

Governance

Promoting responsible business operations and sustainable value creation through management based on high ethical standards, transparency and integrity, supported by effective corporate governance and risk management.

Corporate Governance	251
Compliance	261
Supply Chain	273
Risk Management	282
Information Security	289
Quality Initiatives	304

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 29, 2026)

＜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 29, 2026, the Board of Directors is comprised of 9 members in total: 3 Executive Directors and 6 Non-Executive Directors (including 6 Independent Directors).

In FY2025, the Company held 13 Board of Directors meetings (including one extraordinary meeting) 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) outlook of the final fiscal year of the current Medium-Term Management Plan; 2) future growth strategy; 3) technology strategy; 4) non-financial indicators, human resource development; and 5) internal control and risk management. The Board held 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

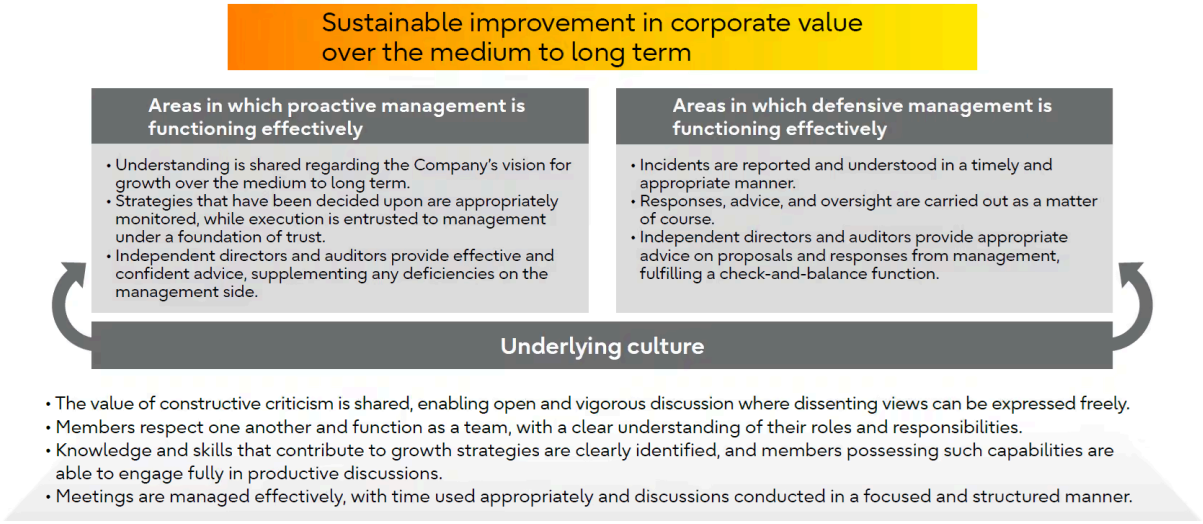
execution status of its tasks and the actions taken regarding individual risks that materialized in FY2025. The Board continued implementing oversight based on these reports.
The Company carries out an evaluation of the effectiveness of the Board of Directors every year to improve corporate value by raising the Board's effectiveness.

Summary of the results of analysis and evaluation for effectiveness of Board of Directors as a whole
It is stipulated in the Policy (2.(3)d) that the Board of Directors analyzes and evaluates the performance of the board of directors meetings every year to maintain and improve their effectiveness, which is publicized in our website

- **[PDF] Corporate Governance Policy**

1. Action taken in FY2025 based on the evaluation of FY2024
The results of the questionnaire survey regarding effectiveness of the Board of Directors in FY2024 showed that the average overall evaluation scores were on an upward trend compared to the previous fiscal year and confirmed that the effectiveness continues to be at a high level. Taking into consideration the results of the interviews of the members of the Board of Directors, the Company defined the state where the effectiveness of the Board of Directors is high as (1) Directors and Audit & Supervisory Board Members with diverse skills work together with mutual respect and (2) the bold management decisions and execution are supported in both offensive and defensive aspects through uninhibited discussions open to constructive criticism, and the Board of Directors is fulfilling its responsibility to aim for sustainable improvement in corporate value over the medium to long term through the flawless functioning of both (1) and (2).
As a result of the evaluation, we received many specific opinions regarding how to select and handle important items on the Board meetings' agenda and how to elevate information provision and conduct of proceedings to improve the quality of discussions. In response to these evaluation results, the Company carried out mainly the following initiatives in FY2025 to further improve the oversight function and quality of discussions of the Board of Directors.
-We sorted out the themes discussed at the Board of Directors meeting with focus on high priority agenda items and offered more systematic and enhanced discussion opportunities through intensive discussions in discussion camps.
-We clarified monitoring targets for confirmation of the progress of the Medium-Term Management Plan and high priority agenda items and formulated an annual agenda schedule. We also facilitated timely reporting and discussions reflecting important milestones and changes with the aim of improving the effectiveness of the oversight function of the Board of Directors.
-For further improving efficiency of the meeting operation and securing sufficient time for discussions, we promoted the use of videos explaining agenda items even more. We also refined our proposal materials to clarify points requiring discussions to improve the quality of discussions.
-We further enhanced information provision to External Directors and Audit & Supervisory Board Members to formulate their own opinions by setting periodic meetings for the CEO and Independent Directors and Audit Supervisory Board Members to exchange opinions and increasing opportunities for discussions by inviting external lecturers.
Further, the Company continued to hold the following events in FY2025 to enhance effective communication among the Board members: (1) The Independent Directors and Auditors Council for Independent Directors and Audit Supervisory Board Members to exchange opinions and share information; and (2) Private sessions exclusive for Non-Executive Directors.

The Company has defined the state where the effectiveness of the Board of Directors is high as (1) directors and Audit & Supervisory Board members with diverse skills appropriately oversee, advise, and execute duties from positions with respective responsibilities while cooperating and functioning as a team with mutual respect and (2) the bold management decisions and execution are supported in both proactive and defensive aspects through uninhibited discussions open to constructive criticism, and the Board of Directors is fulfilling its responsibility to aim for sustainable improvement in corporate value over the medium to long term through the flawless functioning of both (1) and (2).



Definition of "highly effective Board of Directors"

2. Evaluation of FY2025

(1) Evaluation method

For the evaluation of the Board's effectiveness in FY2025, the Company carried out a questionnaire survey of the Board members and held interviews with each member of the Board as in FY2024. As for evaluation items, it added new questions for measuring the level of achievement of the state where the effectiveness of the Board of Directors is high, whose definition was sorted out in the effectiveness evaluation in the previous fiscal year. The questions regarding the operation of the Board of Directors meetings and related formats were sorted out, cut back, and revised into questions aimed at deeply grasping the Board members' opinions and recommendations regarding the future of the Board of Directors.

In particular, we collected opinions from the perspectives of corporate governance structure, criteria for proposals to be submitted to the Board of Directors meetings, the Board structure, agenda items, the Chairperson, operation of the meetings, Executive Nomination Committee and Compensation Committee, information provision, and self-evaluation. We enhanced qualitative analysis to identify challenges for improving the effectiveness of the Board of Directors and grasping specific improvement recommendations while carrying out quantitative evaluation for some parts. The results of the evaluation of the effectiveness of the Board of Directors were reported and discussed at regular Board meetings. Furthermore, the evaluation of the Company's Board of Directors by institutional investors and proxy advisory firms was also reported.

(2) Evaluation

The following shows the evaluation result of the effectiveness of the Board of Directors based on the above evaluation method.

-In the evaluation in FY2025, we carried out quantitative evaluation of the level of the achievement regarding the state where the effectiveness of the Board of Directors is high and confirmed that it satisfied the levels expected by individual Directors and Audit & Supervisory Board Members. Also, the revision of the evaluation items enabled us to broadly grasp opinions and recommendations regarding the ideal state of the Company's Board of Directors, corporate governance system, criteria for proposals to be submitted to the Board meetings, the Board structure, in addition to the existing aspects of its operation and format, and we identified the challenges for improving the effectiveness and sorted out the direction of improvement more specifically.

-As a result of comprehensive consideration of collected opinions, from the perspective of the state where the effectiveness of the Board of Directors is high, we evaluated that it is in a state where its oversight and advisory functions are appropriately fulfilled in light of the previously set definition through open and constructive discussions. Building on this, we will primarily

implement the following measures to further improve the effectiveness.
-From the perspective of contributing to improvement in corporate value over a medium to long term, we will further clarify and narrow down the important themes that come under the Board's province for facilitating focused discussions. At the same time, we will flexibly review the setting of said themes to enhance timely and effective discussions.
-Taking into consideration a system and oversight function that enable us to respond to changes in the management environment even more swiftly, we will advance study of appropriate delegation of authorities to the Management Executives.
-We will implement various measures to further improve efficiency of meeting management with the aim of achieving high quality decision making by the Board of Directors focused on high priority matters.
-Further, to improve the quality of discussions at the Board meetings, we aim to enhance provision of information to Independent Directors and Audit & Supervisory Board Members and incorporate diverse perspectives. Along with this, we will facilitate collaboration between the Board of Directors and Audit & Supervisory Board Members for effective demonstration of the former's oversight function and the latter's audit function, thereby further strengthening the governance function of the Board of Directors as a whole.
The Company's Independent Directors stated that discussions at the Company's Board of Directors were very open, active, and satisfactory in comparison with other companies.

＜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 29, 2026, The Audit & Supervisory Board has five members, comprising two full-time Audit & Supervisory Board Members and three Independent External Audit & Supervisory Board Members.

In FY2025, the Company held 10 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, and attempted to further enhance information sharing and exchanged opinions by leveraging respective expertise of individual member to deepen their understanding of the activities of the Management Executives.

In FY2025, 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

With regard to the audit-related key discussion topics, the Audit & Supervisory Board had sufficient study and discussions with Accounting Auditors of potential risks of material misstatements in the consolidated financial statements and impacts and changes of, and developments in, material events, etc. that occurred in FY2025. In addition to these activities, the Audit & Supervisory Board held two rounds of discussions with the Accounting Auditors on the trend of early disclosure of Yukashoken Hokokusho (Annual Security Report) and sustainability disclosure as well as the next-generation audit leveraging AI to accurately grasp the changes in the environment surrounding accounting audit, and confirmed the current status of the Company and future considerations.

＜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 (six 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 FY2025, the Company held 10 Independent Directors and Auditors Council meetings. The members continuously discussed important management matters such as progress in significant businesses and partnerships related to the management policies, business restructuring of the Company and the Fujitsu Group including mergers and acquisitions, and corporate governance of the Company, 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, the "meeting body for prior explanation" that is attended by full-time Audit & Supervisory Board Members as observers was held 4 times 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.

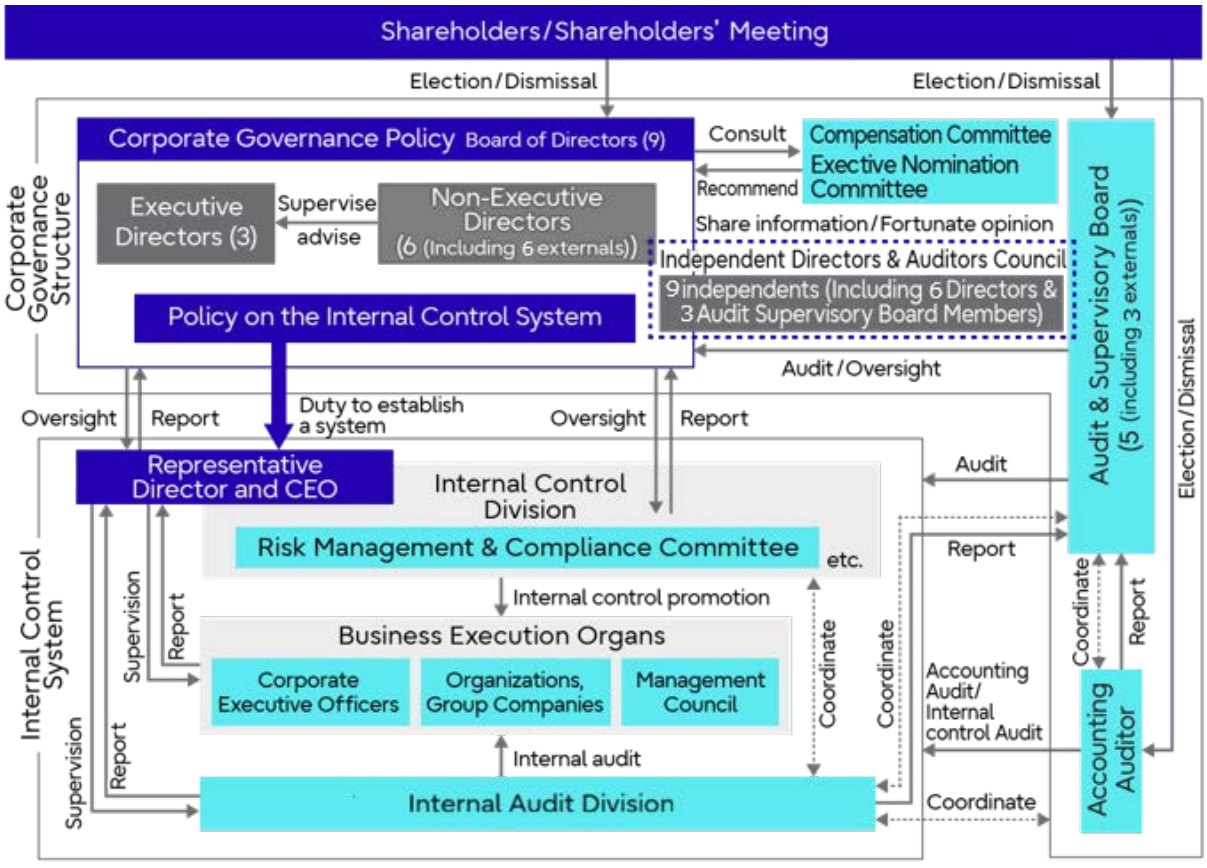
The Executive Nomination Committee deliberates about candidates for Director and Audit & Supervisory Board Member positions in accordance with the "Structural framework" and the "Procedures and policy of Directors and Auditors nomination/dismissal" stipulated in the Company's "Corporate Governance Policy" and provides its findings or recommendations to the Board of Directors. In addition, the Compensation Committee deliberates about the level of base compensation, the method for calculating performance-based compensation, etc. in accordance with the "Procedures and policy of determining Directors and Auditors compensation" stipulated in the Company's "Corporate Governance Policy" and provides its findings or recommendations to the Board of Directors.
Executive Nomination Committee and Compensation Committee consists of three Independent Directors. The Members of the 2 committees appointed in June 2026 are as follows. Additionally, the secretariats of both committees are operated by the Company's HR and legal departments.

- Executive Nomination Committee
  Chairperson: Kenichiro Sasae (Independent Director)
  Members: Yoshiko Kojo (Independent Director), Kunimasa Suzuki (Independent Director)

- Compensation Committee
  Chairperson: Byron Gill (Independent Director)
  Members: Takuya Hirano(Independent Director), Izumi Kobayashi(Independent Director)

In FY2025, the Executive Nomination Committee met 9 times and the Compensation Committee met 7 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 and mix of compensation of Directors, details of evaluation indicators in the performance-related compensation for the Executive Directors, compensation for Audit & Supervisory Board Members, etc. And each Committee provided its findings to the Board of Directors by the end of the period under review. Moreover, the Committees collaborated with the Audit & Supervisory Board to review the candidates for Audit & Supervisory Board Members and the compensation for Audit & Supervisory Board Members. The Executive Nomination Committee also considered the skill matrix, the succession plan for the CEO, etc. and the selection of candidates for External Directors and Audit & Supervisory Board Members, and conducted a peer-review of Non-Executive Directors, while the Compensation Committee also discussed the upper limit of the total compensation amount for Directors.

The diagram below illustrates the Company's corporate governance structure. (As of June 29, 2026).



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.

Basic Policy on Executive Compensation

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

- **[PDF] Corporate Governance Report「Incentive Policies for Directors (page 22, 23); Policy on Determining Remuneration Amounts and Calculation Methods (Page 25, 26, 27)」**

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 126th Annual Shareholders’ Meeting**

Disclosures Relating to Corporate Governance

Board of Directors (as of June 29, 2026)

	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		
	Yoshiko Kojo	Chairperson of the Board of Directors		x
	Kenichiro Sasae			x
	Byron Gill			x
	Takuya Hirano			x
	Izumi Kobayashi			x
	Kunimasa Suzuki			x

- [PDF] Board of Directors (as of June 29, 2026)

FY2025 Attendance at Meetings of the Board of Directors or Audit & Supervisory Board

Meeting	Number of Meetings	Attendance Rate
Board of Directors	13	99.2%
Audit & Supervisory Board	10	98.0%

- [PDF] FY2025 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 29, 2026)

	Name	Independent	Diversity		Skill Matrix				
			Gender	Nationality	Corporate Management	Finance and Investment	Global	Technology	ESG, Academia and Policy
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
Director	Kunimasa Suzuki	x	Male	JP	x		x	x	

- [PDF] Skill Matrix (Directors)

Auditors (As of June 29, 2026)

	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

Compliance

Policies and Structure for Implementation

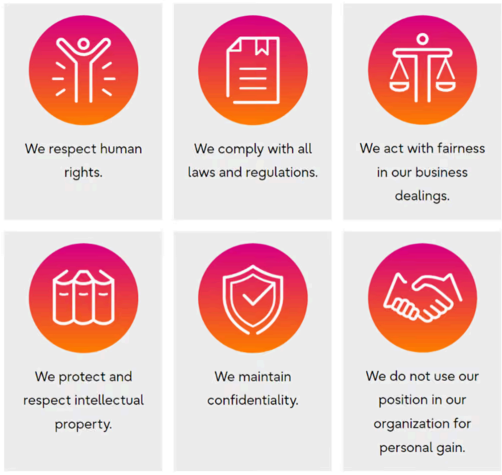
The Fujitsu Group aims to be a trusted corporate group, one chosen by stakeholders for investments, deals, and employment, with each executive and employee carrying out their business duties with a high awareness of compliance, as we fulfill our role as a model company. To achieve this, Fujitsu has established and globally implemented the Global Compliance Program to promote understanding and implementation of the Fujitsu Way Code of Conduct and its explanatory guide, the Global Business Standards (GBS). Through these efforts, we are fostering a high level of compliance awareness and, with senior management leading from the front, cultivating a corporate culture in which no employee tolerates wrongdoing. We also extend these initiatives to all parties involved in Fujitsu's business and seek their understanding and support.
To promote these initiatives, we have established a compliance division under the General Counsel and are carrying out various measures in cooperation with compliance offices in each region.
The results of these activities are reported to the Risk Management & Compliance Committee, which was established based on the "Policy on the Internal Control System" (*1). We also work in cooperation with the Board of Directors and Audit & Supervisory Board Members. In addition, each region collaborates with its Regional Risk Management & Compliance Committee, established as a subcommittee of the Risk Management & Compliance Committee, to promote awareness of and compliance with the Fujitsu Way Code of Conduct throughout the Group.

The operational status of the Global Compliance Program is regularly reported to the Risk Management & Compliance Committee, the Regional Risk Management & Compliance Committee, and the Board of Directors. The development and operation of internal rules, education, and monitoring systems to comply with various laws and regulations related to Fujitsu Group's business are promoted under the practice and supervision of management.

- **(*1) : [PDF] Policy on the Internal Control System (P10-13)**

Fujitsu Way Code of Conduct

The Fujitsu Way contains a Code of Conduct, which outlines the fundamental principles that all Fujitsu Group employees should abide by, as shown on the right.
Fujitsu has also implemented the Global Business Standards (GBS) (*2) in 14 languages and it applies uniformly across the Fujitsu Group. It defines and elaborates on the principles of Fujitsu's Code of Conduct to help executives and employees understand and apply the Code of Conduct in their actions.



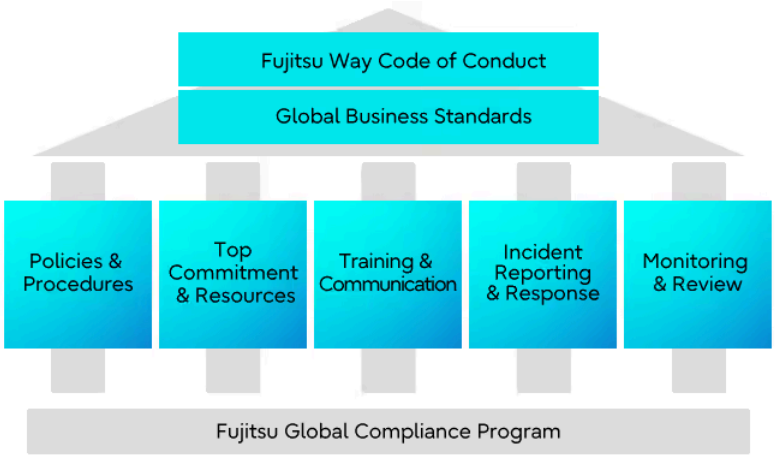
- **(*2) : Global Business Standards (GBS)**

Our employee evaluation criteria include assessing the level of an employee's embodiment of "Our Values" under the Fujitsu Way. One of the values is for employees to act with ethics, transparency and integrity. As such, employee personnel assessment and compensation reflect their level of compliance with the Code of Conduct.

- **Fujitsu Way**
- **Financial Well-being**

Global Compliance Program

Fujitsu has developed the Fujitsu Global Compliance Program to disseminate the Fujitsu Way Code of Conduct and the GBS, and is working to maintain and improve the Fujitsu Group's global legal compliance structure. The Global Compliance Program organizes our various compliance-related activities into five pillars in a systematic manner. The Global Compliance Program promotes external understanding of Fujitsu's compliance structure and its compliance activities, in addition to clarifying what items Fujitsu needs to address on a continual basis. Based on this Global Compliance Program, we implement various policies and initiatives in each region, taking into account factors such as each country/region's legal systems and government institutions guidelines.
When implementing the Global Compliance Program, we establish internal Group rules and assign a compliance officer in each region to be responsible for compliance activities and ensure the structure's implementation. We also continuously provide employees with various forms of training, with the goal of embedding the Fujitsu Way Code of Conduct and the GBS. In addition, we have established an internal whistleblower system in the event of compliance issues, and employees are required to immediately report compliance violations to the Risk Management & Compliance Division if they are discovered. We periodically verify the effectiveness of the Global Compliance Program through measures such as risk assessment, audit, and reviews by external specialists, and continuously work towards improving the Global Compliance Program.



Global Compliance Program

1. Establishing policies and procedures

Fujitsu has established the Fujitsu Group Global Policy, which sets out the minimum content or common matters that should be included in the internal standards of all Fujitsu Group companies (consolidated subsidiaries) both in Japan and overseas. Based on this, we have established common standards (Standard Policies) in each field that all officers and employees of consolidated subsidiaries globally must observe and respect.
Based on the Standard Policy for Compliance, a common policy established with the approval of executive management, all Fujitsu Group companies in Japan and overseas have established their own internal compliance standards and detailed rules for areas that have a particularly large impact on business, such as antitrust laws and bribery, in order to ensure thorough compliance and sustainably increase corporate value.
With regard to bribery and conflict of interest, in addition to principles defined in the GBS, we have established various internal rules that state the advance application and approval processes required for actions such as providing gifts and hospitality to government officials, receiving gifts and entertainment from business partners by our employees, giving donations, sponsorships and charitable contributions to various organizations, including political organizations, and facilitating payments.
We also conduct compliance checks of organizations that receive donations and sponsorships. Furthermore, as one measure for conducting advance surveys and evaluation of transaction risk in regions and fields that are at a high risk for corruption, we perform due diligence at the time of starting new transactions. We screen our suppliers through steps such as requiring suppliers to complete questionnaires according to their risk level.
We also require business partners to comply with laws and regulations through contracts and other means. In addition, even after transactions begin, we continue to monitor whether there have been any changes in the risk levels of our business partners.

2. Top-level commitment and securing of resources

Top management expresses its intentions to strive for compliance proactively and continuously through measures such as sending messages to employees. In doing so, Fujitsu puts the Code of Conduct and the GBS into practice and spread them throughout the entire Fujitsu Group.
The President himself has repeatedly sent out messages to all employees, both in Japan and overseas, regarding the importance of employees understanding the expectations of customers and society and taking autonomous, honest action with the Fujitsu Way Code of Conduct as a guide. Even overseas, regional heads and Group company top managers continuously send out messages which emphasize going beyond mere compliance with the law and focus on the premise of operating as a trustworthy corporation.

Furthermore, we hold Fujitsu Compliance Week every year to increase awareness of compliance companywide. During the week, compliance messages are simultaneously sent to employees by top management (including the CEO) at Fujitsu headquarters and the Heads of each business region, and Presidents of group companies in each country. We also release annually updated Compliance e-Learning to employees of all Group companies, and provide compliance-related activities planned for each region.
Additionally, we have assigned staff in charge of compliance operations in each region, and have formed a global network composed of staff in charge of risk compliance at each Fujitsu Group company. Based on these steps, we have established a system for operation of our Global Compliance Program. In FY2025, officers responsible for compliance in each region visited Japan for a discussion on a future global compliance policy.

3. Training and communication

The Fujitsu Group continuously conducts various training and communication opportunities for executives and employees in order to embed and implement the Fujitsu Way Code of Conduct, the Global Business Standards, and other internal rules.
Standard Policy for Compliance, one of the common standards, stipulates that compliance training be conducted for all Fujitsu Group executives and employees, and compliance e-learning is conducted every year. The contents of this e-learning include risk areas such as bribery, collusion, and security export control, along with how to use our whistleblowing system. Moreover, in order to reflect the results of risk assessment and social conditions, the Compliance Division at Fujitsu headquarters and compliance officers from each region conduct an annual review of the e-learning. In FY2025, compliance e-learning was conducted in 14 languages for all Fujitsu Group executives and employees (approximately 110,000 people). As of April 2026, 97% of all executives and employees have already taken the course.
In addition to the measures listed above, we conduct timely online training and e-learning in accordance with the risk level of each organizational level, region, and division. The training and e-learning is based on laws, customs, and actual business conditions in each country. Every year, Fujitsu and domestic Group companies hold compliance training sessions targeted at newly appointed executives. This training is conducted by lawyers from outside Fujitsu, and the company's legal and compliance divisions. For managers, we periodically conduct internal training where in-house instructors explain the importance of the Code of Conduct and compliance, in addition to discussing typical scenarios and difficult situations. Compliance education is also incorporated into new employee training to help them understand the Code of Conduct and the importance of GBS in addition to training focused on specific risks such as sales and legal.
In addition, to further promote understanding and implementation of GBS, we have created animation videos as easily understood visuals, and explanatory pages to connect the videos to specific utilization and practice. We have developed this globally, as we intend to spread GBS to every executive and employee. We also provide compliance training to partner companies to ensure fair trade. When entering into new business dealings in Japan, we require all project workers to undergo mandatory training to prevent the establishment of inappropriate business relationships, based on examples of compliance issues that may arise in transactions, such as violations of the Act on Preventing Delay in Payment to Small and Medium-Sized Entrusted Business Operators in Relation to Manufacturing Consignment, fraud, and fictitious transactions. We also provide partner training overseas, providing learning sessions to suppliers in the Asia-Pacific region, mainly on fictitious transactions and bribery, and in Europe, to channel partners, marketing agencies, and sales intermediaries, based on examples of all compliance issues that may arise in transactions, such as bribery, conflicts of interest, competition law, and money laundering.
As mentioned above, Fujitsu has designated an annual Fujitsu Compliance Week, during which the CEO and regional heads send out a message to employees and distribute compliance-related news. In addition to these top-down activities, in overseas regions, we establish scenarios of actual compliance issues that could occur and provide opportunities for employees in frontline departments to think about and discuss how to deal with them through role-playing in a variety of positions. Through this, we are deepening employees' understanding of workplace compliance.

4. Reporting and responding to incidents

Establishing an internal whistleblower system

The Fujitsu Group has established an internally and externally accessible portal, Fujitsu Alert, operated by an external vendor, to receive internal whistleblower reports and consultation (including anonymous reports) from all Group employees (including board members, retirees, temporary transfers, contracted employees, part-time employees, dispatch workers, and others) and offer consultations. Group companies also maintain and operate separate internal whistleblower systems.
Through a web form or telephone hotline, Fujitsu Alert accepts reports on suspected wrongdoing or concern from all Fujitsu Group employees and external parties relevant to the Fujitsu Group, including customers and suppliers (anonymously, if applicable). Fujitsu Alert is available in 14 languages 24 hours a day, 365 days a year. It is also used to communicate with reporters regarding the content of their reports, including providing additional information and receiving comments from the Compliance Division.
Fujitsu Alert also serves as reporting system for business partners from which the Fujitsu Group (companies in which Fujitsu has direct or indirect investment of more than 50%) directly procures goods, software or services.

- **Fujitsu Alert**
- **Compliance Line for Suppliers in Japan**

Fujitsu Alert is publicized to employees via periodic messages, compliance training sessions and the website. In addition, Fujitsu periodically confirms trends in the usage of Fujitsu Alert in order to ensure increased recognition for and confidence in the system among employees.

Protection of whistleblowers

Employees are encouraged to report breaches or potential breaches of compliance of which they become aware. Furthermore, if employees are unsure of the appropriate action to be taken, they can seek advice from a supervisor in their division or a specialized division such as the legal division.
Anonymous reports can be submitted to Fujitsu Alert, and we handle information under strict confidentiality with the utmost care in order to preserve anonymity. Even in cases where the whistleblower is indirectly identified during investigation process, we strictly prohibit the adverse treatment of whistleblowers due to their reports, and any such adverse treatment will be regarded as an extremely serious breach of internal policies.

Response to reports

When a breach of compliance is reported on Fujitsu Alert, we will conduct an internal investigation under the supervision of responsible managers who are licensed attorneys, and will cooperate with external attorneys when necessary. Fujitsu directly reports the results of its internal investigations to the Board of Directors and the Risk Management & Compliance Committee. These reports are made independent of the division and/or affiliated companies which are involved in the subject matter under investigation. Depending on the content of the report, the Compliance Division may delegate an investigation to other authorized divisions if deemed appropriate.
The Compliance Division will conduct an appropriate internal investigation in order to understand the facts and review possible countermeasures in accordance with applicable laws and professional standards. The internal investigation includes, but is not limited to, consideration of applicable laws, consideration of appropriate investigation steps, evaluation of collected evidence, documentation of investigation results, and reporting or escalation. Depending on the results of the investigation, Fujitsu provides feedback to the whistleblower if necessary based on applicable laws such as the data protection laws and business laws.
In the event that the investigation has verified problems according to the Code of Conduct, Global Business Standards, or other internal rules, we take corrective measures such as disciplinary action and reflect the results in personnel evaluations.

In order to prevent similar problems from occurring in the future, we remind all parties of rules, revise systems, strengthen monitoring and supervision, and take other necessary measures.
The process for these investigations, etc., is also reviewed and improved at least once a year, including at the time of establishment of the annual plan under the Global Compliance Program and/or at the time of enactment or amendment of relevant laws.
Fujitsu may be either required by law or decide based on business judgment to provide information about compliance violations to certain government and/or judicial agencies (including, but not limited to, government investigative agencies or courts). When making such decisions, compliance officers work together with managers and other relevant divisions as necessary.
Moreover, reports, such as letters or emails, received through channels other than Fujitsu Alert are also investigated when they involve suspected compliance violations, and corrective or other appropriate actions are taken as necessary.

Total of reports to Fujitsu Alert and breakdown

In FY2025, 137 reports were submitted to Fujitsu Alert. Of these, there were no confirmed cases of corruption (bribery included) or legal disputes. The Fujitsu Group takes measures to comply with the laws and regulations of countries where it operates and prevent corruption based on the GBS 5.2 Prevention of Bribery (*3) and the Standard Policy for Compliance.

	FY2025	
	Case reported	Number of actions taken
Total number of cases	137	3
Human rights violations (harassment, discrimination, etc.)	50	1
Violation of laws or internal rules	4	1
No violations (*4)	46	-
Violation of Competition Act (bid rigging, cartels, etc.)	2	0
Violation of laws or internal rules	0	0
No violations	2	-
Bribery	2	0
Violation of laws or internal rules	0	0
No violations	2	-
Violation of conflict of interest policy	7	1
Violation of laws or internal rules	2	1
No violations	5	-
Violation of the Fujitsu Group's or customers' confidential information or personal information protection	9	0
Violation of laws or internal rules	1	0
No violations	8	-
Insider trading, money laundering	0	0
Violation of laws or internal rules	0	0
No violations	0	-
Other	67	1
Violation of laws or internal rules	10	1
No violations	57	-

- [PDF] The number of reports and their breakdown related to Fujitsu Alert

- (*3) : GBS
- (*4) : "No violations" in the chart includes cases under investigation as of May 11, 2026

Filing reports with the Risk Management & Compliance Committee

When executives or employees become aware that compliance violations have occurred, or recognize signs that violations may occur, they are required by the risk management regulations to immediately file a report with the Risk Management & Compliance Committee and in accordance with the reporting system previously established by the head of the division. In addition, we periodically report to the Risk Management & Compliance Committee, the Board of Directors and Audit & Supervisory Board members concerning internal whistleblower reports and consultations, as well as our responses to major compliance issues. Please refer to the Fujitsu Group Integrated Report for the number of meetings of the Risk Management & Compliance Committee and the Board of Directors.

5. Monitoring and reassessment

The Fujitsu Group conducts annual verification of the effectiveness of the Global Compliance Program through reviews of our risk assessment and internal auditing activities, and through reviews by external experts such as law firms. We are also working to continuously improve our Global Compliance Program based on the results of applicable reviews and audits, as well relevant social conditions. Please refer to the Risk Management page regarding our risk assessment activities.
The Compliance Division of Fujitsu headquarters continually assesses risk that mainly targets Group companies located in overseas countries and regions with a high risk of corruption. Through interviews with executives/employees and verification of internal rules and business processes, the Compliance Division analyzes the compliance risks of local businesses. It then proposes countermeasures in accordance with the actual contents and extent of risks, and supports the implementation of those countermeasures.
The status of risk assessment and implementation of the Global Compliance Program are periodically reported to the Risk Management & Compliance Committee, the Regional Risk Management & Compliance Committees, and the Board of Directors. The discussions and decisions made at these meetings are reflected and implemented in a timely manner to activities in the Global Compliance Program.
Additionally, in FY2025, the Fujitsu Group implemented a compliance survey of 4 domestic group companies in order to assess the degree of permeation and embodiment of the Group's stated values in these organizations. The results of the analysis were provided to each company's management and department heads as feedback and utilized as a management tool to enhance compliance awareness. This helped each company and department to independently grasp and work to improve issues, and, when necessary, allows the compliance department to support the examination and implementation of solutions or improvement strategies for issues, as we advance with efforts to promote the spread of Fujitsu's values and ethics.

Initiatives for Security Export Control

From the viewpoint of maintaining global peace and security, the export of goods and the transfer of technology that could be used for the development or production of weapons of mass destruction or conventional weaponry are controlled by an international framework for security export control. In Japan, by following its framework, the regulations for security export control are implemented under the Foreign Exchange and Foreign Trade Act (the Foreign Exchange Act).
In line with one of the Fujitsu Way Code of Conduct, "We comply with all laws and regulations," Fujitsu has enacted "Security Export Control Regulations" internally and thoroughly enforced it as the fundamental policy to promote security export control in accordance not only with the Foreign Exchange Act, but with the Export Administration Regulations (EAR) of the United States applied extraterritorially.
As Fujitsu's management system, the President serves as the Security Export Control Chief Officer, while the Security Export Control Office in the Corporate Governance and Compliance Unit serves as the organizer of the security export control operations. On the operational process, it is required that, before export of goods and the transfer of technology to overseas, their classification and transaction screening (scrutinizing destination country/region, end-use/end-user) are rigidly executed and then all necessary licenses are adequately obtained. "Security Export Control Regulations" also sets the rule

that legal violations shall be reported immediately. When execution of business, to prevent legal violations by misinterpretation and/or overlook of related regulations, Fujitsu closely aligns with the Ministry of Economy, Trade and Industry which has jurisdiction over export administration regulations. To uphold such internal system for security export control, the regular audit is conducted, as well as the export control training is provided to all executives and employees. For domestic and overseas Group companies, the guidance on establishing rules and systems for proper security export control is provided accordingly, and any related activities like educational support, audit support and domestic seminar for information exchange are taken as well. Furthermore, an e-learning course on basic security export control also has been created, which is available in multiple languages for Fujitsu Group companies worldwide.

System to ensure proper financial reporting

In the "Policy on the Internal Control System," which was resolved by the Board of Directors, Fujitsu stipulates the following points.

1. The Company has, apart from the organization that prepares financial reports, an organization under the Chief Financial Officer responsible for establishing, operating, and evaluating internal control over Fujitsu Group financial reporting, to ensure the effectiveness and reliability of financial reports.
2. These organizations create rules for establishing, operating, and evaluating internal control over the unified accounting policies shared throughout the Fujitsu Group and financial reporting.
3. The organization responsible for establishing, operating, and evaluating internal control over financial reporting periodically reports to the Board of Directors and any other relevant person or organization the results of evaluations on the effectiveness of the internal control.

Status of operations

The organization responsible for internal control and internal audits has established the system and assesses internal control over financial reporting throughout the Fujitsu Group, and reports the activity status and assessment results to the Representative Director and CEO, Chief Financial Officer, Audit & Supervisory Board Members and the Board of Directors in accordance with the principles of the "Practice Standards for Management Assessment and Audit concerning Internal Control Over Financial Reporting" published by the Business Accounting Council.

Our approach to tax matters

Tax compliance

Tax compliance at the Fujitsu Group is carried out according to the Fujitsu Way Code of Conduct.
We understand the purpose and essence of each country's tax laws and treaties, as well as other guidelines such as those laid out in the Base Erosion and Profit Shifting (BEPS) Project led by the OECD, and abide by them. We strive to file tax returns and pay taxes appropriately. In transactions between related companies, we will comply with the general rule of an arm's length price and distribute profits appropriately.

Tax Governance

The Director who serves as the Chief Financial Officer is responsible for the proper filing and fulfilment of tax returns and obligations, management of tax risks, and appropriate management of tax expenses. Important matters and risks related to tax are reported to the management meeting and Board of Directors in a timely and appropriate manner for approval.

Transfer pricing

We comply with the principle of arm's length pricing and distribute profits appropriately when conducting transactions between affiliated companies. We do not transfer business profits generated in countries/regions to countries/regions with low tax rates where we do not conduct business transactions.

Tax planning

We do not engage in tax planning that is solely for the purpose of avoiding taxes without business purpose or business substance. Similarly, we will not use tax havens to transfer profits with the intention of avoiding taxes.

Relationships with tax authorities

We strive to build sound relationships with the tax authorities in each country by conducting our business with ethics, transparency, and integrity in accordance with Our Values under the Fujitsu Way.
Based on the above, we aim to achieve proper tax management, in order to continuously improve corporate value.

Tax information

Tax information by region (FY2024)

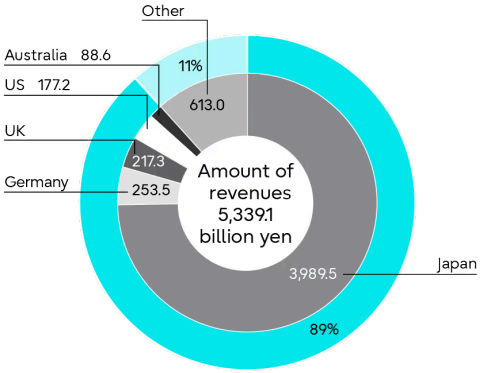
(billion yen)

	Domestic	Overseas (*5)	Europe	Americas	Asia Pacific	East Asia	Total
Amount of revenues	3,989.5	1,349.6	760.7	217.6	267.2	104.1	5,339.1
Amount of tax paid	58.5	9.4	0.9	4.8	2.9	0.8	67.9

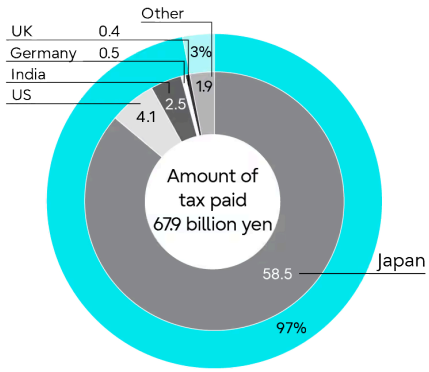
Notes:The amounts indicated above are based on the “Country-by-Country Report” submitted to the Japanese tax authorities, and do not have any direct connection to consolidated financial statements.

- **[PDF] Click here for a PDF file detailing tax information by region (FY2024)**

- (*5) Overseas: Europe includes the Middle East and Africa. East Asia represents the sum of China, Taiwan, and South Korea, while Asia Pacific includes other Asian countries and Oceania.



Breakdown of revenues by country



Breakdown of tax amount by country

Company name and main business (as of the end of March 2025)

Company Name		Main Business
Japan	Fujitsu Ltd. Fujitsu Japan Limited Fsas Technologies Inc. Fujitsu Telecom Networks Limited Fujitsu Frontech Limited Fujitsu Network Solutions Limited Transtron Inc. Ridgelinez Limited Fujitsu Personal System Limited Fujitsu Defense & National Security Limited etc.	●Consulting, system construction, provision of various services related to maintenance and operation, sales of equipment and software for information systems ●Manufacture of network equipment and network systems ●Planning of network systems, consulting, and provision of construction management, operations, maintenance and services ●Consulting and research related to digital transformation ●Provision of front-end technology products and their related solutions and services ●Research, development, construction and maintenance of security-related information and communication systems, and the development, manufacture and sale of equipment and software for information and communication systems
Europe	Fujitsu Technology Solutions (Holding) B.V. Fujitsu Technology Solutions GmbH Fujitsu Services Holdings PLC FUJITSU SERVICES LIMITED GK Software SE etc.	●Consulting, system construction, provision of various services related to maintenance and operation, sales of equipment and software for information systems ●Development of retail software products and provision of sales and related services
Americas	Fujitsu Network Communications, Inc. Fujitsu America, Inc. Fujitsu North America, Inc. Fujitsu Consulting (Canada) Inc. GK Software USA, Inc. etc.	●Development, manufacturing, construction and provision of services related to network equipment and systems ●Consulting, system construction, provision of various services related to maintenance and operation, sales of equipment and software for information systems
Asia Pacific	Fujitsu Australia Limited Fujitsu Asia Pte. Ltd. FUJITSU CONSULTING INDIA PRIVATE LIMITED Fujitsu New Zealand Limited Fujitsu (Thailand) Co., Ltd. etc.	●Consulting, system construction, provision of various services related to maintenance and operation, sales of equipment and software for information systems
East Asia	FUJITSU KOREA LIMITED Fujitsu (China) Holdings Co., Ltd. FUJITSU (XI'AN) SYSTEM ENGINEERING Co.,Ltd. FUJITSU TAIWAN LIMITED FUJITSU HONG KONG LIMITED etc.	●Consulting, system construction, provision of various services related to maintenance and operation, sales of equipment and software for information systems

- [PDF] Click here for a PDF file on company names and main businesses (as of March 31, 2025)

FY2025 performance

Message from management

- During the annual Fujitsu Compliance Week, the President, regional heads, and other senior executives sent out messages to employees about ensuring compliance

Compliance training

- Compliance e-Learning for all officers and employees at the Fujitsu Group (Conducted in 14 languages for approximately 110,000 people): 97% of executives/employees have taken the course as of April 2026.
- Other e-Learning and on-demand training for different regions, companies, positions and/or functions (For example, training conducted for newly appointed executives, managers and overseas assignees, newly hired employees or sales employees).
- Conducted training on fair trade for partner companies

Bribery/Cartels

- No confirmed cases.

Security Export Control

- Regular internal audit: 96 divisions within Fujitsu
- Seminar for employees responsible for export control at Group companies: 26 domestic Group companies
- Audit, training and support for internal control: 16 domestic Group companies and 36 overseas Group companies

Supply Chain

Policy

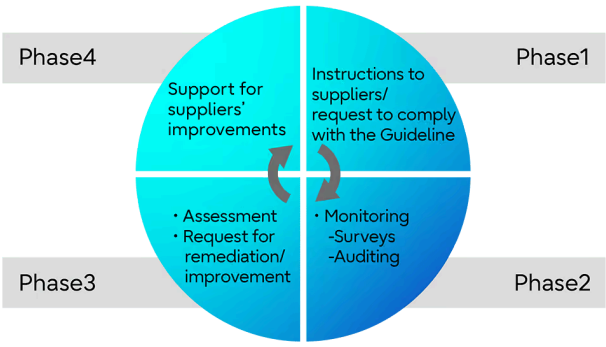
The Fujitsu Group holds “Co-existence with Suppliers”, “Fair and Proper Evaluation and Selection of Suppliers” and “Promotion of Sustainability in Procurement Activities” as the tenets of its Corporate Social Responsibility (CSR) procurement policy, and conducts its global procurement activities accordingly.
In 2005, we developed the "CSR Procurement Guidelines” for sustainable procurement and requested our suppliers in Japan and overseas to comply appropriately. In 2018, we adopted the RBA (*1) Code of Conduct as our "Fujitsu Group CSR Procurement Guidelines." We revised the guidelines in 2023, changed the name to the “Fujitsu Group Sustainable Procurement Policy”, and are now in the process of obtaining written agreements to the Policy from suppliers representing 80% of our procurement spending, including Japanese and overseas Group companies. Fujitsu is also expanding its engagement by confirming agreement to the guidelines as part of the supplier account registration process, and has incorporated this requirement into its standard procurement contract templates. The agreements go beyond simple compliance and include a request that suppliers extend these requirements to companies further upstream in their own supply chains. Through this approach, Fujitsu seeks to ensure that its Code of Conduct is thoroughly embedded throughout the entire supply chain.
The RBA regularly incorporates feedback from stakeholders to support the ongoing development and implementation of its Code of Conduct.
Many of the companies in the Fujitsu Group’s supply chain are currently RBA members, and Fujitsu has adopted the RBA’s Code of Conduct, which reflect the views of workers employed by participating supplier companies, in the Fujitsu Group Sustainable Procurement Policy. Fujitsu requires the suppliers with whom it conducts business involving materials, components, hardware products, and other related items, to comply with these guidelines.

- **(*1) : [PRESS RELEASE] Fujitsu Joins EICC, a Global Corporate Social Responsibility Coalition**
  (which was rebranded to become the Responsible Business Alliance (RBA) in October 2017)

- **Fujitsu Group Procurement Policy**
- **RBA Code of Conduct**
- **[PDF] Fujitsu Group Sustainable Procurement Policy**

Sustainable Procurement Activities & Periodic Reviews

Under the group-wide policy, the relevant divisions in the Fujitsu Group collaborate regarding sustainability activities. Sustainability-related departments within Fujitsu have developed a structure under the supervision of the Sustainability Management Committee, which is chaired by the President and CEO. Under this structure, the progress of activities and the level of target achievement are reviewed twice a year. In the area of procurement, the Global Supply Chain Unit works with the relevant divisions in promoting sustainable activities by suppliers.



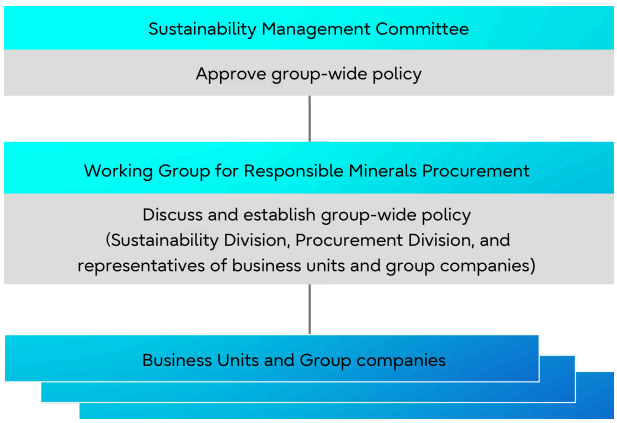
Fujitsu Group Procurement Policy

As part of our commitment to "preventing and mitigating human rights risks across the supply chain, promoting reductions in greenhouse gas (GHG) emissions, and ensuring diversity", we clearly set out the compliance obligations under our Sustainable Procurement Policy and require our suppliers to undertake sustainability activities. Then, to confirm that these activities are being fully implemented by suppliers, we ask them to respond to a sustainability survey (covering human rights, labor, environment, and ethics) plus various other surveys on topics such as information security and Business Continuity Management (BCM). As of FY2025, Fujitsu has also introduced EcoVadis, a third-party assessment tool to visualize and strengthen the management of sustainability risks in the supply chain.
Suppliers targeted for engagement activities related to sustainable procurement are selected based on factors such as strategic business relationships, procurement spend, and continuity of business transactions.

The responses to our surveys are analyzed and the results are returned to the suppliers as feedback. Where a supplier fails to meet Fujitsu's standards, we require them to make improvements. Where there is a particular need to check whether sustainability activities are being fully implemented by a supplier, an audit is conducted. Such suppliers are required to submit a remediation plan for any matters identified by the audit and Fujitsu works with the suppliers to make the necessary improvements. Fujitsu is continually enhancing its processes and promoting sustainable procurement with the goal that sustainability activities will ultimately be properly undertaken by suppliers and will become firmly entrenched.

Addressing High-Risk Minerals

The policy of the Fujitsu Group is to exclude from its products, components and supply chain any minerals that give rise to conflicts ("conflict minerals"), or minerals that are at high risk of being associated with forced labor or human rights violations. (The Fujitsu Group identifies tantalum, tin, gold, tungsten and cobalt as high-risk minerals.) Fujitsu has also established a structure to ensure the transparency of procurement activities in the supply chain and the responsible procurement of minerals. This structure includes the relevant internal divisions and operates under the jurisdiction of the Sustainability Management Committee.



Fujitsu Group Procurement Policy

- **[PDF] Fujitsu Group Policy on Responsible Minerals Sourcing**

Surveys on High-Risk Minerals

As part of its due diligence, the Fujitsu Group conducts high-risk minerals surveys with reference to the "OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas". These surveys use the Conflict Minerals Reporting Template (CMRT) and Extended Minerals Reporting Template (EMRT) developed by the Responsible Minerals Initiative (RMI).

- **[PDF] List of smelters checked in the survey**

Reminders are sent to those suppliers who failed to respond to our survey by the due date. If survey responses reveal insufficient answers, suppliers are asked to resubmit their responses. Where customers indicate that a smelter is considered to be "risky", we ask suppliers using that smelter to re-examine the nature of their dealings with the smelter.
While there have been no confirmed reports yet of smelters having any involvement with armed groups, we will continue to conduct programs aimed at identifying smelters and further increasing transparency in our supply chain.

Promoting Green Procurement

The Fujitsu Group has set out its basic approach to the environmentally sound procurement of components, materials and products in the Fujitsu Group Green Procurement Direction, and we are working with our suppliers to promote green procurement activities.
One focus area of these activities is the reduction of greenhouse gas (GHG) emissions, and the Fujitsu Group is requesting that its suppliers set GHG reduction targets and implement initiatives to achieve those targets. The Green Procurement Direction also requires that Fujitsu and all its related upstream companies expand their efforts aimed at reducing GHG emissions. In addition, as a first step toward water resource conservation, we are asking our suppliers to conduct water risk assessments and promote efforts to reduce water risk in the supply chain.
The Fujitsu Group also conducts surveys of the chemical substances contained in purchased products procured from suppliers, and promotes compliance with all legal and regulatory requirements as well as industry standards in the respective countries and regions. To support these efforts, Fujitsu has released the "Guideline Regarding Non-Containment

Management on Hazardous Substances", which require suppliers to appropriately manage chemical substances.
We will continue to promote activities that reduce environmental impacts throughout our supply chain.

- **Fujitsu Group Green Procurement**

Promoting the Setting of Greenhouse Gas Emissions Reduction Targets in the Supply Chain

With the intention of accelerating the journey to carbon neutrality, the Fujitsu Group has set FY2030 as its new goal to reduce its carbon emissions to zero, 20 years ahead of the previous schedule. The Fujitsu Group has achieved SBTi net zero certification as a result. Moreover, the Group is working to achieve net zero emissions across the entire value chain (Scope 3), including the supply chain, by FY2040.
To work together with our suppliers on reducing GHG emissions in the supply chain, we hold briefings for our major suppliers, calling on them to set reduction targets in line with international standards and then implement initiatives to achieve those targets. To further emphasize societal impact, since FY2024 we have received reduction target settings from targeted suppliers that represent 80% of all supply chain emissions, rather than 80% of procurement spending.

Data Collaboration with Suppliers to Visualize CO_2 Emissions by Product

With the goal of achieving net zero carbon emissions across the entire value chain by FY2040, in FY2024 the Fujitsu Group started collaborating with 45 of its Japanese and overseas suppliers to share data on CO_2 emissions at the product level(product carbon footprint (PCF)). Under this program, the Sustainability Value Accelerator, a Fujitsu service offering, is used to calculate PCFs in compliance with both international and Japanese rules, and then share that data with the companies concerned. As well as being designed with data confidentiality in mind, this offering also provides automated calculation functions and multilingual support. These features allow information to be shared quickly and easily across national, regional, and language boundaries, helping to build trust among participating companies and encouraging broader participation.
While allowing for national and regional characteristics and language differences, Fujitsu is working with local promotional organizations and overseas suppliers to encourage the collection and sharing of PCF data from upstream stages in the supply chain, such as the provision of raw materials and components. Through these efforts, Fujitsu is improving the visibility of CO_2 emissions across the entire supply chain and enabling more accurate identification of product-level emissions, thereby accelerating decarbonization initiatives throughout the value chain.

Promoting Diversity in the Supply Chain

The Fujitsu Group is committed to ensuring diversity throughout the supply chain. We believe that an environment in which diverse human resources are afforded equal opportunities and can leverage each other's values and abilities is essential to fostering innovation and, ultimately, to building and developing a robust, sustainable supply chain.
Given that societal issues and challenges differ depending on the country and location, our supplier diversity initiatives are based on policies developed and implemented according to the characteristics of each country/location. In Japan, for example, since women's empowerment figures prominently on the social agenda, we are promoting activities under the theme of supporting women's empowerment in the supply chain. Specifically, as a first step toward visualizing the status of our initiatives and to foster awareness, we are asking our major suppliers to register information on the status of women's empowerment at their companies in the "Database of Companies Promoting Women's Participation and Advancement in the Workplace" established by the Ministry of Health, Labor and Welfare.

Promoting Information Security Measures

Based on the “Cybersecurity Management Guidelines” issued by Japan's Ministry of Economy, Trade and Industry (METI) and the Information-technology Promotion Agency (IPA), the Fujitsu Group, along with its suppliers, has adopted the goal of “eliminating information security incidents”, and is continually implementing measures to prevent such incidents or recurrences. These measures include education, raising awareness, auditing and sharing information.
In recent years, there has been a significant increase in the commercial use of external services such as cloud computing and social media. There has also been a rapid increase in opportunities for the use of smart devices such as smartphones and tablet PCs. Regarding the risk of information leaks, it is necessary to prevent not only incorrectly addressed emails being sent by mistake and the theft or loss of PCs and smart devices, but also new kinds of risks such as in-house crimes and cyber terrorism. In this context, when the Fujitsu Group consigns work to suppliers, including those outside Japan, it promotes education and awareness by requiring the same standards of information security management and handling of personal information as it applies to its own operations. If any serious problem regarding information security is discovered at a supplier, or if the supplier fails to immediately implement corrective measures and no improvement is observed, Fujitsu will take steps such as reviewing its business relationship with the supplier.

Enhancing Supply Chain BCM

The Fujitsu Group sees the enhancement of Business Continuity Management (BCM) throughout its supply chain as essential to ensuring a stable supply of products and services in the event of major disasters or other unexpected contingencies. Accordingly, the Fujitsu Group is committed to continuously enhancing resilience throughout the entire supply chain.

As part of these efforts, we collaborate with suppliers to collect and consolidate site information and improve supply chain visibility. This enables rapid risk detection and impact assessment during disruptions, supporting early situational awareness, timely response and mitigation. We also utilize risk simulation tools to forecast potential impacts and work continuously with suppliers to strengthen resilience across the supply chain.

Communication with Suppliers

Feedback of Assessment Results in the Suppliers' Performance Review System

Under the Suppliers' Performance Review (*2) system, the Fujitsu Group evaluates and provides feedback to its major product-related and solutions development-related suppliers. Suppliers who do not meet Fujitsu’s standards are asked to make improvements.

- (*2) : Suppliers’ Performance Review: A program developed by Fujitsu that assesses the performance of procured goods and the basic profile of enterprises in terms of quality, technology, price, supply and CSR.

Building an Integrated Risk Management Platform

The Fujitsu Group is also working to improve its responses to information security risks, credit and compliance risks, and geopolitical risks, including those relating to sanctions. Under this policy, the Group is working to centrally consolidate and visualize supply chain risk information and resilience assessment data published by external organizations. We are integrating this information with data held by Fujitsu, including sales, production, procurement, and survey results. Fujitsu is building an integrated risk management platform (Third-Party Risk Management Platform) that comprehensively identifies and analyzes risks from multiple perspectives, and links them to timely response action, thereby strengthening governance across its supply chain.
Fujitsu intends to focus its efforts on leveraging advanced digital technologies to build a resilient supply chain capable of responding flexibly and promptly to changes in the external environment. In this way, we can contribute to ongoing value creation and help build a sustainable society.

Strengthening Procurement Compliance

Education by Procurement Divisions

Fujitsu Group conducts training programs for our procurement staff to disseminate awareness of sustainability and ensure that procurement is socially responsible. This training provides education in compliance and risk management (BCM activities), and includes topics such as sustainable procurement, green procurement, the Act on Proper Transactions with Small and Medium-Sized Entrusted Business Operators (Fair Transactions Act) and the Act on Securing the Proper Operation of Worker Dispatching Businesses and Protecting Dispatched Workers (Worker Dispatching Act).

Initiatives Related to the Fair Transactions Act and the Guidelines for Price Negotiations to Ensure Appropriate Transfer of Labor Costs

The entire Fujitsu Group makes every effort to maintain legal compliance in accordance with the Fujitsu Way Code of Conduct and Global Business Standards (GBS). The Fujitsu Group also provides company-wide education and training on the Fair Transactions Act and the guidelines for price negotiations to ensure appropriate transfer of labor costs

Announcement of "Declaration of Partnership Building"

Fujitsu has developed and announced its “Declaration of Partnership Building” in order to build new partnerships by promoting cooperation and coexistence with suppliers and value-creating businesses.
The Declaration of Partnership Building is an initiative introduced by the “Council for Promoting Partnership Building for the Future”, whose members include the Chairman of Japan Business Federation, the President of Chamber of Commerce and Industry, the President of the Japanese Trade Union Confederation, and relevant ministers (Minister of Economy, Trade and Industry, Minister of State for Special Missions (Minister of State for Economic and Fiscal Policy), Minister of Health, Labor and Welfare, Minister of Agriculture, Forestry and Fisheries, and Minister of Land, Infrastructure, Transport and Tourism).
Details of the Declaration of Partnership Building and Fujitsu's declaration are available on the portal site operated by the National Association of Small and Medium Enterprise Promotion Organizations.

- **Portal site: Declaration of Partnership Building (Japanese text only)**

Supplier Reporting Hotline

The Fujitsu Group receive reports from suppliers regarding any actions that are potential or actual instances of non-compliance in our purchasing activities. Channels have been set up both internally and externally through which we can verify and investigate the facts of each report and respond quickly.
Fujitsu's internal reporting standards prohibit any adverse treatment of its own staff making such reports or of staff from suppliers making the reports.
Our agreements with suppliers also include explicit provisions on the elimination of anti-social forces and other such groups with the aim of preventing harmful actions by such anti-social forces (and avoiding any encouragement of their activities).
The Fujitsu Group, including its suppliers, will have no relationship whatsoever with anti-social forces.

- **Supplier Compliance Line (Japanese text only)**

Participation in and Promotion of Industry Standard Initiatives

The Fujitsu Group is a member of the Responsible Business Alliance (RBA), an international alliance dedicated to responsible business conduct. Fujitsu respects the RBA Code of Conduct and works collaboratively with suppliers to promote sustainable procurement in its supply chain.
Fujitsu also actively participates and collaborates in international initiatives such as the Partnership for Carbon Transparency (PACT), led by the Japan Electronics and Information Technology Industries Association (JEITA) and the World Business Council for Sustainable Development (WBCSD). Through these activities, Fujitsu promotes efforts to address environmental and social issues across its entire supply chain, together with initiatives designed to visualize and reduce GHG emissions throughout the lifecycle of its products and services. We also work to advance and promote sustainable procurement practices more widely across the industry as a whole.

FY2025 Performance

Obtaining Agreement to the Procurement Policy

- Obtained written agreement to the Fujitsu Group Sustainable Procurement Policy from 692 suppliers.

Sustainability Surveys

- Sustainability survey responses received from major suppliers in Japan and overseas (including Fujitsu Group companies): 1,240 companies
  For suppliers that failed to meet the required standards, Fujitsu provided corrective support through supplier engagement. For service providers where risks were identified, Fujitsu conducted bilateral audits to confirm the presence or absence of issues and responded by focusing on supporting the establishment and improvement of fundamental management systems. Gradually, Fujitsu considers measures that include third-party audits and promotes staged corrective and improvement measures based on the level of risk and the characteristics of the business relationship.

【FY2025 Sustainability survey – Number of responding companies】

Japan	602 companies
Overseas	638 companies

【FY2025 Domestic supplier risk assessment results】

High	5%
Medium	56%
Low	28%

High-Risk Mineral Survey Results

- Responses received from 61.1% of suppliers surveyed
- Smelters operated by 804 companies were checked; of those, 338 companies were compliant with the RMI-certified Responsible Minerals Assurance Process (RMAP).

Implementing GHG Emissions Reductions in the Supply Chain

- We completed the setting of emissions reduction targets for 80% of our suppliers based on their FY2022 emissions volume.

Ensuring Diversity in the Supply Chain

- We requested suppliers with head offices in Japan, which accounted for 80% of procurement value in FY2022, to register their targets in the “Database of Companies Promoting Women's Participation and Advancement in the Workplace” (333 companies already registered).
- We also achieved procurement KPIs in overseas subsidiaries from companies with a diverse set of attributes (eg, SMEs, women-owned/led businesses, minority-owned businesses)

Promoting Information Security Measures

- Voluntary status inspections of information security measures were conducted (November 2025): 2,321 companies

Communication with Suppliers

- Held business policy briefings for suppliers to share procurement policies and business strategies, and requested action be taken to address security and compliance risks. 328 companies participated.
- Held online sessions for suppliers where the relevant executives explained Fujitsu's policies and initiatives relating to sustainability management and human capital management. The suppliers present were encouraged to accelerate their own efforts in the areas of human rights and employee well-being. Around 400 companies participated.

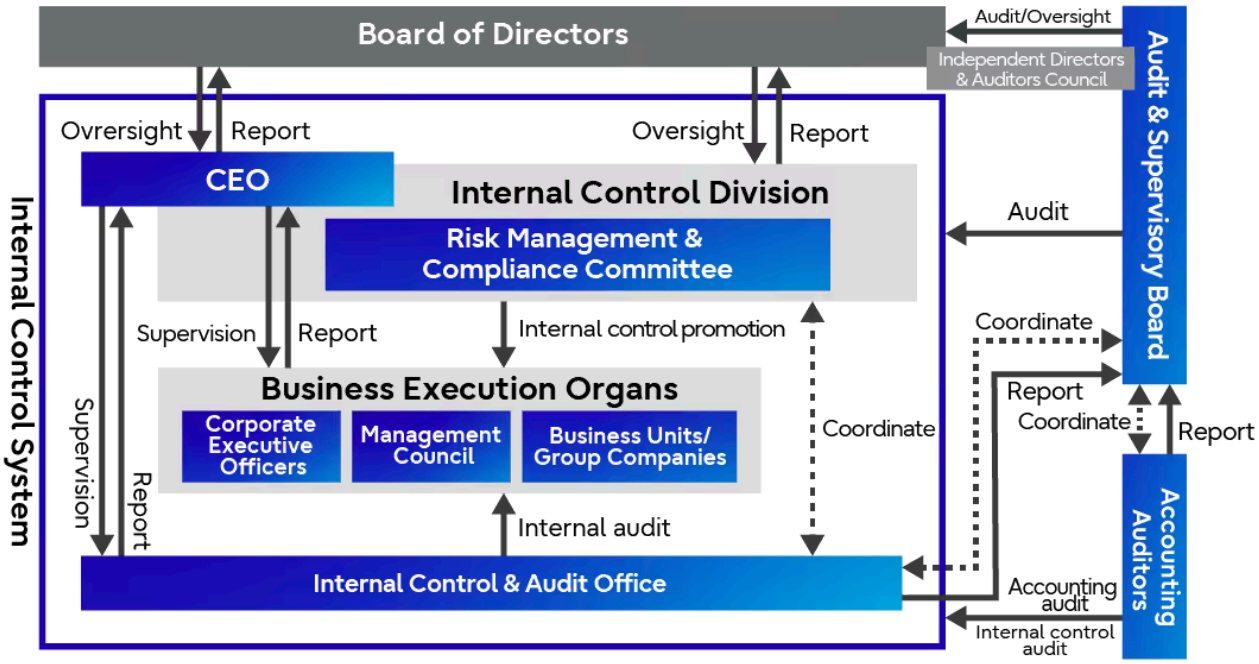
Strengthening Procurement Compliance

- Held sessions for global procurement staff to share procurement-related issues and initiatives.

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, 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 significant risks of the Fujitsu Group
  The Risk Management & Compliance Committee Secretariat (Corporate Risk Management Office, Second line) identifies and reviews the 16 significant risks considered important to the Fujitsu Group, taking into account environmental changes affecting the Group. Risk scenarios are defined for each significant risk, and they are classified into pure risk and management risk.
- Assignment of risk management departments (Second line)
  A risk management department is assigned to each significant risk, and is responsible for maintaining control over that specific risk.
- Evaluation of risks to the Fujitsu Group
  Each month, the risk management departments, Business Units, and Group companies evaluate the impact of each significant risk, the likelihood of its occurrence, and the status of mitigation measures.
- Ranking and mapping of significant risks
  Based on the evaluation results of the Group, we rank significant risks and create risk maps to visualize their significance. By plotting to four quadrants on a risk map, significant risks are evaluated across four levels (avoid, transfer, reduce, hold). From these evaluation results and status of materialized risks, their significance is evaluated and critical risks for that financial year are identified.
- Reports to the Risk Management & Compliance Committee and Board of Directors
  Analyses are conducted based on the evaluation findings, and mitigation policies are discussed and determined to address critical risks and significant risks to the Group.
- Issues corrective guidance and improvement instructions to Business Units and Group companies
  Based on the evaluation results for the Group, feedback is provided to Business Units and Group companies on an ongoing basis, advising them on improvements.
- Risk monitoring within Business Units and Group companies

Monthly risk monitoring is conducted 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 apply those rules promptly when risks materialize, based on risk management standards and the rules for escalating risks to the Risk Management & Compliance Committee.
- Analyze risks and deploy mitigation measures, while reporting to the Board of Directors as necessary, to prevent recurrence.

By cycling through this risk management process and having the risk management departments, Business Units and Group companies monitor it each month, we aim to reduce risks across the Fujitsu Group and to minimize the impact when risks materialize.

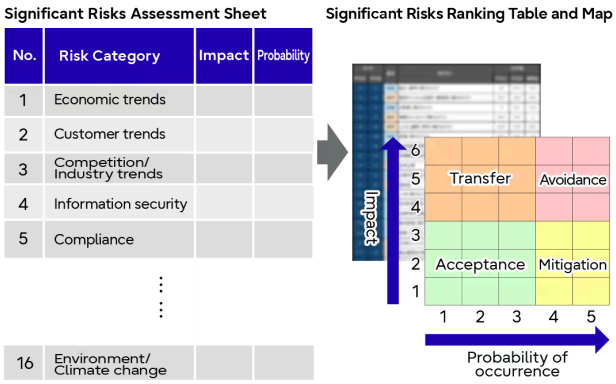
Critical risks

Considering the findings from evaluations conducted in the Potential Risk Management Process and the status of materialized risks, we have chosen to focus on critical risks based on their impact on achieving the Fujitsu Group's business strategies and goals. Consequently, we have identified the following two significant risks as critical risks for FY2026:

- Security risks
- Deficiencies or flaws in products and services



Risk management process



Visualization of significant risks

Significant risks to the Fujitsu Group (*1)

- 1. Security risks (Pure risk)
- 2. Deficiencies or flaws in products and services (Pure risk)
- 3. Risks of natural disasters and unforeseen incidents (Pure risk)
- 4. Human rights risks (Pure risk)
- 5. Compliance risks (Pure risk)
- 6. Financial risks (Management risk)
- 9. Risks related to competitors and industries (Management 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)

- **7. Risks related to the environment and climate change (Pure risk)**
- **8. Risks related to Fujitsu Group facilities and systems (Pure risk)**
- **14. Risks related to investment decisions and business restructuring (Management risk)**
- **15. Risks related to public regulations, public policies 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://global.fujitsu/ja-jp/ir/library/secreport**
- 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 to enhance the organization's risk responsiveness by improving its risk management skills.
Refer to the "FY2025 Performance" section for information on education outcomes for FY2025.

Group-wide disaster management

The basic policy of Fujitsu and its group companies inside 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. For activity outcomes for FY2025 refer to the "FY2025 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. These include events such as 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 and BCM in our supply chain, refer to the PDF listed below. For activity outcomes for FY2025, refer to the "FY2025 Performance" section.

- **[PDF] BCM activities**

FY2025 performance

Risk management education

Fujitsu Group new executive training: 44 people —

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

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: 648 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 110,000 people

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

Disaster Management Forum: 529 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 (December 2025, Organizational Training: 531 people; January 2026, Data Center Outage: 16 people): 547 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 globally will be enhanced by identifying issues through training and making continuous improvements.

Disaster management & BCM training

Fujitsu Group joint disaster response drills: FY2025 Drill - Eruption of Mt Fuji (widespread volcanic ash falls in the Greater Tokyo Metropolitan 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”, “Nankai Trough Megaquake” and “Eruption of Mt Fuji”.)

BCP Awareness Week —

An awareness training event centered on a hypothetical scenario involving the loss of 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 ensure continued improvement in 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."

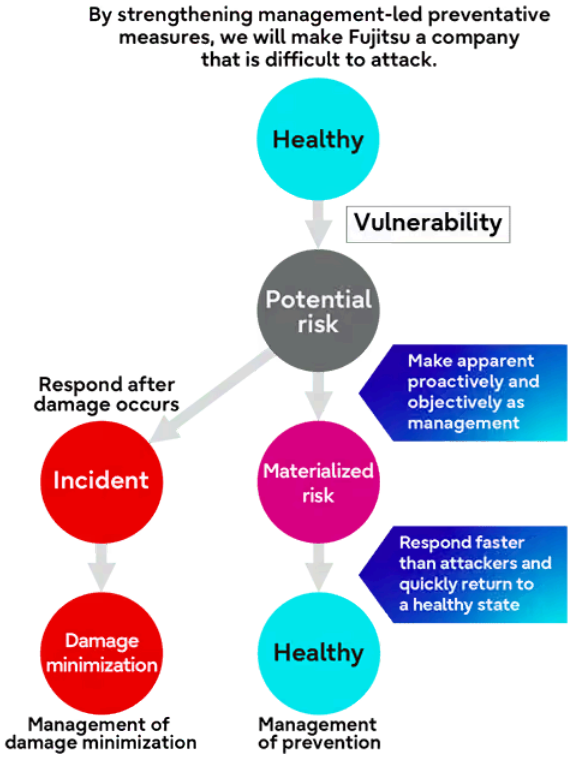
Approach to security management

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.
To achieve this, Fujitsu has established mechanisms to proactively identify potential risks by anticipating a wide range of risk scenarios. These mechanisms enable the comprehensive identification of potential risks and the determination of the field organizations responsible for addressing them. Identified risks are analyzed (e.g., attack difficulty) and assessed (e.g., likelihood and potential impact) to determine response strategies and priorities. For high-priority risks, the organization

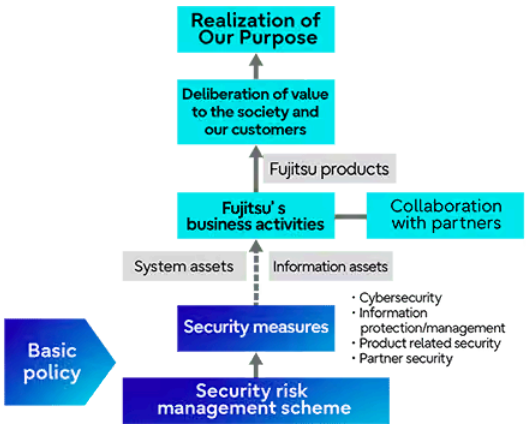
responsible for company-wide security control (CISO organization) under the CISO (Chief Information Security Officer) directly guides the relevant field organizations in implementing the necessary countermeasures.



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.



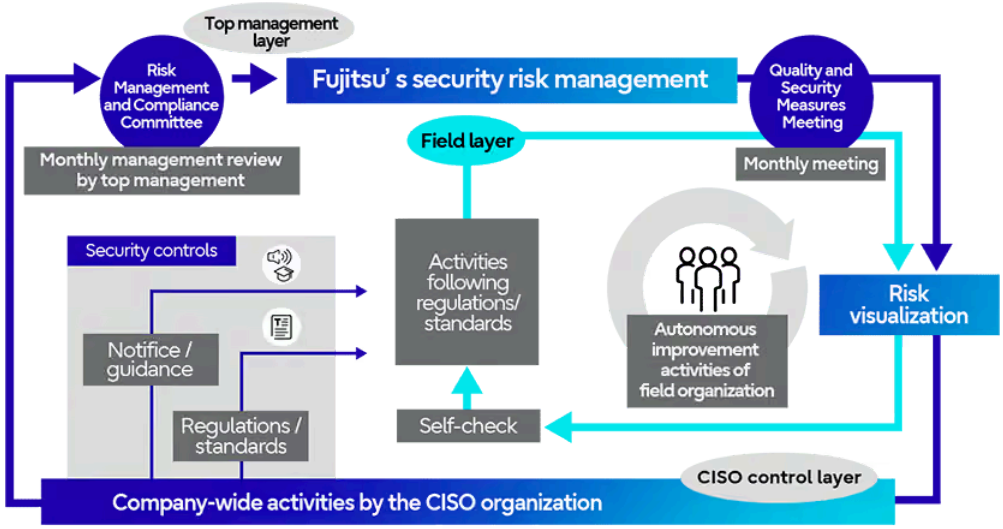
Security risk management to realize purpose

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>

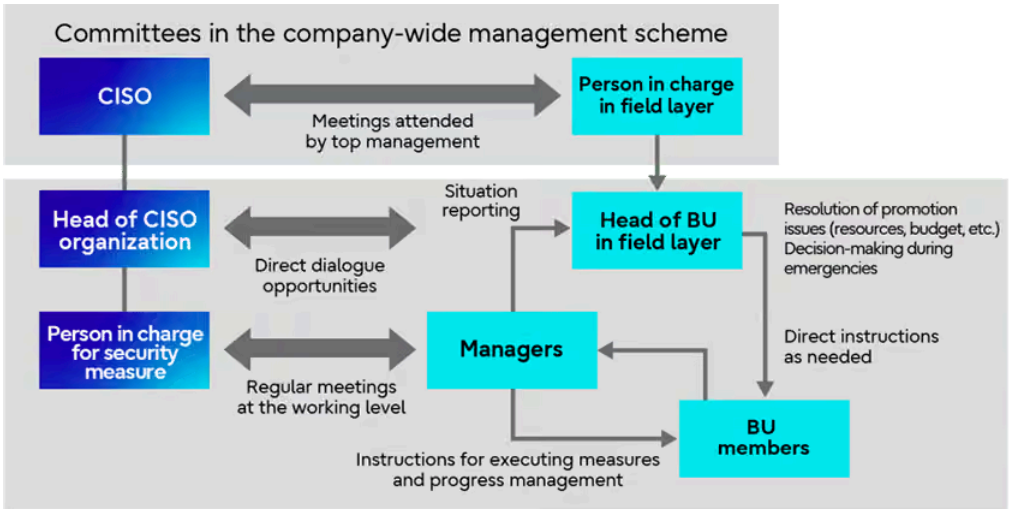
This scheme promotes company-wide security by fostering a shared understanding of risk status and the progress of security measures through two key meetings: the Risk Management and Compliance Committee, chaired by the CEO of the Fujitsu Group, and Regular Meetings on Quality and Security Measures, which 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.

Responsibility for implementing security measures has been incorporated into the duties of field organization heads, and 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 141 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.

- **Basic Policy on Fujitsu Group Information Security**

- (*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.

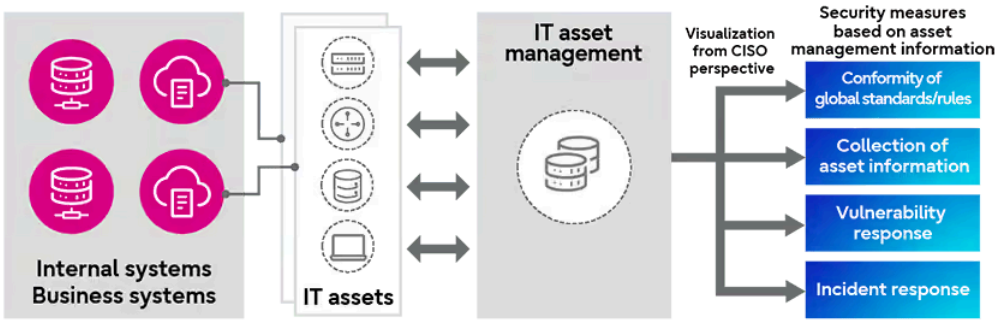
Cybersecurity measures

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>

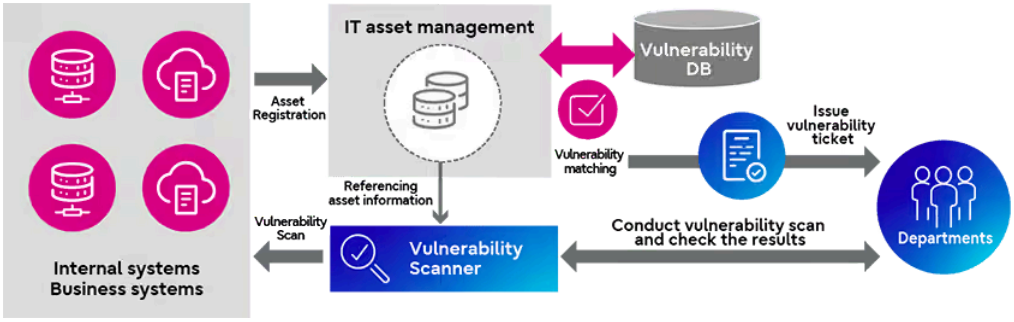
To support our customers' safe, secure, and sustainable business activities, we have centralized and visualized the IT asset management data of the IT systems (business systems) for our globally operating customers, as well as internal IT systems. This helps us promptly identify and remediate any security 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 establishing 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.

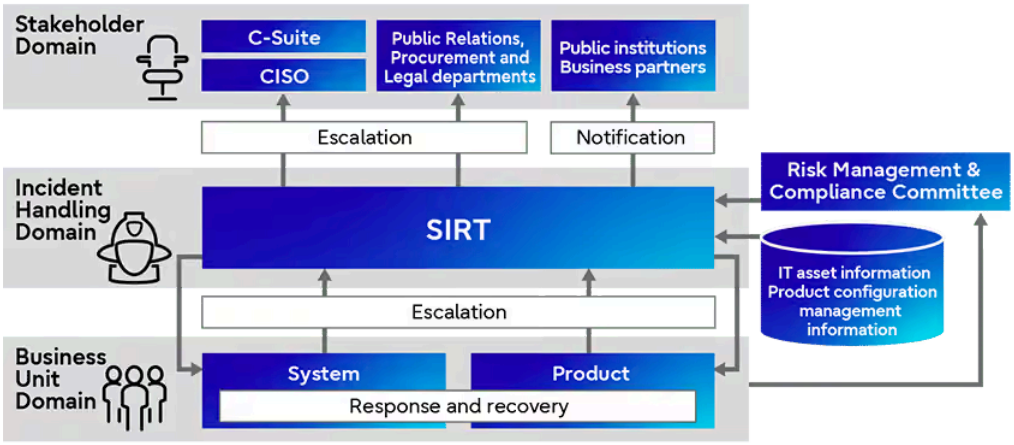
(1) Escalation
When a security incident is confirmed to have caused damage to the system managed by a department or to a personal terminal, the incident and the extent of the damage are assessed according to preestablished procedures, and immediate emergency measures to be carried out, while also escalating 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>

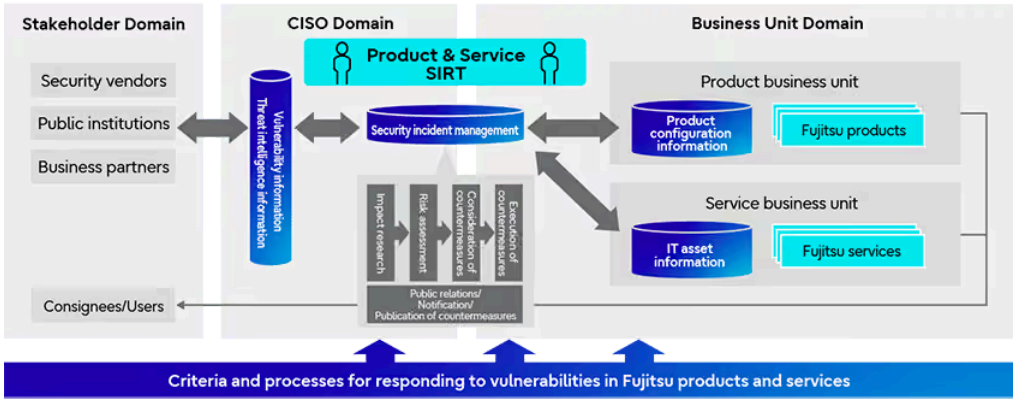
To protect customers who use Fujitsu's products and services, we centrally manage product configuration information, IT asset information, and threat intelligence information, which includes vulnerability information. In addition, to enable prompt and proactive response to risks arising from vulnerabilities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

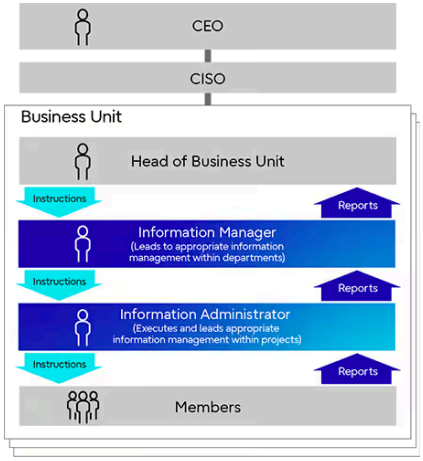
Fujitsu and its Group companies in Japan implemented the Information Protection Management System in order to appropriately protect confidential information (including personal information) of the Group and third parties. We also apply a PDCA cycle that covers from the "(1) Roles & Responsibilities" 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 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 Systems (7 Points)

<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) is provided at least once annually for all employees including executives. Information management training materials are also available to employees at any time.
(Ref) Number of participants in 2025 : 35,073

(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 2025-2026

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 (*8). In regard to the handling of personal information, we post and announce privacy policies on public websites in each country.

- (*8) 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 (*9) 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 FY2025.

- (*9) 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 FY2025, 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.

- **Third-party Evaluation and Certification**

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.

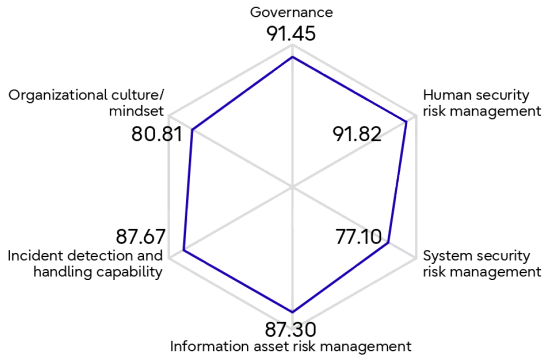
Visualization of organizational maturity

<Maturity monitor>

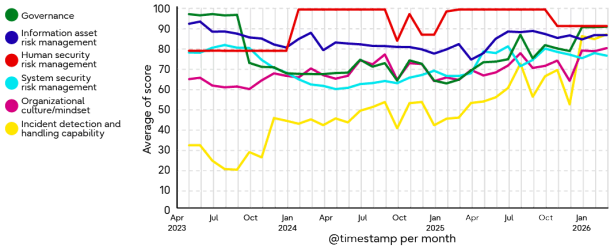
At Fujitsu, we digitally score factors such as the occurrence of vulnerabilities within organizations and the speed at which they are remediated, and visualize them as indicators of organizational maturity.
By visualizing the maturity level of each department at Fujitsu headquarters and Group companies 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 (*10), or Cybersecurity Capability Maturity Model, and SIM3 (*11), 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.

- (*10) C2M2: Cybersecurity Capability Maturity Model
- (*11) SIM3: Security Incident Management Maturity Model



Organizational maturity



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 April 2026)

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 cybersecurity 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 FY2025: 1 time company-wide training sessions, 1 time targeted e-mail training session

<Strengthening information security structure and human resource development>

In an effort to change employees’ mindsets and behavior regarding information security within the Fujitsu Group, the CISO and the CISO organization regularly disseminate information 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. The Fujitsu Global Quality Policy outlines our quality management system, standards for product and service quality, and controls by the quality management department. Each organization and Group company implements its structure and quality management system in accordance with these regulations.

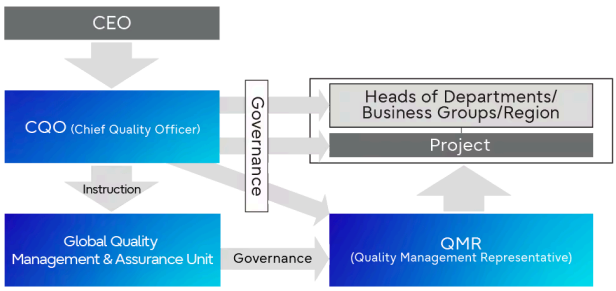


Fujitsu Global Quality Policy / Quality Standards System

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.

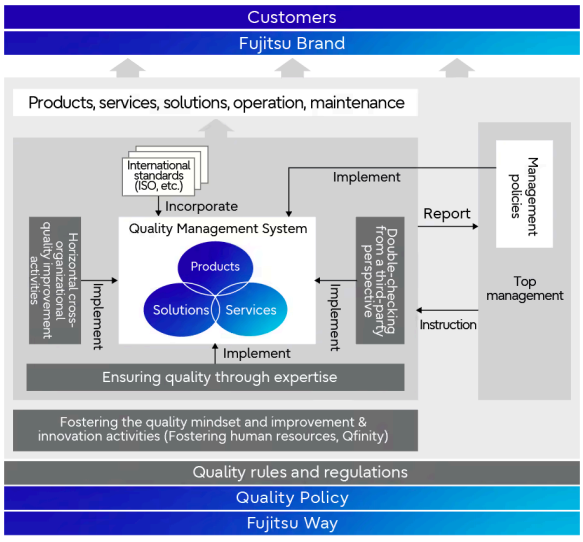


Our quality management structure

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.

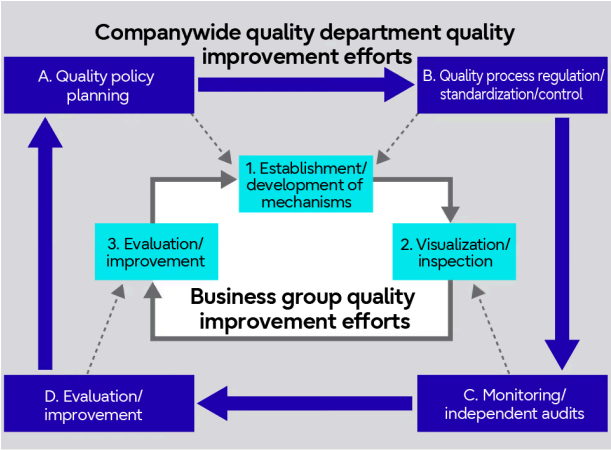
This is why we built our Quality Management System (QMS): to coordinate among these business units as appropriate for the product or service. Our QMS periodically verifies the progress in light of international certification standards such as the ISO in the aim of achieving process improvements to realize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

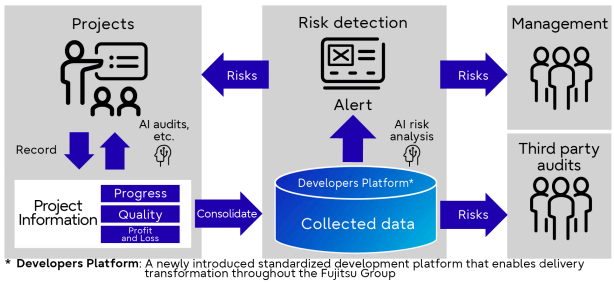
- (*1) Qfinity :
  Qfinity, an internal branding term which combines the words “quality” and “infinity,” represents the DNA of the Fujitsu Group: the “infinite pursuit of quality by each and every employee.” Qfinity is an improvement and innovation activity launched throughout the Fujitsu Group in FY 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.
Amid the shift to AI-powered development and increasing complexity of information systems, 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.
We aim to improve the project success rate by using AI to identify potential future risks based on this accumulated data and urging the teams to plan and implement countermeasures. Additionally, extraction and visualization of risks from quality data obtained in daily activities leads to self-directed improvements, as project members in the field notice risks by themselves.
We have taught the previous experiences and knowledge of our third-party audit department to AI, enabling AI audits that can analyze project status from a third-party audit perspective and present risks and proposed countermeasures. Project results can be checked anytime, anywhere, and as many times needed, and the AI is used by many projects as a readily accessible advisor, evolving into a more accurate and efficient tool that supports the improvement of project quality. Furthermore, we are working to establish a quality assurance process based on AI-driven development, aiming to achieve both quality assurance and increased development speed when AI is used in each phase of development.



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

Mechanism for objectively assessing field decisions

< Quality assurance processes that support service delivery >

To provide customers with higher value than ever before and ensure stable system operation, we have changed to the "One Delivery" project structure—one that is not organization-dependent. We are further upgrading our delivery functions through the continuous consolidation and optimization of our delivery system. "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

Value creation for customers and stable system operation



One Delivery Quality Assurance Process

stage those projects with potential troubles.
Through the “One Delivery Quality Assurance Process,” the entire Fujitsu Group provides higher quality services with greater stability.