Management Systems

The Fujitsu Group seeks the continued improvement of its corporate values, and carries out business management in which each function and position are made clear in the value creation process.

Corporate Governance

Basic Stance on Corporate Governance

As a resolution of the Board of Directors meeting held in December 2015, Fujitsu established the " Corporate Governance Policy" to define the company's basic stance on corporate governanace. The policy set out a framework of Fujitsu's corporate governance structure as follows;

Structural framework

The company outlines the following rules to ensure the effective oversight and advice from a diverse perspective of Non-Executive Directors (hereinafter, the term used for the combination of Independent Directors and Non-Executive Directors appointed from within the company) to Executive Directors on their business execution as part of the Board of Directors function while taking advantage of the company with the Audit & Supervisory Board system:

a Same number or more Non-Executive Directors responsible for oversight are appointed as Executive Directors responsible for business execution.

b Independent Directors are appointed as the core members of Non-Executive Directors, and at least one Non-Executive Director is appointed from within the company.

c Independent Directors must meet the independence standards (hereinafter referred to as "Independence Standards") established by the company.

d In nominating Non-Executive Director candidates, the company takes account of the background of candidates and their insight on the company's business.

e The company has the Audit & Supervisory Board Members' external audit and oversight on the Board of Directors, the voluntary Executive Nomination Committee and Compensation Committee composed mainly of Non-Executive Directors and Auditors (hereinafter, the term used for the combination of Non-Executive Directors and Audit & Supervisory Board Members), and the Independent Directors & Auditors Council, all function to complement the Board of Directors.

f Independent Audit & Supervisory Board Members shall be the External Audit & Supervisory Board Members who meet the Independence Standards.

・Corporate Governance Policy and Independence Standards for External Directors & Auditors
http://pr.fujitsu.com/jp/ir/governance/governancereport-b-en.pdf

Overview of Corporate Governance Structure (as of June 26,2017)

Overview of 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 oversight function of the Board of Directors has been strengthened by actively appointing External Directors with high independence and diverse perspective.

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.

The Board of Directors is comprised of 10 members in total: 4 Executive Directors and 6 Non-Executive Directors (including 4 External Directors and two of them are women).

Overview of the Audit & Supervisory Board

The Company has an Audit & Supervisory Board that performs the auditing and oversight functions. The auditing and oversight functions are carried out by Audit & Supervisory Board Members, who review the Board of Directors as well as business execution functions and attend important meetings, including meetings of the Board of Directors.

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

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 to ensure the transparency and objectivity of its process for nominating Directors and Audit & Supervisory Board Members and its process for determining executive compensation as well as to ensure the fairness of the method and level of executive compensation.

The Executive Nomination Committee deliberates about candidates for Director and Audit & Supervisory Board Member positions in accordance with the Framework of Corporate Governance Structure and the Procedures and Policy of Directors and Auditors Nomination stipulated in the Company's Corporate Governance Policy and provides its recommendations to the Board of Directors. In addition, the Compensation Committee provides its recommendations about the level of base compensation and the method for calculating performance-based compensation to the Board of Directors in accordance with the Procedures and Policy of Determining Directors and Auditors Compensation stipulated in the Company's Corporate Governance Policy.

According to the Corporate Governance Policy, each committee is composed of a majority of Non-Executive Directors and Auditors with at least one Independent Director. In fiscal 2016, each committee consists of three Non-Executive Directors and Auditors (including two Independent Director) and one Executive Director. Both Committee's members in fiscal 2016 are as follows.

Chairman of both Committees: Tatsuzumi Furukawa
Members of both Committees: Jun Yokota Masami Yamamoto, and Chiaki Mukai

The FY 2016 term of the above committee members ended at the close of the regular Annual Shareholders’ Meeting on June 26 2017. Appointment of members of the committees for fiscal 2017 is scheduled for July 2017.

Independent Directors & Auditors Council

Fujitsu established this council as part of its initiative to strengthen its growth-oriented governance, which serves to improve profitability over a medium- to long-term horizon. The Independent Directors & Auditors Council is comprised of all independent officers (including four External Directors and three External Audit & Supervisory Board Members).

To invigorate discussions on the medium- to long-term direction of the Company at its Board of Directors Meetings, Fujitsu established the council to enable Independent Directors & Auditors, who maintain a certain degree of separation from the execution of business activities, to consistently gain a deeper understanding of Fujitsu’s business. In the Independent Directors & Auditors Council, members share information and exchange viewpoints so that they can each formulate their own opinions.

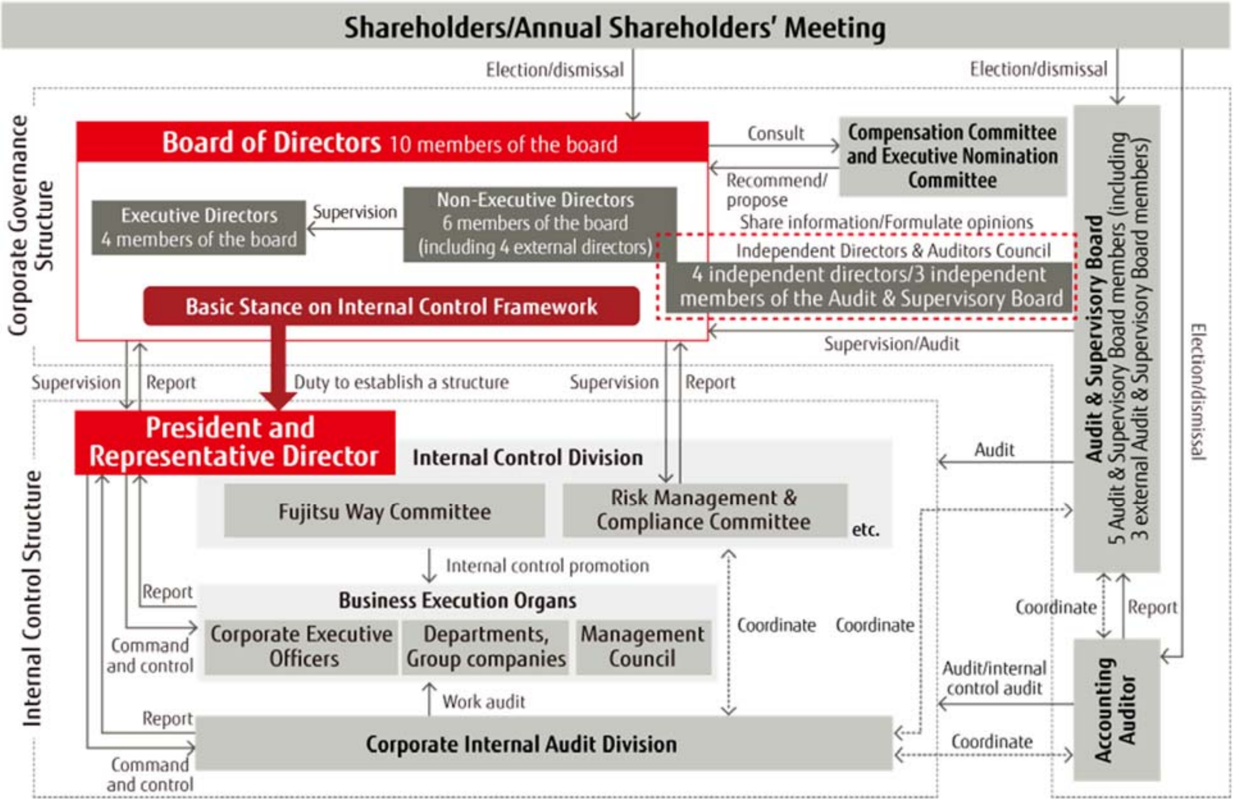
Reasons for Adoption of Current Corporate Governance System

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.

The Board of Directors comprises same number or more Non-Executive Directors as Executive Directors to ensure its capacity to correct faulty, insufficient, or excessive business executions. While External Directors should be the core of Non-Executive Directors on account of their high independence, at least one Non-Executive Director is appointed from within the company to complement the External Directors’ knowledge in the business fields and the corporate culture of the company so that the efficiency of oversight performance by the Non-Executive Directors are enhanced.

Corporate Governance Structure

(as of June 26, 2017)


Shareholders/Annual Shareholders' Meeting
Election/dismissal
Election/dismissal
Corporate Governance Structure
Board of Directors 10 members of the board
Executive Directors
4 members of the board
Supervision
Non-Executive Directors
6 members of the board
(including 4 external directors)
Basic Stance on Internal Control Framework
Consult
Compensation Committee and Executive Nomination Committee
Recommend/propose
Share information/Formulate opinions
Independent Directors & Auditors Council
4 independent directors/3 independent members of the Audit & Supervisory Board
Supervision/Audit
Audit & Supervisory Board
5 Audit & Supervisory Board members (including 3 external Audit & Supervisory Board members)
Election/dismissal
Supervision
Report
Duty to establish a structure
Supervision
Report
Internal Control Structure
President and Representative Director
Internal Control Division
Fujitsu Way Committee
Risk Management & Compliance Committee
etc.
Audit
Internal control promotion
Report
Business Execution Organs
Command and control
Corporate Executive Officers
Departments, Group companies
Management Council
Coordinate
Coordinate
Coordinate
Report
Audit/internal control audit
Accounting Auditor
Work audit
Report
Command and control
Corporate Internal Audit Division
Coordinate

Policy on the Determination of Executive Compensation

Compensation of Directors and Audit & Supervisory Board Members is determined in accordance with the Executive Compensation Policy below, which was determined by the Board of Directors following the recommendation by the Compensation Committee.

[Reference] Executive Compensation Policy

To secure exceptional human resources required to manage the Fujitsu Group as a global ICT company, and to further strengthen the link between its financial performance and shareholder value, while at the same time improving its transparency, Fujitsu establishes its Executive Compensation Policy as follows.

Executive compensation is comprised of the following: "Base Compensation," specifically a fixed monthly salary in accordance with position and responsibilities; "Performance-based Stock Compensation," which is a long-term incentive that emphasizes a connection to shareholder value; and "Bonuses" that are compensation linked to short-term business performance.

Basic Compensation

Base compensation is paid to all Directors and Audit & Supervisory Board Members. A fixed monthly amount shall be determined for each executive in accordance with the position and responsibilities of each executive.

Bonuses

- Bonuses shall be paid to Directors who carry out executive responsibilities. The amount of a bonus shall reflect business performance in the respective fiscal year.
- As a specific method for calculating a bonus, Fujitsu shall adopt an "On Target model" that uses consolidated revenue and consolidated operating profit as indices and the amount shall be determined in accordance with the degree of achievement of the performance targets for the respective fiscal year.

Performance-based Stock Compensation

- Performance-based stock compensation shall be granted to Directors who carry out executive responsibilities,in order to share the profit with shareholders and as an incentive to contribute to enhancement of medium- tolong-term performance.
- A base number of shares in accordance with respective rank, performance judging period (three years) and mid- to long-term performance targets in terms of consolidated sales revenue and consolidated operating profit, and coefficient according to performance achievement level vis-à-vis the mid- to long-term performance targets shall be set in advance. The number of shares to be allocated for each fiscal year shall be calculated by multiplying the base number of shares and the coefficient according to the performance achievement level, and the total number of shares calculated shall be allocated upon completion of the performance evaluation period.

In accordance with the resolution of the Annual Shareholders' Meeting, the total amount of Base Compensation and Bonuses (monetary compensation) for Directors shall not exceed 600 million yen per year, Performance-linked Compensation (non-monetary compensation) shall not exceed 300 million yen per year, and the total number of shares to be allocated shall not exceed 430,000 shares per year. The Base Compensation for Audit & Supervisory Board Members shall not exceed 150 million yen per year.

(Reference) Types of Executive Compensation and Eligibility

Category	Basic Compensation		Bonuses	Performance-based Stock Compensation
	Management Oversight Portion	Business Execution Portion		
Directors	○	–	–	–
Executive Directors	○	○	○	○
Audit & Supervisory Board Members	○		–	–

Basic Stance on 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, Fujitsu is working toward the practice and penetration of the FUJITSU Way, the basic principles behind the Fujitsu Group's conduct. At the same time, the Board of Directors has articulated the Policy on Internal Control Framework as systems and rules to pursue management efficiency and control the risks arising from the Company's business activities.

Overview of the Policy on the Internal Control System

The Policy on the Internal Control System sets forth internal structures of the Fujitsu Group, including the following.

Decision-making and Structure of Management Execution

By dividing the management execution authority of the President & Representative Director, who is the chief executive officer, among the corporate executive officers, and by establishing a Management Council to assist in the President and Representative Director's decision-making, the Company aims to enhance management effectiveness.

In addition, the framework makes clear that the President & Representative Director bears responsibility for the construction and operation of an internal control framework, and the Board of Directors shall fulfill its oversight responsibility by appropriately examining the operation of the internal control framework.

Risk Management System

The Company shall establish a Risk Management & Compliance Committee, and in addition to preparing systems to control the overall risk of financial losses of the Fujitsu Group, the Company shall also prepare systems for managing risks pertaining to defects and failures in products and services, as well as systems for managing contracted development projects, information security, and financial risk.

Compliance System

Primarily through the Risk & Management Compliance Committee, the Company shall promote the preparation of the internal rules, education, and oversight systems required for compliance with the Code of Conduct set forth by the FUJITSU Way, and also with laws and regulations concerning the business activities of the Fujitsu Group.

The Company shall also prepare management systems to ensure the appropriateness of financial reporting, as well as systems for information disclosure and internal auditing.

・The Policy on the Internal Control System and the Overview of the Status of Operation of the System
http://www.fujitsu.com/global/Images/notice117b.pdf

Overview of the Status of Operation of the System to Ensure the Properness of Fujitsu Group Operations

1. Systems to Ensure that Directors Carry Out Their Responsibilities Efficiently

The Company delegates management execution authority of the President and Representative Director to Corporate Executive Officers in order to ensure the efficiency of decision-making and management execution.

The Management Council, in principle, meets three times a month, discusses important management execution and assists the President and Representative Director in decision-making.

In addition, rules for delegation of duties and various systems for approvals and reaching decisions are put in place and are operated so that efficient and proper management execution is ensured based on these rules and systems.

2. Risk Management System and Compliance System

The Company positions the risk management system and the compliance system at the heart of the "Policy on the Internal Control System" and has established the Risk Management & Compliance Committee(the "Committee"), which supervises these systems globally and reports to the Board of Directors.

The Committee is chaired by the Representative Director and President and consistsmainly of Executive Directors. The Committee meets periodically and determines policies for preventing risks in business operations from arising and for countermeasures for losses caused by risks that have arisen.

The chairman of the Committee has appointed a Chief Risk Compliance Officer (CRCO) who executes the Committee's decisions.

Regarding compliance violations and risks in business operations, including information security, the Committee has established and operates a system that covers not only the Company but the Fujitsu Group and ensures reporting to the Committee in a timely manner. It also operates the internal reporting system.

The Company has appointed a Chief Information Security Officer (CISO) under the Committee and formulates and implements information security measures. In addition, the Company has established the Cyber Security Committee under the Committee. While ensuring security throughout the Fujitsu Group, the Company is working to ensure and enhance information security of customers through products and services that embody Fujitsu's security practices.

In the course of operating the systems described above, besides reporting when risk shave arisen, the Committee periodically reports the progress and results of its activities tothe Board of Directors and is supervised.Immediately after the violation of the Antimonopoly Act concerning transactions withTokyo Electric Power Co., Ltd. came to light, the Company established a special compliance investigation committee and conducted a thorough investigation of the compliance violation. This was one of the extraordinary measures implemented by the Committee under the supervision of the Board of Directors.

3. System to Ensure Proper Financial Reporting

As for a system to ensure proper financial reporting, the Company has established the FUJITSU Way Committee. Under this committee chaired by the Representative Director and President and consisting of Executive Directors and some Corporate Executive Officers.

Under this committee's direction, the responsible organization has established a system called "Eagle Innovation." In accordance with the rules established by the Company based on the principles of the Practice Standards for Management Assessment and Audit concerning Internal Control Over Financial Reporting published by the Business Accounting Council, internal control over financial reporting throughout the Fujitsu Group is assessed.

4. System to Ensure the Properness of Fujitsu Group Operations

The risk management system, the compliance system, and the system for ensuring proper financial reporting cover the Fujitsu Group.

Especially for risk management and compliance systems, Regional Risk Management &Compliance Committees have been established for individual Regions, which are geographical executive divisions of the Fujitsu Group worldwide. These regional committees are positioned under the Risk Management & Compliance Committee to function so that the entire Fujitsu Group is covered.

In addition, as a part of a system to ensure the properness of Fujitsu Group operations, the Company has established the Rules for Delegation of Authority called "Global DoA" that determines authority for decision-making of important matters of Fujitsu Group companies (excluding certain subsidiaries) and the decision-making process. The Company has its Group companies comply with the Global DoA. In addition, Group companies are required to report on their operations to the Company. In this way, the Company has put in place systems for decision-making and reporting of important matters at the Group.

The status of operation of the internal control system centering on the above is periodically reported to the Board of Directors.

・Corporate Governance Report (As of June 27, 2017)
http://pr.fujitsu.com/jp/ir/governance/governancereport-en.pdf

Compliance

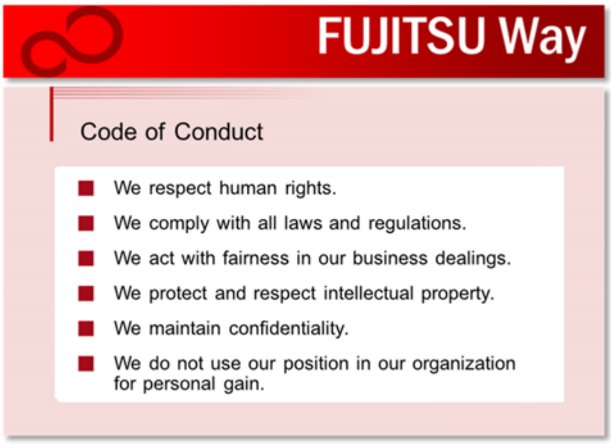
Activities Promoting Compliance

The Risk Management & Compliance Committee, directly reporting to the Board of Directors and headed by the President, supervises compliance matters globally for the entire Fujitsu Group, in accordance with our Basic Policy on Establishment of Internal Control System.The Risk Management & Compliance Committee is responsible for and has appointed a Chief Risk Management & Compliance Officer (CRCO) who executes the committee’s decisions concerning compliance and also works to raise awareness of and compliance with our Fujitsu Way Code of Conduct throughout the Group by establishing the Global Compliance Program and coordinate with the Region Risk Management & Compliance Committee set up in each region as a lower committee.

The Risk Management & Compliance Committee and the Region Risk Management & Compliance Committees monitor the implementation status of the Global Compliance Program on a periodical basis and report to the Board of Directors.

The Fujitsu Way Code of Conduct

The Fujitsu Way includes the following Code of Conduct, with which all Fujitsu Group employees must comply:



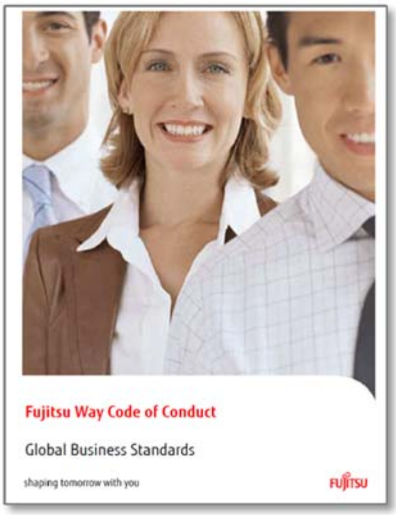
FUJITSU Way

Code of Conduct

- We respect human rights.
- We comply with all laws and regulations.
- We act with fairness in our business dealings.
- We protect and respect intellectual property.
- We maintain confidentiality.
- We do not use our position in our organization for personal gain.

Fujitsu has also rolled out our Global Business Standards (GBS), which provides further guidance on how to apply the Fujitsu Way Code of Conduct and to ensure compliance with laws and regulations. The GBS is available in 20 languages to be applied uniformly across the Fujitsu Group.

・GBS (Global Business Standards)
http://www.fujitsu.com/global/about/philosophy/codeofconduct/gbs/index.html



Fujitsu Way Code of Conduct

Global Business Standards

shaping tomorrow with you

Initiatives by Top Management

Through messages from top management to employees as well as other regular communication regarding our commitment to compliance, Fujitsu is working to promote our Code of Conduct and GBS across the Fujitsu Group.

In FY2016, Fujitsu's President sent repeated messages to all employees in Japan after the competition matter in connection with the sale of communication equipment to electric power companies, declaring again our determination to break away from compliance breach, including bid rigging and cartel. Other executives in the executives in the management also worked to embed a culture of compliance by visiting sales offices in Japan and explaining the importance of compliance to employees directly.

In overseas Group companies, the region heads and the top management are continuously sending messages to their employees, explaining our corporate culture of "Zero Tolerance". For example, on December 9, 2016, four overseas regions coordinated messaging declaring Fujitsu's support of the United Nation's "International Anti-corruption Day".

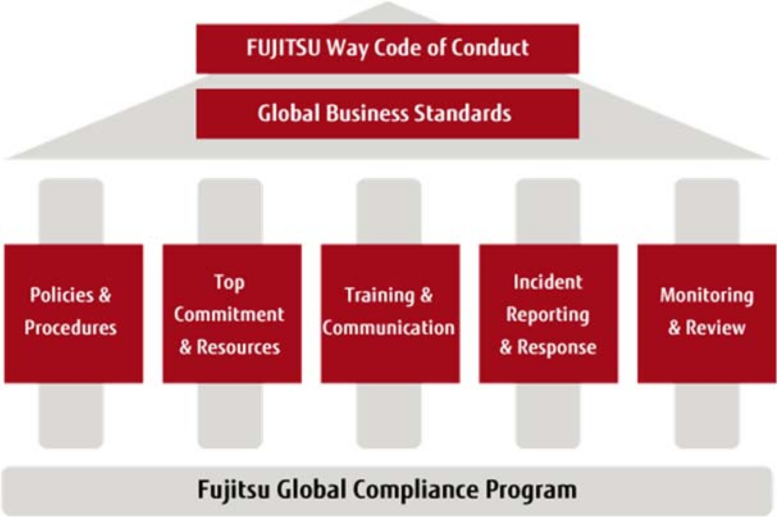
Promoting the Global Compliance Program

In order to promote and implement the Fujitsu Way Code of Conduct and GBS, Fujitsu has established the Global Compliance Program (GCP) and is working to maintain, review and improve its global structure for legal compliance across the Fujitsu Group.

The GCP systematically organizes our existing activities concerning compliance into five pillars, clarifies items that Fujitsu should continuously work on, and seeks to promote external understanding of our compliance structure and activities.

Various measures and approaches are taken in each region based on the GCP, as well as local laws and government guidelines.

Fujitsu Global Compliance Program


FUJITSU Way Code of Conduct
Global Business Standards
Policies & Procedures
Top Commitment & Resources
Training & Communication
Incident Reporting & Response
Monitoring & Review
Fujitsu Global Compliance Program

1. Establishment of Rules and Procedures

The Fujitsu Group has established and implemented various internal rules to align globally with the GBS.

In Japan, to enforce compliance and enact sustainable improvement in our corporate value, we established the Compliance Policy with the approval of the Risk Management & Compliance Committee, and have applied the rule throughout domestic group companies. We established more specific and detailed regulations and guidelines based on the Compliance Policy in the areas with significant impact on business: antitrust, anticorruption and anti-social forces. In our overseas entities, with the approval of the Risk Management & Compliance Committee, we have been establishing basic internal rules that are the minimum requirements to be globally implemented within each entity. These rules are organized in the form of global guidelines, which are in turn adopted by our overseas Group companies, allowing them to take into account the applicable laws, culture, and customs of each country. We issued the General Compliance Guideline, corresponding to the Compliance Policy in Japan above, for overseas Group companies, along with a global guideline on competition law, and other guidelines concerning the prevention of bribery, covering matters including the proper procedures for giving gifts and entertainment to government officials, due diligence on third party suppliers, and facilitation payments. In addition, we have developed an online third party due diligence process that is being used by major overseas Group companies in Europe, Asia, Oceania, and North America.

2. Top-level Commitment and Securing of Resources

As noted above, Fujitsu is working to promote and implement the Fujitsu Way Code of Conduct and GBS across the Fujitsu Group through messages from top management to employees and other regular communication of our commitment to compliance.

We have also assigned compliance officers to each region, Japan, EMEIA, Asia, Americas, and Oceania, and have formed a global network with local risk and compliance representatives, in order to secure a structure to execute our GCP.

The compliance representatives from overseas Group companies meet annually at the Global Compliance Forum to share and discuss headquarter's policies concerning the execution of GCP, as well as share their experiences in risk management and compliance. Also, the risk and compliance representatives in Fujitsu and domestic Group companies meet annually at the Risk and Compliance Seminar to share updates and knowhow related to risk management and compliance.

3. Training and Communication

To embed and implement the Fujitsu Way and GBS, Fujitsu Group conducts various compliance training and awareness raising activities for executives and employees. The Fujitsu Group has been printing the Code of Conduct of the Fujitsu Way on wallet-size cards and has been distributing these to Group employees. These cards are designed to serve as a quick reference of the Code of Conduct for employees when they are uncertain about a decision in the course of daily operations in dealing with customers and/or business partners.

INTERNAL USE ONLY

Japanese

FUJITSU Compliance Training
(Cartel/Bid-Rigging/Bribery)

December 2016
FUJITSU LIMITED
FUJITSU UNIVERSITY

Click [次へ] to continue with the learning course.

Learning Format

Fujitsu and domestic Group companies conduct compliance training for executives every year, which is provided by outside lawyers as well as Fujitsu's legal and compliance function. For new managers, we also regularly hold in-house training where a Fujitsu instructor explains the importance of the Code of Conduct and compliance, while also providing case studies of typical scenarios and situations.

In FY2016, Fujitsu and domestic Group companies provided an e-learning course called "Compliance of Fujitsu Group: Cartels/Bribes" for the employees (Target completion rate is 100 %. Completion rate of Fujitsu is 97% as of March 2017, and the domestic Group companies are still conducting the training.). Aimed to increase the effectiveness of the training by completely renewing the contents from the previous versions to include documentary drama that introduces Fujitsu's antitrust case referenced above. We also conducted a series of face-to-face training for over 3,700 employees of public sector business and other sales divisions.

For overseas Group companies, we also conduct compliance training based on the laws, custom and realities of business in each country and region. In FY2016, we provided e-learning courses on anti-trust/anti-competition and on the GBS. These courses were provided in 20 languages to 51 overseas Group companies. We also conduct face-to-face trainings for high-risk departments and entities. For example, we conducted anti-bribery training in South Korea following the enactment of a significant anti-bribery law in September 2016.

Going forward, we will continue to engage in these activities and conduct face-to-face training focused on prevention of cartel and bribery.

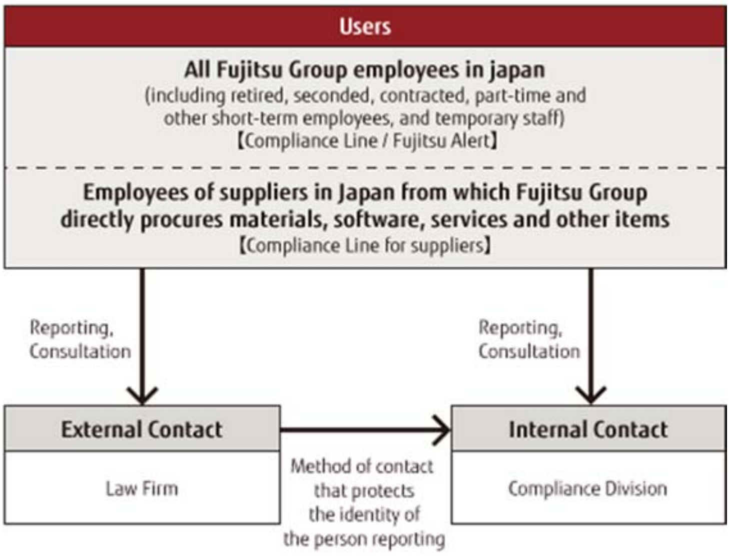
4. Incident Reporting and Response

(1) Whistleblowing Hotline

Fujitsu Group has been operating the Compliance Line/Fujitsu Alert for both internal and external reports. The Compliance Line/Fujitsu Alert handles reports and provides consultations for all employees in the Fujitsu Group (including retired, seconded, contracted, part-time or other short-term employees as well as temporary staff). Both domestic Group companies and overseas Group companies have established are operating internal reporting system. These reporting lines are made known to the employees via websites, posters and wallet-size cards with contact information. Reports are accepted in 20 languages, at any time, on any day.

Moreover, we opened a Compliance Line for Suppliers in Japan to handle reports and inquiries from the employees of companies that directly supply Fujitsu and domestic Group companies with their products, services or software, etc.

Our Compliance Line/ Fujitsu Alert and Compliance Line for Suppliers system forbids any and all retaliation against any individual or supplier who makes the report, and meticulous care is taken in handling the information so as to preserve their anonymity. If the issue raised is substantiated, the relevant practice is corrected and measures are taken to prevent recurrence.


Users
All Fujitsu Group employees in japan
(including retired, seconded, contracted, part-time and other short-term employees, and temporary staff)
【Compliance Line / Fujitsu Alert】
Employees of suppliers in Japan from which Fujitsu Group directly procures materials, software, services and other items
【Compliance Line for suppliers】
Reporting, Consultation
Reporting, Consultation
External Contact
Law Firm
Method of contact that protects the identity of the person reporting
Internal Contact
Compliance Division

(2) Report to the Risk Management & Compliance Committee

Our Risk Management Rule stipulates that the executive or the employee who recognizes a compliance violation or signs of violation must immediately report to compliance team, who will then report to the Risk Management & Compliance Committee and the Board of Directors if necessary, following the reporting structure set by the Head of Business Unit.

The status of key compliance issues is reported regularly to the Risk Management & Compliance Committee and the Board of Directors.

5. Monitoring and Assessment

Through activities such as risk assessments and audits, we periodically check the efficacy of the GCP and work to continually improve it.

Last fiscal year, Fujitsu started the review of audit plan in order to confirm observance of the Antimonopoly ACT, and we will continue to implement as a more effective audit program by incorporating opinions from the external experts going forward.

For overseas, Fujitsu headquarters' compliance team conducts risk assessments by visiting Group companies in countries and regions with a high risk of corruption, and through the interviews with executives and employees, as well as checks on internal policies and processes, the compliance team analyzes the potential compliance risks in local business and provides proposals and supports to mitigate these risks.

The outcome of all risk assessments and the status of the GCP implementation are reported regularly to the Risk Management & Compliance Committee, the Region Risk Management & Compliance Committees and the Board of Directors.

Response to Compliance Matters

In July 2016, Fujitsu Limited was found to have violated the Antimonopoly ACT concerning order coordination for equipment for electric power security communication for Tokyo Electric Power Co., Ltd.(TEPCO) and Fujitsu received an cease and desist order and a surcharge payment order. Subsequently, in February 2017, Fujitsu was found to have violated the Antimonopoly Act concerning transactions of hybrid optical communication equipment and transmission-path equipment for Chubu Electric Power Co., Inc.

Fujitsu's sales personnel in charge of Chubu Electric Power had already stopped engaging in order adjustment with other companies before the TEPCO case was detected. Following the detection of TEPCO case, Fujitsu swiftly conducted an internal investigation based on the resolution by the Board of Directors and found that similar order adjustment had been conducted with Chubu Eletric Power. Subsequently, having received approval by the Board of Directors, Fujitsu swiftly applied for immunity from or reduction of surcharge and received the above finding in February 2017.

Because of the timely application for immunity from or reduction of surcharge, Fujitsu was fully exempted from payment of the surcharge and was also not subject to a cease and desist order. Fujitsu deeply apologize for all the concerns that we have caused by letting this regretful incident occur.

Fujitsu has taken disciplinary action against the employees who took part in the violation, and given salary reduction to 7 executives including the Chairman and the President based on the resolution of the Board of Directors (10-30% of the monthly salary was reduced for 3 months).

Immediately following the detection of TEPCO case, the President swiftly declared that all bid rigging and cartel behavior will not be tolerated, and has sent repeated messages to all executives and employees. The executives in charge of business has also reminded employees of the intention to compliant. Additionally, Fujitsu has conducted compliance training as mentioned above to all executives, employees, and the entire Group.

Furthermore, in Japan, Fujitsu has established a domestic compliance program based on the Japan Fair Trade Commission’s “Compliance Program for Companies to Comply with The Antimonopoly Act”, in order to secure effectiveness of the GCP. Based on this program, Fujitsu consider “training”, “audit” and ”emergency response” as focused measures, and is working on creating an environment that fosters “zero tolerance” for bid rigging.

Going forward, Fujitsu will continue to strengthen the compliance activities based on this program and strive to prevent reoccurrence in order to win back the trust quickly.

Initiatives for Security Export Controls

For the purpose of maintaining global peace and security, the export of goods and the transfer of technology that could be utilized for the development or production of weapons of mass destruction, conventional weapons, etc. are strictly controlled under an international framework for security export controls (“International Export Control Regimes”). Japan is also implementing security export controls consistent with the same framework under the “Foreign Exchange and Foreign Trade Act”.

Following the stipulation to "comply with all laws and regulations" in the Fujitsu Way Code of Conduct, we are thoroughly working to implement our Security Export Control policy in line with not only Japan's “Foreign Exchange and Foreign Trade Act”, but also the U.S.'s extraterritorial “Export Administration Regulations” (EAR).

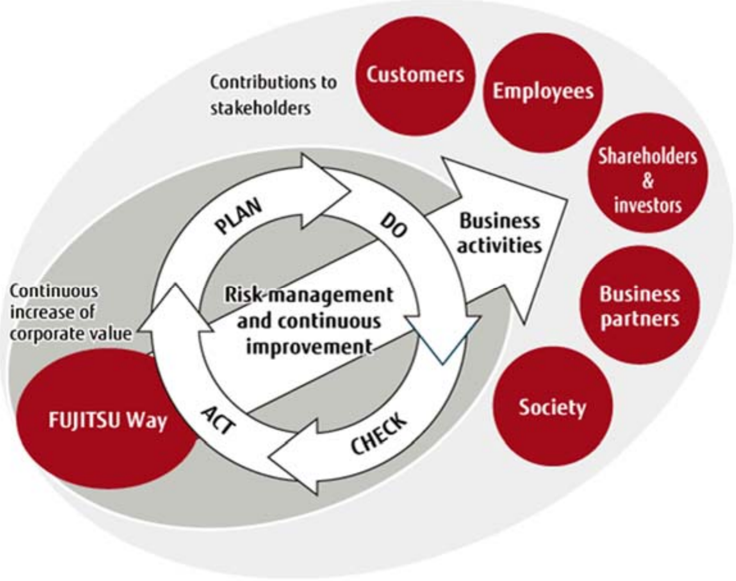
Fujitsu has established a system by which our President is the designated Chief Export Control Officer for the company and the “Security Export Control Office” in the “Legal, Compliance and Intellectual Property Unit” is the designated organization in charge. Product classification and transaction screening (of end use and end users) is performed by this office for all export of goods and overseas transfer of technology, so that the export of goods or transfer of technology will not happen without export licenses required by governments. Furthermore, the above Security Export Control policy requires us to issue a prompt report in the event of a legal violation. In terms of business execution, we strive for strict management to prevent any acts that could lead to non-compliance with export control laws, keeping close touch with the Ministry of Economy, Trade and Industry as the competent authorities for security export control in Japan. In order to maintain an appropriate level of export controls, we conduct annual export control audits and provide export controls training for executives and employees. In FY2016, we conducted regular internal audits of 30 in-house departments, assessed the appropriateness of internal operations, and provided guidance for making improvements.

Fujitsu also offers guidance to Group companies inside and outside Japan for developing frameworks for security export controls and tailoring in-house rules, provides in-house export control training and audits, and annually organizes the gathering of Group companies to exchange mutually beneficial information. In FY2016, we offered an e-learning course to all employees of the Group’s 64 companies in Japan, and a total of approximately 44,000 employees took the course. The Security Export Control Office also visited 7 Group companies in East Asia and Southeast Asia for the purpose of audits, training, and strengthening of frameworks for security export controls. Since FY2013, the Office has also been developing an e-learning training course covering security export controls in 20 languages for Group companies located across the globe.

Risk Management

Risk Management Guidelines

Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and indeed all stakeholders. Properly assessing and dealing with the risks that threaten the achievement of our objectives, taking steps to prevent the occurrence of these risk events, and establishing measures to minimize the impact of such events if they do occur and to prevent their reoccurrence are assigned a high priority by management. Moreover, we have built a risk management and compliance system for the entire Group and are committed to its continuous implementation and improvement.



Business Risks

The Group identifies, analyzes and evaluates the risks that accompany business activities and works on measures to avoid or reduce them, and to deal with them quickly in the unlikely event that they materialize.

Major Business Risks[*1]

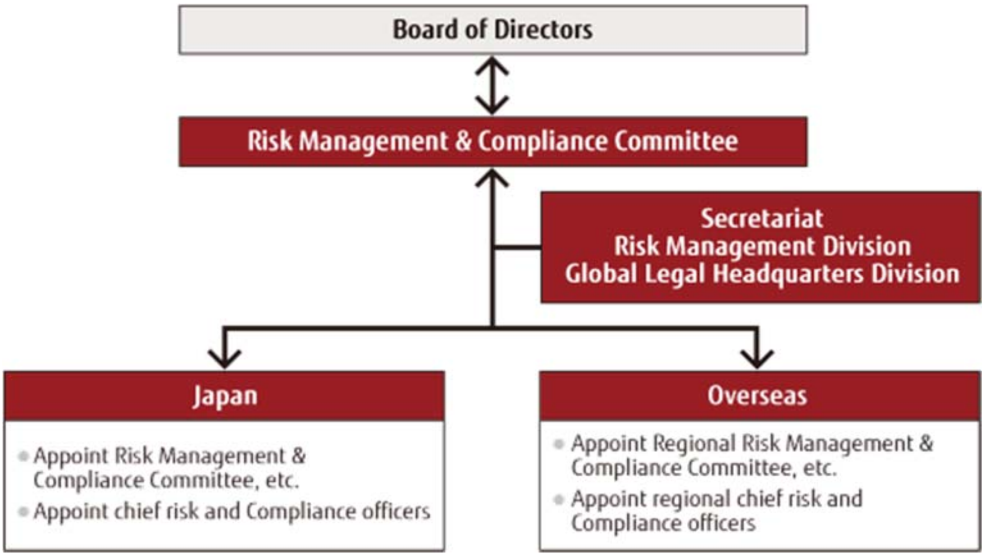
- Economic and financial market trend risk
- Customer risks
- Competitor and industry risk
- Investment decision and business restructuring risk
- Supplier and alliance risk
- Public regulations, public policies and tax matters risk
- Natural disasters and unforeseen incidents risk
- Financial reporting risk
- Financial risk
- Product and service deficiencies and flaws risk
- Compliance risk
- Intellectual property rights risk
- Security risk
- Human resource risk
- Fujitsu’s facilities and internal system risk
- Environmental risk

[*1]: These are just some of the business risks. More detailed risk-related information can be found in our earnings report, securities reports and other published reports.

Risk Management & Compliance Structure

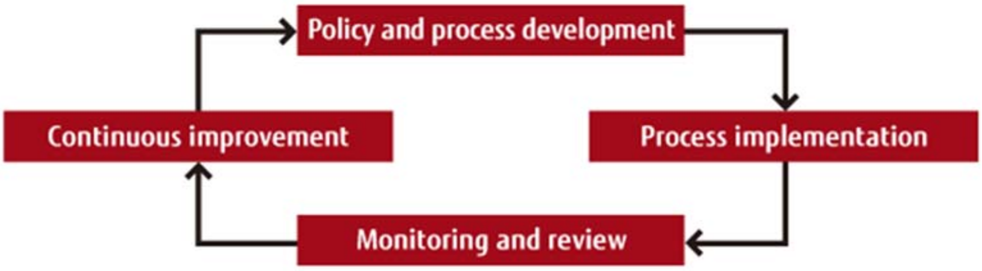
In order to prevent potential risks of loss in business execution from materialization, to respond aptly to materialized risks, and to prevent their recurrence, the Fujitsu Group has established a Risk Management and Compliance Committee under the Board of Directors. This committee acts as the highest-level decision-making body on matters involving risk management and compliance.

The Risk Management and Compliance Committee assigns Chief Risk and Compliance Officers to each of the Fujitsu Group's divisions and Group companies in Japan and overseas. Also, we established Regional Risk Management and Compliance Committees in April 2016. These organizations work collaboratively with each other, building a risk management and compliance structure for the entire Fujitsu Group that encourages them to both guard against potential risks and mitigate risks that have already materialized.

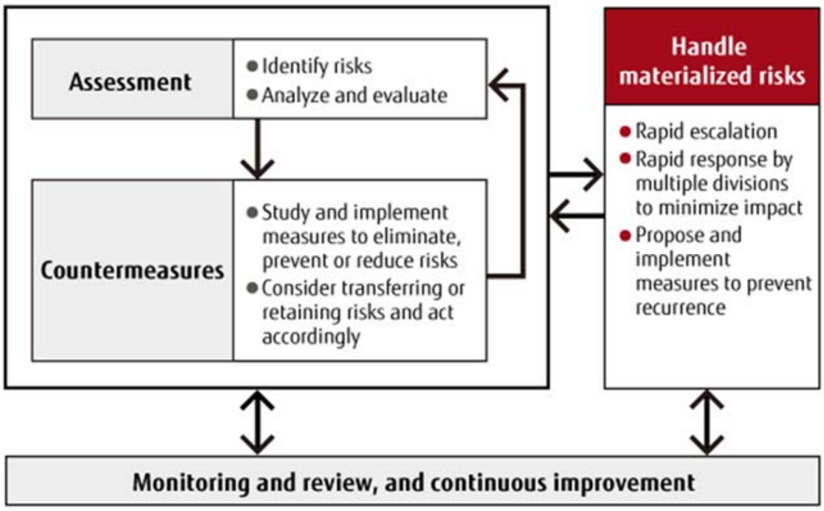

Board of Directors
Risk Management & Compliance Committee
Secretariat
Risk Management Division
Global Legal Headquarters Division
Japan
Appoint Risk Management & Compliance Committee, etc.
Appoint chief risk and Compliance officers
Overseas
Appoint Regional Risk Management & Compliance Committee, etc.
Appoint regional chief risk and Compliance officers

The Risk Management Framework

The Risk Management & Compliance Committee is responsible for grasping the status of risk management and compliance in all Fujitsu business groups and Group companies in Japan and overseas, establishing the appropriate policies and processes, etc., and both implementing and continuously improving them. In practical terms, it decides on risk management regulations and guidelines, applies them and continuously reviews and improves them.



Risk Management Processes


Assessment
● Identify risks
● Analyze and evaluate
Countermeasures
● Study and implement measures to eliminate, prevent or reduce risks
● Consider transferring or retaining risks and act accordingly
Handle materialized risks
● Rapid escalation
● Rapid response by multiple divisions to minimize impact
● Propose and implement measures to prevent recurrence
Monitoring and review, and continuous improvement

The Risk Management & Compliance Committee, which maintains regular communications with Chief Risk Compliance Officers, identifies, analyzes and evaluates the risks of business activities, and sets out and reviews the responsive measures, upon confirming the detailed measures intended to deal with major risks by averting, minimizing, transferring or retaining them. It also reports identified, analyzed, and evaluated important risks regularly to the Board of Directors.

The Risk Management Committee also prepares responses against the materialized risks despite the implementation of various preventive measures. If a critical risk such as a natural disaster, product breakdown or defect, a problem with a system or service, a compliance violation, an information security breach, or an environmental problem materializes, the department or Group company reports immediately to the Risk Management & Compliance Committee. The Risk Management & Compliance Committee coordinates with the related divisions and workplaces for rapid resolution of the problem by appropriate measures such as establishing a task force. At the same time, the Risk Management Committee strives to identify the causes of the problem and propose and implement solutions. Additionally, for critical risks, the committee also reports as appropriate to the Board of Directors.

The Risk Management & Compliance Committee continuously confirms the implementation status of these processes and works to make improvements.

Risk Management Education

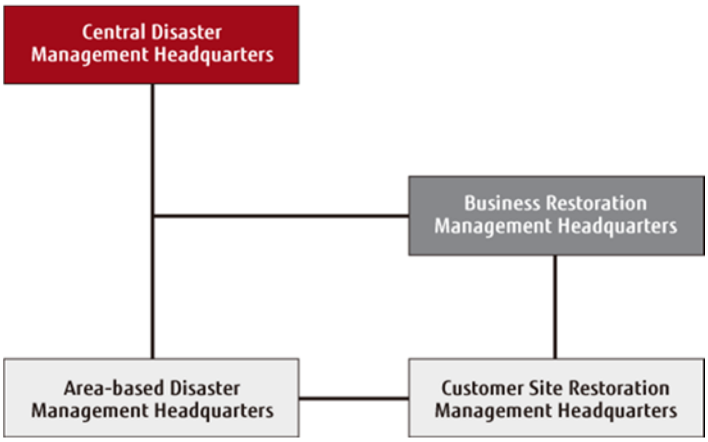
To enforce risk management across the entire Fujitsu Group, we conduct education and training at every level.

Specifically, in activities aimed at newly appointed executives and managers as well as Chief Risk Compliance Officers, we are working to communicate our basic concepts on risk management and the rule for prompt escalation to the Risk Management and Compliance Committee; to introduce specific examples of troubles concerning products, services, and information security; and to continually improve awareness and strengthen response capabilities with regard to risk management.

Examples of education programs implemented in FY2016

- New executive training: Training for around 80 newly appointed executives in Fujitsu Limited and the domestic Group companies.
- Risk compliance seminar: The seminar targeted at risk compliance officers and their assistants in Fujitsu Limited and the domestic Group companies, and was attended by around 200 participants.
- Group-wide disaster response drills, mock disaster exercises, BCM training, etc.: As well as enhancements to the central response functionality of the entire Fujitsu Group, disaster response drills and BCM training are conducted throughout the year at a range of different levels, including for entire business units or Fujitsu Group companies (offices or factories throughout the country).
- Training for personnel stationed outside Japan: Group training in areas such as risk management and safety for around 200 personnel working outside Japan.

Group-Wide Disaster Management


Central Disaster Management Headquarters
Business Restoration Management Headquarters
Area-based Disaster Management Headquarters
Customer Site Restoration Management Headquarters

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

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

To verify the efficacy of our disaster preparedness systems and enhance our response capabilities, we conduct drills tailored to every level, from the entire company through to task force, workplace and even the individual level. 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, consider and implement measures to address those issues, and work toward continually improving our capacity to prepare for disasters and sustain our business operations.

Fujitsu Group Joint Disaster Response Drills

On Japan's annual National Disaster Preparedness Day on September 1st, we carry out nationwide disaster response drills that incorporate mock disaster exercises. These drills are used to build a group-wide disaster preparedness organization to ensure and verify that the Group companies in Japan are fully versed in the essentials of dealing collaboratively with the various major disasters likely to impact the different regions.

FY2016 marks the 22nd year of systematic training drills for a potential major earthquake in Tokyo or along the Nankai trough. This year's drills, which were held at around 90 companies including Fujitsu Headquarters, envisioned a "Hokuriku-Shin'etsu earthquake" affecting large numbers of customers and the Fujitsu Group companies.

In the course of these drills, we collaborated with the affected offices to identify key initial response measures and steps to allow continued business operation, and confirmed the measures needed to assist in restoring customers' ICT systems. In addition, training was carried out at sites throughout Japan to verify the initial response procedures adopted by local recovery task forces immediately after a disaster (checking employee safety, assessing the extent of damage to work premises, rescue and aid activities, etc.).

These training exercises provide a channel for examining the issues identified and for improving the organization's disaster preparedness and its capacity to sustain its business operations.

Carrying Out Joint Inspections by Specialist Teams

Joint inspections are conducted at facilities selected from among all the Fujitsu Group companies in Japan as being those most at risk and where any damage would have the greatest impact. These inspections are led in the field by teams drawn from internal departments for environmental management, facility management, risk management and the safe operation of manufacturing equipment and processes. The teams check that laws are being upheld and also conduct inspections and provide guidance intended to prevent accidents that could arise from aging infrastructure or from fires and other natural disasters. This serves to boost safety at the inspected facilities.

The sharing of case studies illustrating the improvements and the most successful disaster preparedness measures resulting from these inspections also helps to promote consistent safe operations throughout the entire Fujitsu Group in Japan.

Business Continuity Management (BCM)

Recent years have seen a significant increase in the risk of unforeseen events that threaten continued economic and social activity, such as earthquakes, floods and other large-scale natural disasters, disruptive incidents or accidents, and pandemics involving infectious diseases.

To ensure that we 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, the Fujitsu Group in Japan has formulated a Business Continuity Plan (BCP) and also promotes Business Continuity Management (BCM) as a way of continuously reviewing and improving that BCP for establishing in the field. Through the BCM process, the lessons learned in the course of the Great East Japan Earthquake and the 2016 Kumamoto earthquake are now reflected in our BCP.

Improving Business Continuity Capability through Training

To fulfill our social responsibility as a company that supports social infrastructure, the Fujitsu Group companies in Japan organizes and analyzes business continuity issues at the business and site levels, and conducts ongoing training aimed at strengthening and improving our business continuity capability.

Promoting Appropriate BCM Activities through Business Continuity Capability Surveys

Our business continuity capability survey checks and assesses the level that Fujitsu units and Fujitsu Group companies in Japan have achieved in implementing management, education, and training in business continuity, and the level of their measures to resume business activities within the target recovery time objective.

The purpose of the business continuity capability surveys is to clarify the performance indicators (levels) to be achieved in the Fujitsu Group in Japan. By putting in place measures aimed at attaining those indicators, we are promoting appropriate BCM activities (workload and investment optimization) by the Fujitsu Group.

Training Specialists in BCM

The Fujitsu Group in Japan is systematically training specialists in order to further promote, implement and improve BCM. With the support of the Company-wide Promotion Office, BCM specialists from each department practice actual BCM activities to understand the essence of BCP and to become able to appropriately perform BCM activities.

Looking ahead, we plan to promote BCM activities within units and companies, centered on specialists with practical experience, to improve the business continuity capability of the Fujitsu Group in Japan.

Measures Against Infectious Diseases

The Fujitsu Group in Japan is also formulating countermeasures against new strains of influenza and other infectious diseases based on a three-pronged approach of safeguarding lives, preventing the spread of infection, and ensuring business continuity. We created a "Pandemic influenza Preparedness Action Plan" that stipulates preventive measures in everyday operations and the response process to be used if an outbreak occurs. We work to disseminate these to all employees through e-Learning and by distributing pamphlets. To assist with the continued operation of social infrastructure businesses and of our customers' businesses in the event of a pandemic or a particularly virulent new strain of influenza, we have also formulated a "Business Continuity Plan for New Influenza Strains (BCP)."

Strengthening BCM for Our Entire Supply Chain

In order to consistently supply products and services even under unforeseen circumstances, the Fujitsu Group has been continuously supporting the improvement of business continuity capability with our business partners since FY 2007, with the belief that it is essential to strengthen business continuity capability along our entire supply chain. With this in mind, the Fujitsu Group in Japan is promoting BCM activities throughout the entire supply chain, with efforts that include providing support for improvement of business continuity capability in our suppliers. Refer to the following for details:
“Enhancing Supply Chain BCM” with our suppliers

Information Secutiry

Basic Policy

To realize the "creation of a safe, pleasant, networked society" as proposed in the FUJITSU Way group vision and values, the Fujitsu Group is working to ensure and improve information security based on the "Fujitsu Group Information Security Policy," our global security policy.

Fujitsu Group Information Security Policy

As a company that places ICT as our core business, the Fujitsu Group's corporate vision is to contribute to the "creation of a safe, pleasant, networked society," under which we work to ensure information security throughout the group, while ensuring and improving the level of customer information security by providing ICT products and services.

With the publication of the "Cybersecurity Management Guidelines" by the Ministry of Economy, Trade and Information and the Information-technology Promotion Agency, Japan (IPA) in December 2015, our Risk Management and Compliance Committee, which reports directly to the Board of Directors, reviewed our group-wide global security policy, and in April 2016 formulated the "Fujitsu Group Information Security Policy."

Fujitsu Group Information Security Policy (excerpt*)
(Global Security Policy)

I. Purpose

In accordance with the "Cybersecurity Management Guidelines" formulated by the Ministry of Economy, Trade and Industry, the purpose of the Information Security Policy (hereafter, the "Basic Policy") is to set forth the measures, frameworks, and other basic matters required to ensure information security within the Fujitsu Group, as well as execute our corporate vision set forth in the FUJITSU Way, by which we have declared, both internally and externally, that the Fujitsu Group aims to ensure information security throughout the group and actively work to ensure and improve the information security of our customers through our products and services as a company that has placed ICT as the core of its business.

II. Basic Principles

(1) The Fujitsu Group, in all its business dealings, shall appropriately handle information provided by customers and partners as individuals and organizations, thereby protecting the rights and interests of said individuals and organizations.

(2) The Fujitsu Group, in all its business dealings, shall appropriately handle trade secrets, technical information, and any other information of value, thereby protecting the rights and interests of the Fujitsu Group.

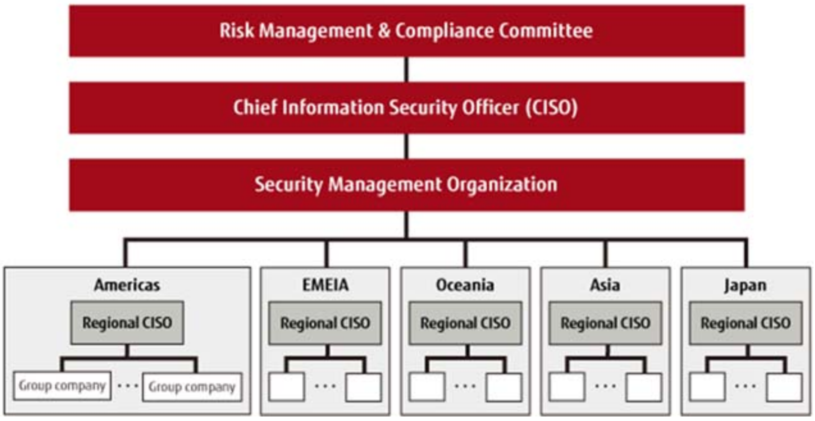
(3) The Fujitsu Group shall endeavor to conduct research and development and train personnel, as well as provide products and services that contribute to ensuring and improving our customer's information security in a timely and reliable fashion in order to contribute to the continued growth of our customers and society as a whole.

・Fujitsu Group Information Security Policy (full text)
http://www.fujitsu.com/jp/documents/about/csr/management/security/security-2016-04.pdf

Management Frameworks

Given the recent increase in cyberattacks, the Fujitsu Group appointed a Chief Information Security Officer (CISO) under the authority of the Risk Management and Compliance Committee in August 2015. Moreover, in aiming to strengthen our global information security management framework, we have appointed Regional Chief Information Security Officers (Regional CISO) around the world under the authority of the CISO. Specifically, we are working to strengthen the global information security governance that supports our global ICT business in the five regions of the US, EMEIA, Oceania, Asia, and Japan.

Information Security Management Frameworks

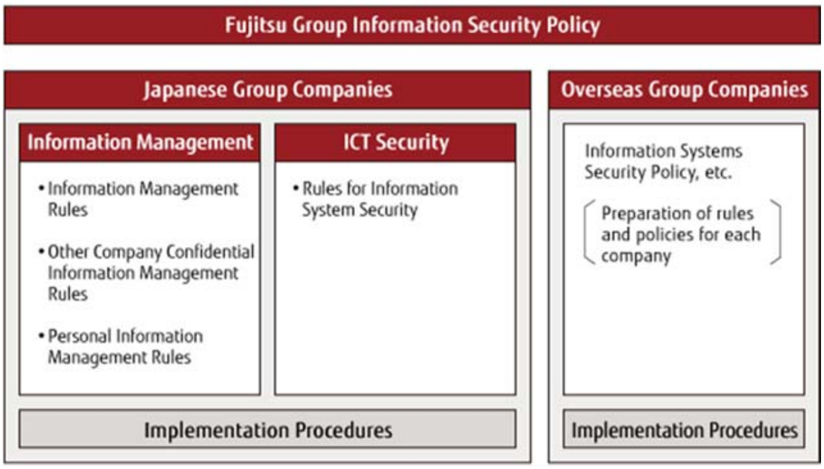


Security Management Function

Company Security Policy Formulation

Based on the "Fujitsu Group Information Security Policy," each Fujitsu Group company around the world prepares internal policies for information management and ICT security, by which they implement information security measures. Under the shared global Fujitsu Group Information Security Policy, we have prepared policies related to information management and information security for the group companies. each overseas group company creates and prepares unique rules and policies in accordance with the restrictions of the respective country.

Framework of Information Security Rules


Fujitsu Group Information Security Policy
Japanese Group Companies
Information Management
• Information Management Rules
• Other Company Confidential Information Management Rules
• Personal Information Management Rules
ICT Security
• Rules for Information System Security
Implementation Procedures
Overseas Group Companies
Information Systems Security Policy, etc.
Preparation of rules and policies for each company
Implementation Procedures

Security Inspection and Auditing

The Fujitsu Group conducts information security audits for each business department globally. These audits are conducted by an audit department that is independent of the business departments. The audits are conducted in a manner that considers the characteristics, business strategies, and ongoing information security measures, etc., of the different business departments. For example, , in addition to conducting on-site investigations to determine whether setup is in accordance with the rules at the time the intranet was installed, we also preform audits at the time public servers on the internet go on-line, as well as regular vulnerability audits in Japan.

In accordance with ISO27001 compliant security requirements, overseas group companies utilize assessment tools to evaluate the management condition. Business departments that have been audited then work to improve their information security measures based on the audit results.

Information Security Training

To prevent information leaks, we feel it is important to raise the security awareness and skill level of each individual employee, not simply inform our employees of the various policies. Therefore, all 100,000 employees of Fujitsu and group companies in Japan are provided with information security training during new employee training and promotion/advancement training, and all employees, including officers, are provided with security e-Learning in both Japanese and English every year.

Similarly, we provide employees of our overseas group companies with security training once per year in approximately 10 languages. Moreover, we provide international information security managers with the required security training for managers.

Information Security Awareness Development

Fujitsu Group conpanies in Japan formulated and raised a new domestic shared group slogan, "Declaration for complete information management! Information management is the lifeline of the Fujitsu Group" in 2007. Along with posting educational posters in the business offices of Fujitsu and our domestic group companies, we place seals on every employee's work computer, for example, to raise the awareness of each individual employee regarding information security.

In addition to these measures, we encourage the alertness of our employees by using our intranet to inform them of the frequent and global occurrences of information leaks, and hold security check days once per month as a way of ensuring that our managerial employees verify the security status of their own departments.

Complete Information Management Seal

Collaboration with Partners

As a result of dramatic changes in the ICT environment in recent years, the risk of information leaks has never been higher. In response, the Fujitsu Group has held information security presentations not only for Group employees but also for domestic business partners to which we outsource software development and services, and has worked to share information on challenges and to thoroughly implement prevention measures. In detail, please refer to the folliwing pages;

「With Our Suppliers」：Promoting Information Security Measures（http://www.fujitsu.com/global/about/csr/society/procurement/）
「Infomration Security Report 2017」P.10：Collaboration with Partners
*English version of Information Security Report will be published by the end of August, 2017.

Security Measure Implementation Function

In accordance with the security policies for all companies, the Fujitsu Group implements the following security measures for all companies across the entire group. In detail, please refer to the page. 11 of Infomration Security Report 2017.

- Network Security
- E-mail Security
- Internet Access Security
- Remote Access
- Endpoint Security
- Authentication Security

Monitoring, Analysis, and Evaluation Function

Security Monitoring

We record 1 billion logs per day using security monitors located around the world. When implementing information security management, it is essential to efficiently and effectively manage these logs.

The Fujitsu Group has established a Security Operations Center (SOC) that functions 24 hour a day, 365 day a year, and have created a mechanism that allows for fast, accurate incident and security alert response. The logs generated from the "Security Monitors" installed in multiple locations within the company's network are compiled and centralized in the "Log Integration Management System." These logs are then transmitted to "Systemwalker Security Control," a log automation and control tool, which then sends an alert notification e-mail to the SOC if it confirms a threat.

The SOC is comprised of "Local Operators," "Incident Managers," and "Security Assistants," who analyze the details of the received alert notification e-mail, determine the quality, scope, and weight of the threat, rank the response priority, and handle the threat in a fast, accurate manner.

White Hat Hacker Internet Behavior Surveys

To respond to the evolving threat of cyberattacks, we use white hat hackers to investigate global incidents and vulnerabilities, and use cyber intelligence to investigate logs based on the risk information generated from unauthorized access and malware analysis, thereby minimizing the risk of new threats and preventing the occurrence of incidents.

Personal Information Protection

Fujitsu acquired the PrivacyMark* in August 2007, and have continuously worked to strengthen our personal information protection framework, which includes annual personal information handling training and audits. Our domestic group companies have also acquired the PrivacyMark when necessary, and work to ensure personal information management. On the public websites of our international group companies, we post privacy policies designed to meet the laws and social requirements of each country. For a list of domestic group companies that have acquired the PrivacyMark, please see Third-party Evaluation and Certification (p.37) discussed later.

*PrivacyMark：
A certification system relating to the handling of private information. The system is operated by the Japan Institute for Promotion of Digital Economy and Community.

Information Security Report

Since 2009, Fujitsu has globally publicized its information security efforts through its annual "Information Security Report" in order to maintain trust from its shareholders, customers, and other stakeholders.

「Infomration Security Report 2017」
*English version of Information Security Report will be published by the end of August, 2017.