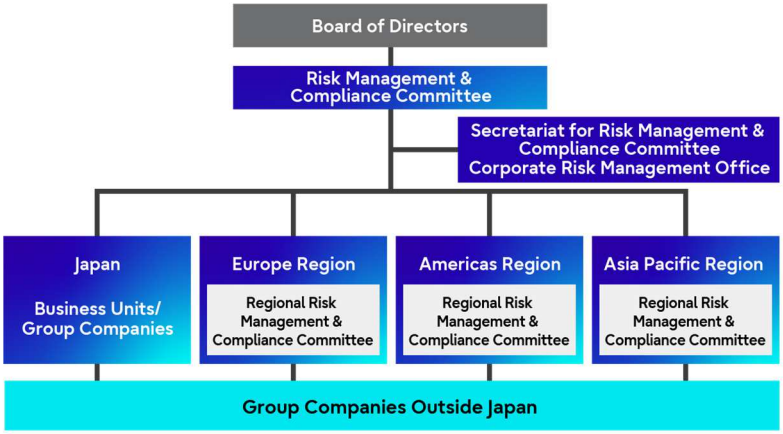
Chaired by the CEO and composed of Board Members, the Risk Management & Compliance Committee continually assesses and verifies risks that could result in losses to the Fujitsu Group and implements risk control measures such as formulating preventive measures for materialized risks in business execution. To minimize losses arising from the materialization of risks, and in an effort to prevent their recurrence, the Committee regularly analyzes the risks that have materialized and reports to the Board of Directors.

In addition, the Risk Management & Compliance Committee has established a Regional Risk Management & Compliance Committee in each region outside of Japan to operate as subordinate committees in a global structure. The committee also assigns Risk Management & Compliance Officers to the business units, group companies and regions for both Japan and overseas. These organizations collaborate to build a risk management and compliance structure for the entire group.

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



Risk Management & Compliance Structure



Furthermore, to strengthen the risk management functions of the Fujitsu Group, we created the Corporate Risk Management Office, which reports directly to the CEO and is independent of the business units. This body carries out the secretariat functions of the Risk Management & Compliance Committee and, under the leadership of the Chief Risk Management Officer (CRMO), is responsible for interpreting risk-related information and spearheading rapid, appropriate responses where required.

Based on the initiatives taken to date, we have appointed a Chief Quality Officer (CQO) as the person responsible for quality for the entire Group, as we believe that Company-wide and cross-organizational measures led by top management are more essential than ever to further strengthen measures and ensure effectiveness. Furthermore, we have enhanced the structure and functions of our Risk Management & Compliance Committee, chaired by the CEO, and have strengthened this framework to ensure constant and thorough Company-wide responses.

Specifically, the CQO will be included as a member of this committee, which has been the venue for deliberations on important risk compliance issues related to the Fujitsu Group. This framework was established in which concrete measures are determined and promptly implemented, including Company-wide measures related to information security and system quality, as well as responses to individual events. By establishing such a framework, we could thoroughly implement risk management led by the CEO, assigning more strengthened authority than ever to the CISO and CQO to supervise the process, including different CxO areas such as personnel systems and investment resources. Additionally, to ensure the rapid and effective implementation of measures, the committee is held every month.

Main Business Risks *

- Economic and financial market trends
- Customers
- Competitors and the industry
- Investment decisions and business restructuring
- Suppliers, alliances, etc.
- Public regulations, public policy and tax matters
- Natural disasters and unforeseen incidents
- Finance
- Deficiencies or flaws in products and services
- Compliance issues (including human rights risks)
- Intellectual property
- Security
- Human resources
- Fujitsu Group facilities and systems
- Environment and climate change

* 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"

Processes

After identifying and reviewing the key risks associated with business activities from among the various risks around the Fujitsu Group's operations, every year we investigate, analyze, assess, and visualize the possibility of key risks occurring, the potential impact, the status of measures, and so on.

Based on the assessment outcomes, the Risk Management & Compliance Committee confirms the key risks, issues instructions on further measures, and reports to the Board of Directors. The policies and measures determined by the committee are fed back to the entire Group, and the risk management departments established for each key risk then appropriately manage the measures across the Group as part of efforts to minimize risks.

Information obtained through the potential risk management process is disclosed to stakeholders via such documents as securities reports and the Fujitsu Group Sustainability Data Book.

In addition, when a risk materializes, the committee has established mandatory rules such as rapid escalation to the Risk Management & Compliance Committee in accordance with risk management regulations, and ensures that all employees are aware of these regulations to raise awareness of risk management.

By implementing such process and confirming by the risk management department on a quarterly basis, we aim to reduce risks across the Fujitsu Group and to minimize the impact when risks become apparent.

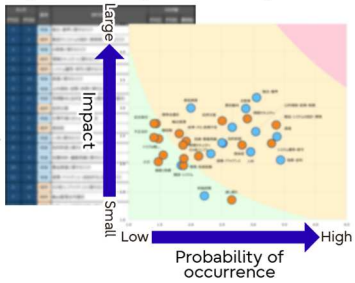
Risk Management Process

Visualization of Key Risks

Key Risk Assessment Sheet

No.	Risk Category	Impact	Probability
1	Economic trends		
2	Customer trends		
3	Competition/ Industry trends		
4	Information security		
5	Compliance		
⋮			
32	Environment/ Climate change		

Key Risk Ranking Table and Map



Risk Management Education

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.

Refer to the "FY2022 Performance" section for information on education outcomes for FY2022.

Group-Wide Disaster Management

The basic policy of Fujitsu and its group companies in Japan is to ensure the safety of staff and facilities when disasters occur, to minimize harm and to prevent secondary disasters. We also aim to ensure that business operations resume quickly, and that we can assist in disaster recovery for our customers and suppliers. To this end, we are building robust collaborative structures in our internal organizations and strengthening our business continuity capabilities.

In particular, we are working to build "area-based disaster management systems" that enable the Group offices in each region to cooperate effectively and to promote responses via the management structures in each business unit and group company.

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 even individuals. 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 FY2022 refer to the "FY2022 Performance" section.

- Group-wide disaster management, joint disaster response drills, verification activities

Business Continuity Management

Recent years have seen a significant increase in the risk of unforeseen events that threaten continued economic and social activity. Such events include earthquakes, floods and other large-scale natural disasters, disruptive incidents or accidents, and pandemics involving infectious diseases. To ensure that Fujitsu and its group companies in 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.

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

For more information on our BCM activities, infectious disease countermeasures and BCM in our supply chain, please refer to the PDF listed below, and for activity outcomes for FY2022 refer to the "FY2022 Performance" section.

- BCM activities, infectious disease countermeasures, supply chain BCM

FY2022 Performance

Risk Management Education

- **Fujitsu Group new executive training: 26 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.

- **Fujitsu Group new manager training: 1,257 people**

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

- **Disaster Management Forum: 450 people**

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

Serious Incident Response Training

- **Information security incident response training: 70 people**

  By training through implementing and verifying a series of flows relating to initial responses to an information security incident, we aim to accelerate our incident response capability.

- **Product and service problem response training: 95 people**

  We assess the impact of product and service problems and conduct simulated responses with external parties. This includes confirming and verifying the collaboration process between organizations, identifying issues, and undertaking continuous improvements.

Disaster Management & BCM Training

Joint disaster response drills: The FY2022 theme for Japan's annual nationwide disaster response drills that incorporate mock disaster exercises was the "Nankai Trough Megathrust Earthquake". These drills are used to ensure and to verify that Fujitsu and its group companies in Japan are fully versed in the essentials of dealing collaboratively with major disasters. (Proposed scenarios include "Tokyo Inland Earthquake" and "Nankai Trough Megathrust Earthquake".)

Information Security

Policy

Fujitsu Group appointed dedicated Chief Information Security Officer (CISO) in October 2021. Under the new information security regime, we are striving to secure and improve information security for our customers through our products and services, while also ensuring the information security of the entire Fujitsu Group.

Management Structure

We have established Regional CISOs in Japan and three international regions (Americas, Europe and Asia Pacific) under the CISO to implement globally consistent security policies and measures. They align the headquarters' policies with security requirements specific to each country to bolster information security through our globally integrated system.

We have also been building a system to strengthen the CISO's control over relevant departments to achieve the ideal state of information security by assigning security managers in charge of autonomous information security enhancement of each department in Fujitsu Headquarters and its group companies inside and outside Japan.

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

Information Security Management System Run by CISO and Information Security Managers

Information Security Initiatives

Our Goals for Information Security

With the rapid increase in more skillful and more sophisticated cyber-attacks, enhancing information security has become an urgent issue for national economic security and for corporate economic activities.

We have set up our goals for information security as described below. To achieve them, we respond to cyber-attacks with ever-evolving advanced information security and by continuing to reform the awareness of each employee and our organizational culture as it is the key to success. Together with relevant departments and employees, we are developing processes, rules, and systems to promote cybersecurity and working to strengthen information security for the entire Fujitsu Group as well as a safer business environment for our customers and partners.

Our Goals for Information Security

- **Proactive information security**
  - Continuous evolution of information security to support diverse work styles in the age of digital transformation (DX)
  - Autonomous information security response by employees and organizations
- **Defensive information security**
  - Cyber-attack prevention by addressing vulnerability
  - Enhanced monitoring to minimize cyber risks in case of emergency

Initiatives

Cross-departmental Application of Recurrence Prevention Measures and Visualization of Security Risks

In response to information security incidents involving our project information sharing tool, "Project WEB" and cloud service, "FJcloud-V/NIFCLOUD", we have been applying recurrence prevention measures across different departments under the dedicated CISOs' system. By 2022 we had completed the application of one of the principal recurrent prevention measures, "multi-factor authentication of web systems" in Japan. We also continue to promote corrective measures by visualizing security risks through company-wide security inspections.

In 2023, we will continue our efforts to achieve our goals for information security by taking appropriate corrective measures through visualization of security risks and evolving information security based on the following major themes:

What Visualization of Security Risks Can Achieve

- **Autonomous risk control by internal relevant departments**
  Objectively visualized risks related to information management and information system security are reviewed and promptly addressed by relevant department within the company. In case of critical system or information, an organization under the direct control of CISOs conducts direct inspection to objectively confirm the risk content with more accuracy.
  Moreover, the information management literacy of each employee and the organization (internal factors) and the actual status of cyber-risks (external factors) are also visualized and shared (Visual control). Having each employee understand this and take this personally (developing a sense of ownership) fosters an organizational culture of autonomous information security measures (taking initiatives).
- **Accurate correction of digitally visualized risks**
  Introduction of CMDB (*1) and Information Management Dashboards (*2) allows digital visualization of information system vulnerability and information management deficiencies. Correcting the visualized risks mechanically, not manually, minimizes security risks accurately and speedily.

(*1) CMDB：Configuration Management Database
CMBD is a database that automatically collects and centrally manages information systems' configuration information of hardware, software, network, etc.
The collected information is utilized for security inspections and audits, handling vulnerability, and responding to security incidents.

(*2) Information Management Dashboard: digitalized information management register.
The Fujitsu Group maintains a digitalized information management register, which controls managers, management locations, and scope of sharing of the confidential information.
Any deficiencies detected through consistency checks between the Dashboard and the actual information management status

(such as audit logs of storage services) will be readily and quickly corrected through a trouble ticketing system, or set a workflow for the solution.

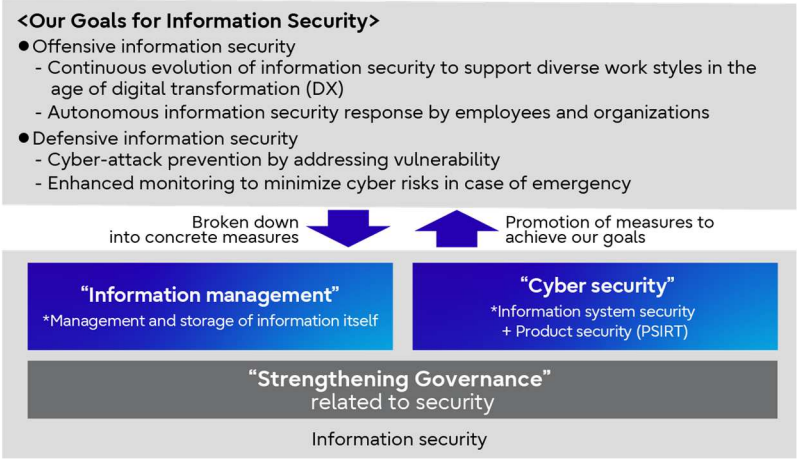
- **Evolution of information security with technology**
  From 2023, we will unify our authentication infrastructure to promote centralized and visualized management of user IDs, authorization information and trail logs.
  With this authentication infrastructure, we will seek to conduct behavior analysis using trail logs and optimize authorization information in conjunction with the analysis results.

Main Measures

We will introduce the main measures tied to each theme from the following three perspectives.

- **Cyber-security**
  Introduction of information system security (or ensuring and maintaining the safety and reliability of information systems and networks), as well as measures related to activities to maintain the security of our products and service
- **Information management**
  Introduction of measures to maintain and manage the confidentiality, integrity and availability of information itself, including critical information (confidential or personal information)
- **Governance enhancement**
  Introduction of measures to strengthen governance to instill and establish security measures and enhance the security of the entire organization.

Overall Picture of the Goals and Security Measures



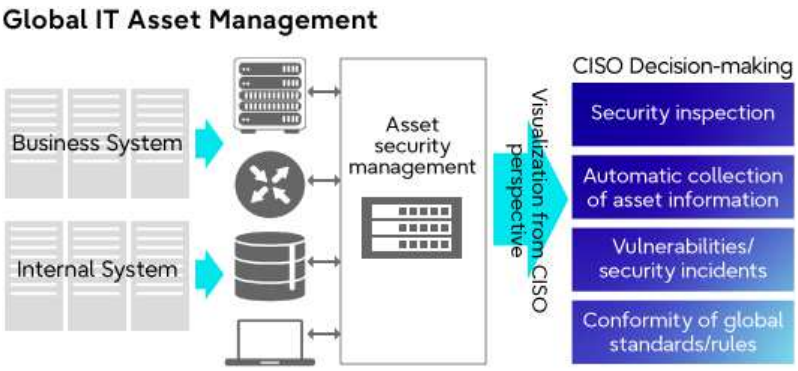
Cyber Security

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

Measures Linked to Centralized IT Asset Management

Autonomous Correction Through Centralized and Visualized IT Asset Management

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



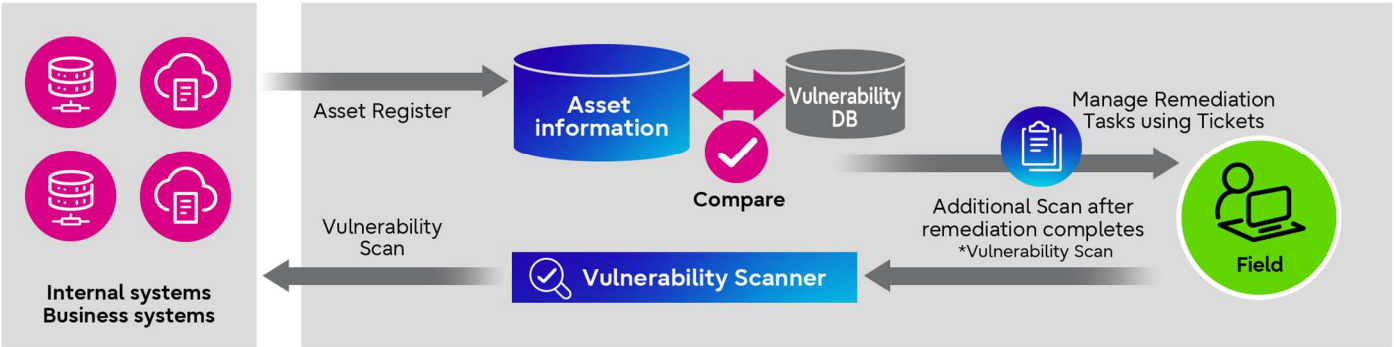
Vulnerability Scanning of Systems Exposed to The Internet

We provide vulnerability scanning mechanism in systems exposed to the Internet from the outside based on IT asset management information. This enables our relevant departments managing those systems to conduct autonomous periodic scans and take corrective actions triggered by vulnerability detection. By conducting periodic inspections through this mechanism on annual basis, we ensure implementation of countermeasures against vulnerabilities. Moreover, we inspect critical systems with more accuracy through third-party audits conducted by an organization under the direct control of the CISOs. In 2023, we will promote the automation and mechanization of this process.
Furthermore, we have also established a mechanism to ensure that vulnerabilities of systems not exposed on the Internet are thoroughly addressed, by regularly updating IT asset management information, checking it against the vulnerability database, and, in case of any critical vulnerability, issuing tickets (corrective tasks) to responsible department.

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 vulnerability as well as vulnerability information in Fujitsu Group's systems exposed to the Internet. The obtained threat intelligence allows impact analysis and prompt corrective 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.

Vulnerability Scanning of Internet-exposed Systems



Thorough Monitoring

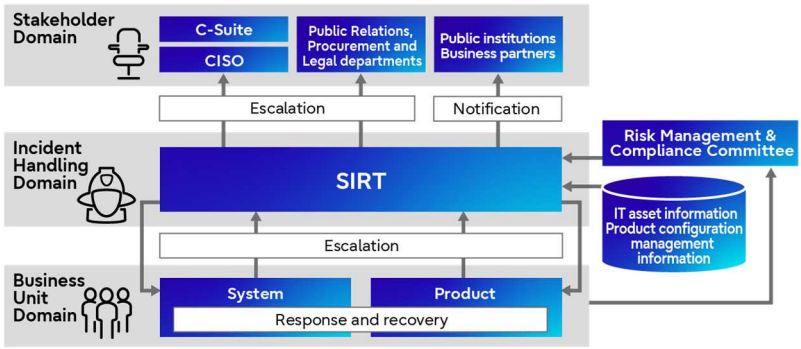
The cyber security environment is constantly changing, and attack methods are becoming more complex and sophisticated. Under these circumstances, the Fujitsu Group takes a zero-trust approach, based on the concept that 100% prevention of intrusion by cyber-attack is impossible, to reinforce security monitoring. We will improve the internal guidelines for security monitoring and conduct periodic system inspections to grasp and visualize the current situation. We will also work to ensure a sound monitoring system to enhance detection capabilities and earlier response to cyber-attacks. Furthermore, we ensure that critical systems are thoroughly monitored through third-party inspections conducted by an organization under the direct control of the CISOs.

Response to Incidents

As a company that supports customers' safe and secure business activities, we must respond immediately to cyber-attacks that are becoming increasingly skillful and sophisticated. To that end, we have created an incident response process on the premise that a contingency is inevitable, so that in such cases our organization can quickly implement the series of processes of escalation to higher levels, response, recovery, and notification.

1. **Escalation process**
   We have standardized, and are continuously improving, the process of calculating an impact of each incident risk and escalating accordingly, to bolster the organization's ability to respond to any incident.
2. **Incident response and system recovery process**
   After receiving information on attacks and vulnerabilities, we will take actions for prompt recovery by formulating a system recovery plan that includes appropriate incident handling, patch application plan and business continuity plan (BCP) for the affected product or system.
3. **Notification process**
   To ensure accountability to our stakeholders, we strive to properly share and report incident information.
4. **Activities to have the processes take root in the organization**
   The Fujitsu Group conducts regular education and training on incident response to raise employees' awareness and implement activities for the incident response processes to take root.

Incident Response Processes



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. In our company, technical experts and members who take the lead on the path to the solution work together to handle security incidents, following various processes, including the escalation process.
In addition, we have been accumulating information on attacker's tools, processes, and access methods and improving technical knowledge and skills of our response team members through continuous training. We also review the incidents we, including our global group companies, have handled to continuously improve our response capabilities, including upgrading our structure, rule and processes and accumulating know-how, so that we can speed up our response and minimize the impact.

Risk Prevention in Our Products and Services

PSIRT Manager System

To protect our customers who use our products and services, we have assigned PSIRT Managers in internal relevant departments to be responsible for centralized management of information on product configuration, IT asset and threat intelligence, including vulnerability information, as well as for vulnerability response. This is a system that enables speedy and proactive response to risks caused by vulnerabilities in our products and services.

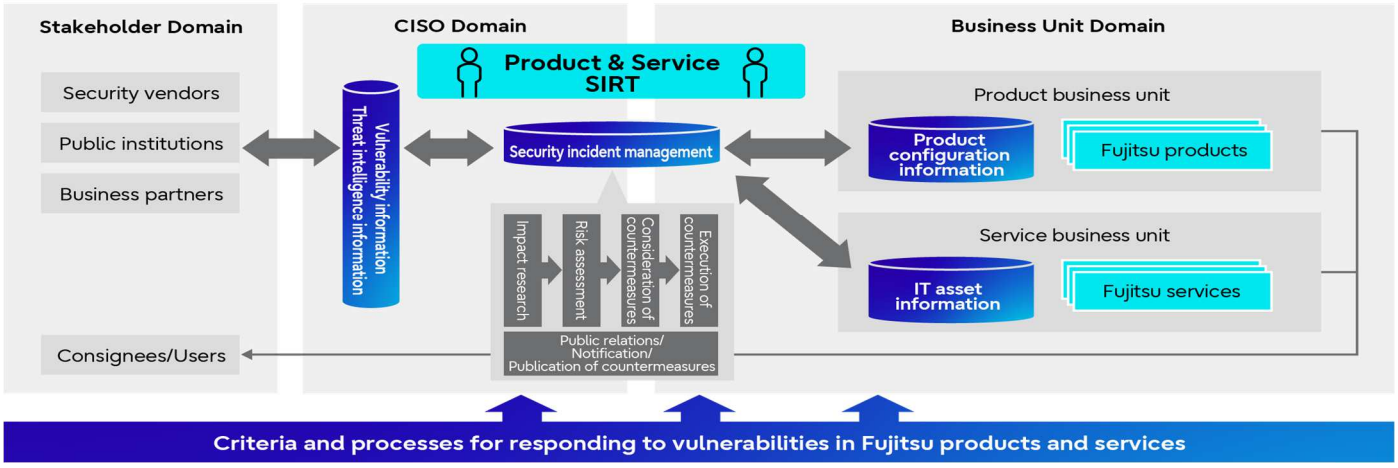
Formulation of Processes

To accelerate estimation of the risks to products and services, as well as consideration and execution of countermeasures against them, we created standards and processes to handle the risks caused by

vulnerabilities. We are continuously improving those processes based on statistical analysis by data scientists and track record of our responses.

Earlier problem resolution through prompt vulnerability response based on these systems and processes will prevent secondary damage to customers and minimize the impact on their business continuity.

Vulnerability Response Framework in Fujitsu Products and Services



Information Management

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

Furthermore, we provide various automation support tools that utilize information management dashboards to support appropriate information management. We make improvements as necessary to realize operations that are both effective and safe.

Information Protection Management Systems (7 Points)

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 information through a global network that is centered on the CISO and overseen by the CEO. We appoint management staff for each department, clarify roles, and promote the appropriate handling of information.

(2) Policies & Regulations

In order to handle information correctly, we have formulated necessary rules, procedures, and an annual activity plan. We also periodically review our policies and rules, including responding to legal amendments.

(3) Training & Awareness

In order to improve the awareness and skills of each employee, we provide necessary information according to employees' positions and roles. We also hold various training sessions and disseminate information in response

to changes in the work environment (for example, telecommuting, etc.).
Every year, we carry out information management education (e-Learning) for all employees including executives, and publish internal information management learning materials that can be studied at any time.
*Number of participants in 2022: 37,343

(4) Self-Inspection

We identify and classify our information assets, conduct risk analysis, and carry out periodic inventory check.

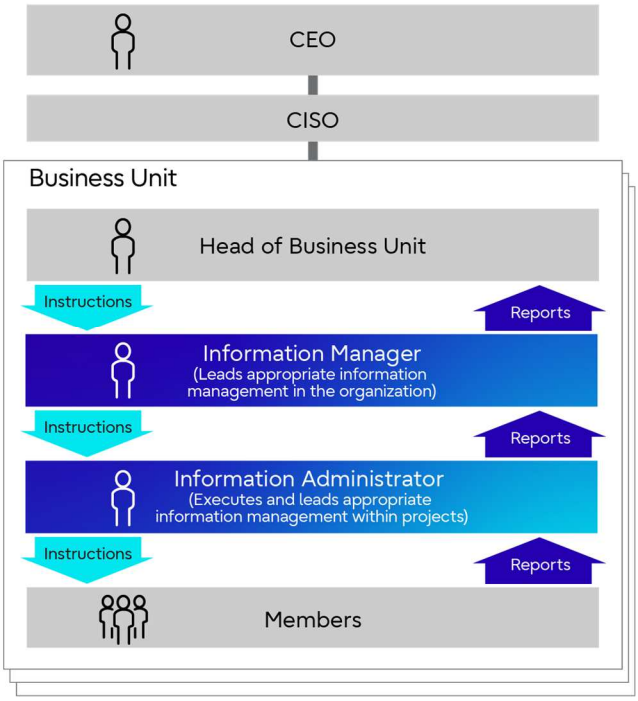
(5) Incident Response

We have established a system for fast and appropriate response to information management incidents. We have also set up escalation routes, procedures, etc., on a global scale.

(6) Audit

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

Information Protection Management System and Roles



(7) Review

We are working to improve and review our Information Protection Management System by considering external opinions (including audit results, incidents, and complaints), law revisions, and changes in the environment.

Protection of Personal Information

Fujitsu has established a global Personal Information Protection System to strengthen the protection of personal data. Under the leadership of the organization under the direct control of the CISOs 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 (*1). In regard to the handling of personal information, we post and announce privacy policies on public sites in each country.

(*1) 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), the obligation to report within 72 hours of a data leakage, etc.

In Japan, with the objective of protecting personal information, Fujitsu Group obtained certification for the PrivacyMark (*2) by the Japan Information Processing and Development Center (JIPDEC) in August 2007. We are continually working to strengthen our Personal Information Protection System. Our domestic Group companies also obtain the PrivacyMark as necessary and work to thoroughly manage personal information.

(*2) The PrivacyMark
The PrivacyMark is granted to businesses that handle personal information appropriately under a personal information protection management system that is in compliance with JIS Q 15001:2017.

In FY2022, Fujitsu Customer Service Center Personal Information Protection Desk did not receive any consultations or complaints regarding customers' privacy. No customer information was provided to government or administrative agencies in accordance with the Act on the Protection of Personal Information.

Acquisition of Information System Certification

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

- Third-party evaluation/certification audit results (link)

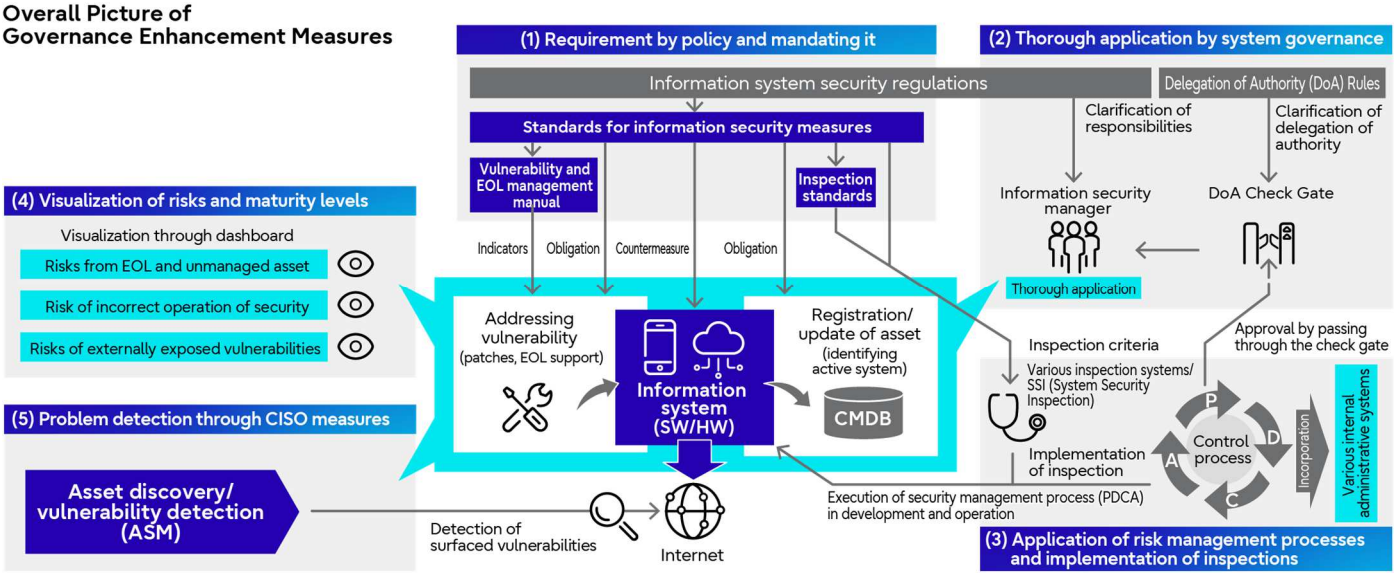
Governance Enhancement

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

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

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

Overall Picture of Governance Enhancement Measures

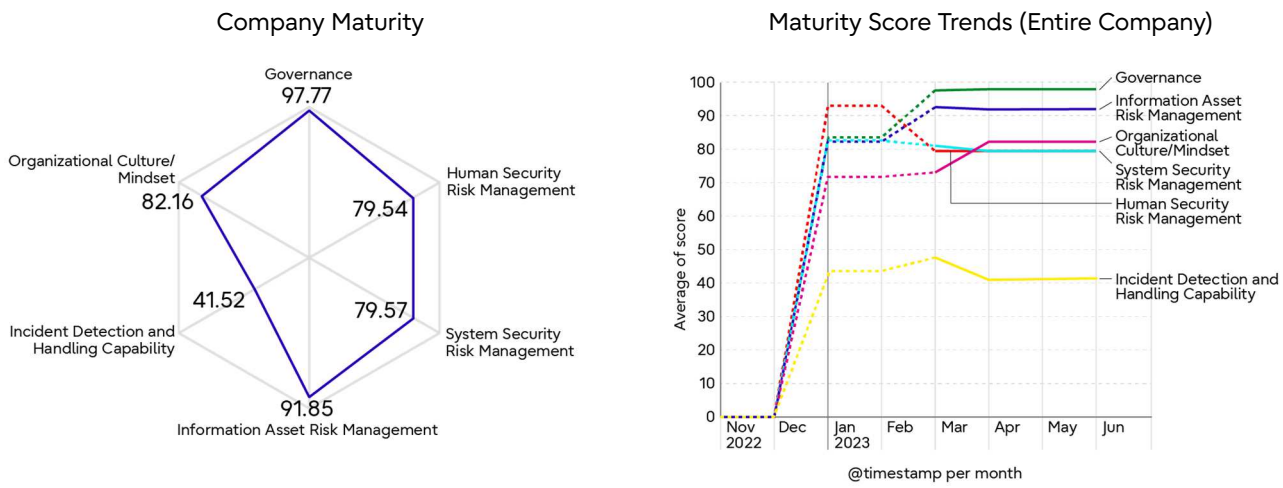


Metering of Security Maturity Levels

Fujitsu evaluates the security maturity levels of organizations by automatically collecting and scoring infrastructure configuration values, security logs, audit data and other data. By visualizing the maturity level of each department at Fujitsu Headquarters and each group company on a monthly basis, we foster a culture of autonomous implementation of specific measures and corrective actions based on an understanding of the current situation and differences from targets, and thus promote self-purification effects of cyber security measures in each department.

Inspired by the C2M2 (*1), or Cybersecurity Capability Maturity Model, and SIM3 (*2), or Security Incident Management Maturity Model, both of which have been proven in Japan and overseas, our security maturity level evaluation indicators incorporate a unique method of scoring maturity mechanically from data taken from security measures. The evaluation score is capped at 100 points. 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 2023, we will conduct 8-axis evaluation, adding external organizational collaboration and supply chain risk management.

(*1) C2M2：Cybersecurity Capability Maturity Model
(*2) SIM3：Security Incident Management Maturity Model



Visualized Graph of Security Maturity Levels (sample)

Dissemination and Spread of Framework Rule Process

We are implementing mainly two initiatives to unify and raise the level of security measures on a global basis.

Fujitsu Group Standards for Information Security Measures

The first is the formulation of "Fujitsu Group Standards for Information Security Measures" which set the standard security measures in the group. Consisting of more than 200 management measures based on the global standards NIST's CSF (*1), SP800-53 (*2) and ISO/IEC27002, it will establish rules for the application of management measures according to the importance of information systems and other factors. We are also preparing materials such as manuals and guidelines to support the application of such management measures.

Risk Management Framework

The second is the development of "Risk Management Framework," a framework for security risk management in the group. Based on the global standards NIST's SP800-37 (*3), the framework will establish a set of processes to identify and manage security risks of each organization and information system in a systematic and appropriate manner. It will establish rules for periodic risk management in each organization and risk management in the development and operation phases of each information system. We will incorporate these processes into the Fujitsu Group's various business processes to ensure that they are well understood and widely accepted.

By sharing these two initiatives within the Fujitsu Group and executing a series of processes of "Risk Management Framework," we will apply management measures based on the "Fujitsu Group Standards for Information Security Measures" to each organization and information system, while we will run a continuous improvement process. This will help us with our pursuit for effective implementation of security measures and realization of "security by design."

(*1) CSF：Cybersecurity Framework
(*2) SP800-53：NIST SP800-53 Rev.2 Security and Privacy Controls for Information Systems and Organizations
(*3) SP800-37：NIST SP800-37 Rev.2 Risk Management Framework

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

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

In addition, we hope that regular information sharing by the CISOs and an organization under their direct control within the company, as well as vitalization of security managers' community, will contribute to creating a

corporate culture that does not allow information management and security measures to take a backseat to business convenience and cost reduction. To achieve this goal, we are working on the following:

<Security Education and Training>

In addition to basic education on information management and cyber-security, we thoroughly disseminate the lessons learned from the latest trends and incident responses. We also work to improve the skills of our professional personnel by issuing guidelines on system monitoring for system managers. As 100% prevention of incidents is difficult, we have changed from efforts not to allow contingencies to happen, to efforts that take contingencies into consideration. As a part of such efforts, we conduct incident response training for employees. For instance, we annually provide system engineers (SEs) and business producers involved in business and internal operations with practical training under a scenario of an incident. In the event of an incident with a social impact, we also conduct incident training for executives and relevant departments to ensure a quick response and minimization of the impact.
In addition, we carried out targeted e-mail drills twice in the FY2022 to promote the security mindset in each employee. We will continue this drill at least once a year.

<Strengthening the Security Management Structure and Human Resource Development>

Fujitsu Group will work to reform each department's security-related way of thinking and behavior by having the CISO and an organization under their direct control periodically share information within the company, assigning security managers to support each department, and stimulating their community.
In 2023, we redefined the image of security personnel, especially that of security managers working in the field. We also reviewed our professional certification system. After clarifying their functions and responsibilities, we revised the system, including the compensation system, and have been reinforcing the security system in organizations in the field of Japan ahead of schedule since January 2023.
We also strive to better the security maturity level of each department lacking security-related experience by sharing with it their actual status visualized through the above-mentioned "metering of security maturity levels" and by having the security managers' community communicating with it periodically.

Quality Initiatives

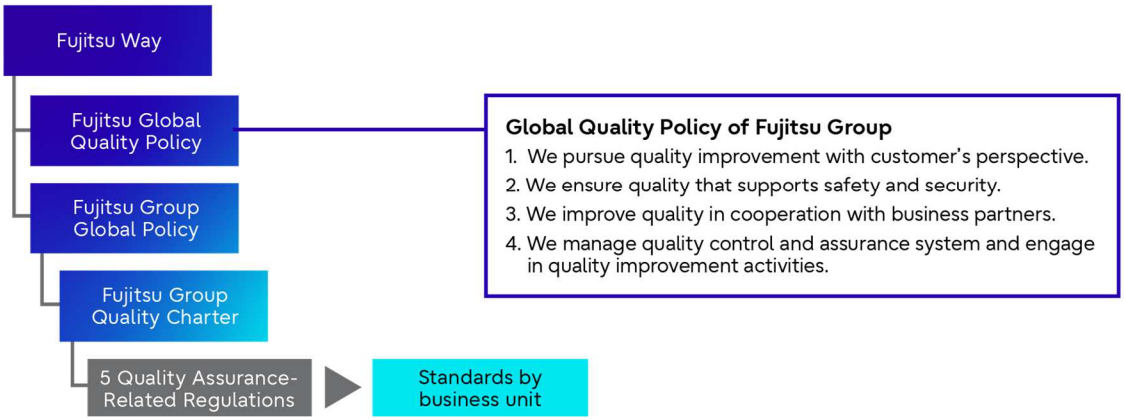
Quality Policy

In addition to establishing a corporate philosophy and charter that applies to all products/services, the Fujitsu Group has also established regulations and standards to uphold customer requests, various features of our products/services, and laws and restrictions. These are all based on the Fujitsu Way. As a result, each of the Fujitsu Group's businesses provides safe and secure products/services supporting the businesses and lifestyles of various customers including developing social infrastructure.

The Fujitsu Global Quality Policy represents a way of thinking, shared across the entire Group, for implementing a value system which holds the Fujitsu Way in high regard, "Trust: We contribute to a trusted society using technology."

This quality policy was established in order to continue providing our customers with products/services that they can feel secure using, but also to define quality as a foundational part of our business, and come to a shared understanding of the policy worldwide.

System of Quality Policy Rules and Regulations



Fujitsu has established the Fujitsu Group Quality Charter under the Fujitsu Group Global Policy, as well as five quality assurance-related regulations (such as Shipment, Registration, and Release Regulations, as well as Safety Promotion Regulations), in order to implement the Fujitsu Global Quality Policy in Japan.

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

Implementation Policy for the Safety of Our Products and Services

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

1. Observation of laws and regulations

   We observe laws and regulations concerning product and service safety.
2. Efforts to secure safety

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

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

4. Collection of incident information, etc.

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

5. Handling of incidents

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

Our Quality Management Structure

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

Furthermore, Fujitsu established Quality Management Representatives in each business organization, region and Group company to monitor Groupwide quality management under the leadership of the CQO. Following the decision-making of the CQO, the Global Quality Management & Assurance Unit formulates shared policies, standardization, and quality improvement measures as the headquarters of quality. By deploying these shared measures through Quality Management Representatives, we are working toward providing products/services with consistent and optimal quality for our customers all over the world.

In addition to working with individual divisions and regions with regards to their quality assurance efforts, we also coordinate across the entire Group to share knowledge and information that transcend organizational boundaries. This helps us make better use of these efforts, and allows us to solve quality assurance issues that are shared across organizations.

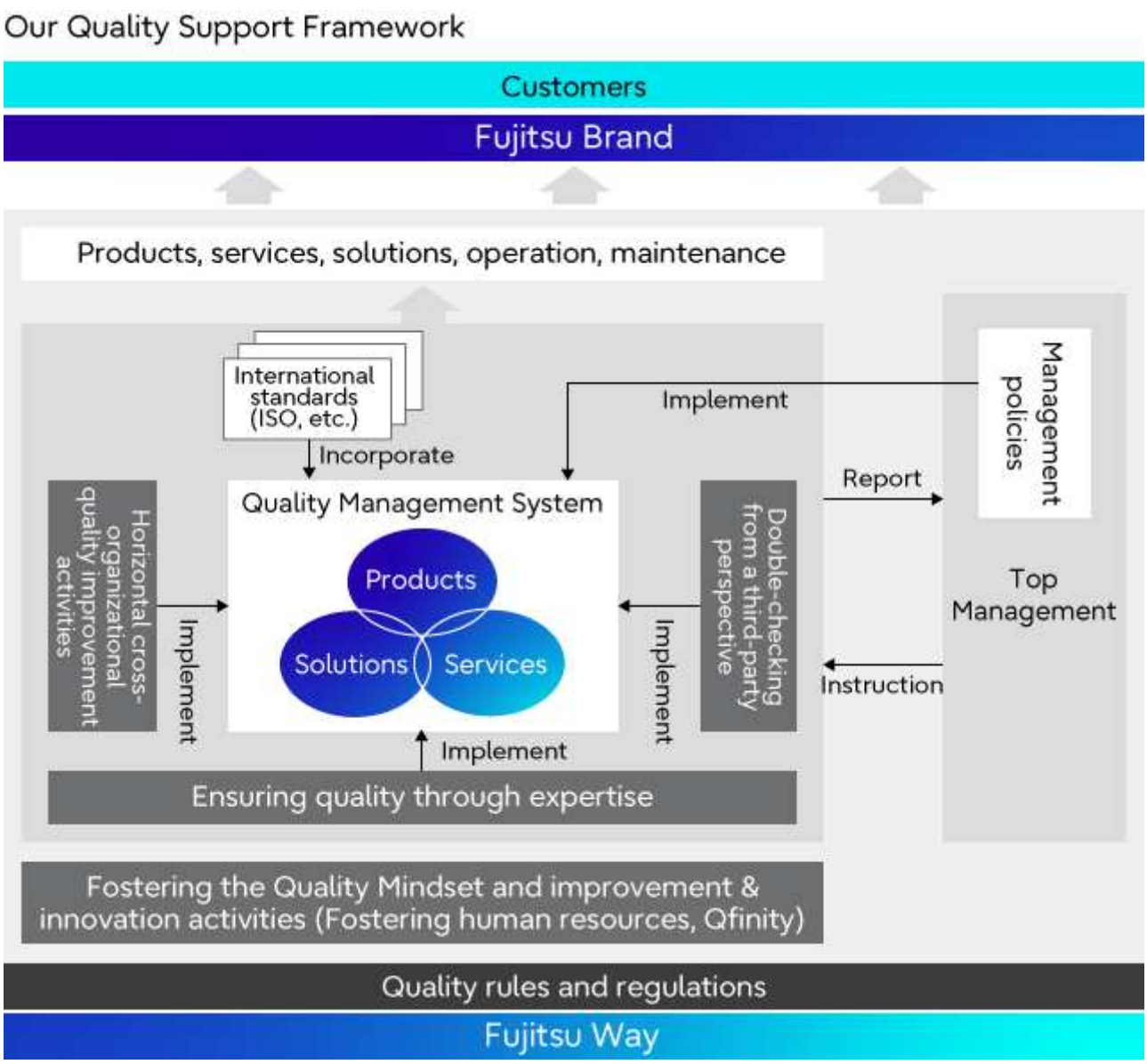
This sharing of effective quality assurance efforts increases the overall quality of Fujitsu's products/services, and helps to prevent issues from occurring and reoccurring.

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.



Companywide Quality Improvement Cycle

Within the Fujitsu Group, each organization has established and operates its own quality management system, and by implementing a cycle spanning from the formulation of shared policies and measures to evaluation and decision making, we are working to improve quality strategically involving the entire Group.

(1) Policies and measures

Objectives are set and reviewed, and quality measures for achieving them are planned and rolled out across the entire Fujitsu Group. In addition to internal control using regulations and rules, quality processes are also standardized to ensure a stable quality.

Companywide Quality Improvement Cycle

(2) Implementation and monitoring

The projects of each business are monitored to ensure that business is executed following quality measures, rules and standardized processes. In case a quality concern arises, the situation is rectified or improved through audits and inspections. Additionally, training is provided to continuously increase employee skill levels.

(3) Response to issues

If a problem related to product/service quality is found, the matter is managed as a quality incident and prompt action/measures are taken. In the case of a serious quality incident, following the Risk Management Regulations, the matter is immediately reported from the field to the Risk Management & Compliance Committee at the Fujitsu headquarters, and under the committee's instructions, the relevant departments address the incident jointly and consider ways to prevent recurrence. The recurrence prevention measures are shared with other departments through Quality Management Representatives in an effort to prevent the same incident from occurring at other Fujitsu Group companies.

(4) Evaluation and reporting

Our approach to quality is regularly examined and analyzed, with consideration also made toward additional measures if necessary. After reporting updates to executive management on a regular basis, action is taken following their decision making and instructions. This cycle is then repeated following a short timeline in an effort to improve quality through an all-hands-on-deck approach including executive management and the heads of business organizations.

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 and engage in quality improvement of products and services.

Quality Governance

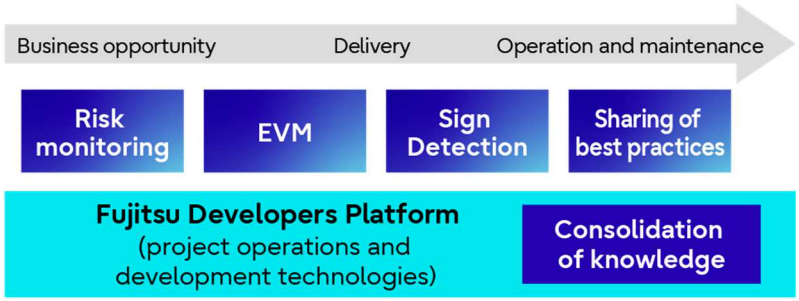
Under the newly appointed CQO, we are working to strengthen quality governance across the entire Fujitsu Group as well as prevent major incidents from reoccurring and enhancing the quality of products/services.

The process of strengthening quality governance involves rolling out a platform for risk assessment and decision-making model within the Fujitsu Group to correctly assess risks and take thorough action against it.

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

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

Mechanism for Objectively Assessing Field Decision



Decision-Making Model

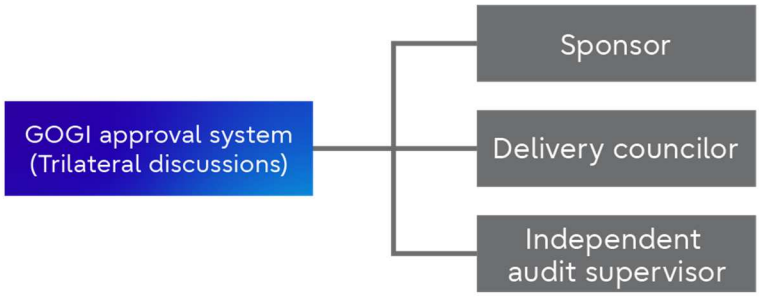
For business opportunity and projects, we have adopted a GOGI approval system (consensus to approve) led by stakeholders. In addition to the conventional judgment of business groups/regions (sponsor), the development departments (delivery councilor) and the Global Quality Management & Assurance Unit (Independent audit supervisor) deliberate from multiple perspectives. Through these trilateral discussions, decisions are made from multiple angles, not only business but also quality, technology, and resources.

We strive to provide better proposals to our customers by setting up check gates for each phase of business opportunity and development, and making decisions through trilateral consensus to prevent the promotion of erroneous projects and the occurrence of quality issues.

As connectivity increases globally, the expectations placed on the Fujitsu Group are also undergoing significant changes.

As we take on an increasing number of first-time business and initiatives, we utilize these mechanisms as a foundation to make quick and accurate decisions and prepare for various risks.

Consensus-based Decision-making Model



FY 2022 Performance

Violation of Laws and Regulations Concerning Product Safety

- Violation of laws and regulations concerning product safety: 0

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.

We also established a consultation service to provide support for customers' applications.

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

- Product information and labeling violations: 0
- Product defect involving violation of Japan's Radio Act: 1
- Defect in violation of the EU Electromagnetic Compatibility Directive: 1

ISO9001 / ISO20000 Certification Status

Fujitsu is continuously working to improve processes under the QMS.

- ISO9001: 22 divisions certified
- ISO20000: 9 divisions certified

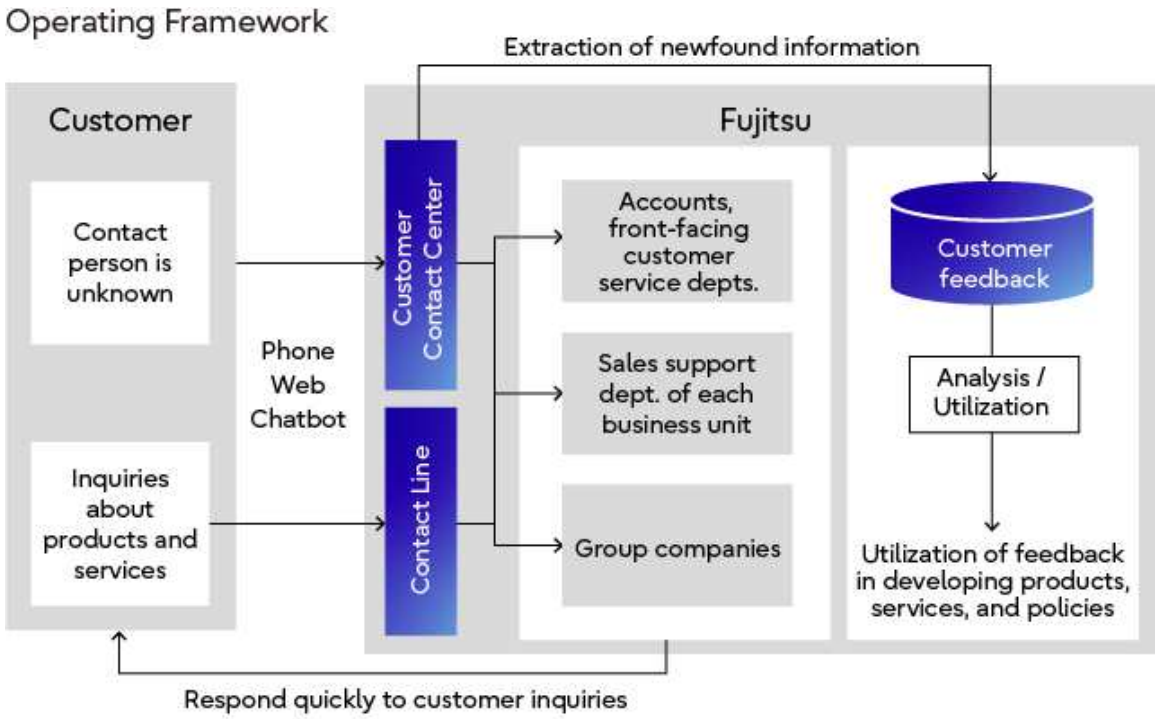
Working With Our Customers

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 roughly 40,000 annual 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 text only)

Advertising and Promotion Policy

At Fujitsu, we work to make sure that our advertising makes use of fair and appropriate language and symbols, and are in adherence to laws and internal regulations. In FY 2023, we will engender the trust of society through innovation, and promote our initiatives to make the world a more sustainable place, so that those efforts will be more widely recognized. We also set goals (KPIs) and monitor these indices via the PDCA cycle to see if they

have been achieved, in order to determine whether our advertising policies have been effective and cost-effective.

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

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

- Advertising and Promotion (Japanese text only)

