# Management Frameworks

Independent of the chief information officer (CIO), the Fujitsu Group has appointed a chief information security officer (CISO) under the authority of the Risk Management and Compliance Committee to strengthen its information security governance as a global ICT company.

## Information Security 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. By separating out the responsibility for information security management, traditionally handled by the chief information officer (CIO), and appointing an independent officer dedicated to and specialized in information security management, we organized a framework that more rapidly and accurately manages risk measures in light of the growth of increasingly sophisticated cyberattacks.

Moreover, in aiming to strengthen our global information security management framework, we have appointed regional chief information security officers (regional CISOs) 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.

### ■ Risk Management and Compliance Committee

The Risk Management and Compliance Committee reports directly to the Board of Directors, which handles risk management and compliance for the entire Fujitsu Group. The committee consists of Fujitsu's representative director president, executive, and chief risk management & compliance officer. The committee is also in charge of handling information security risk, which is a major risk.

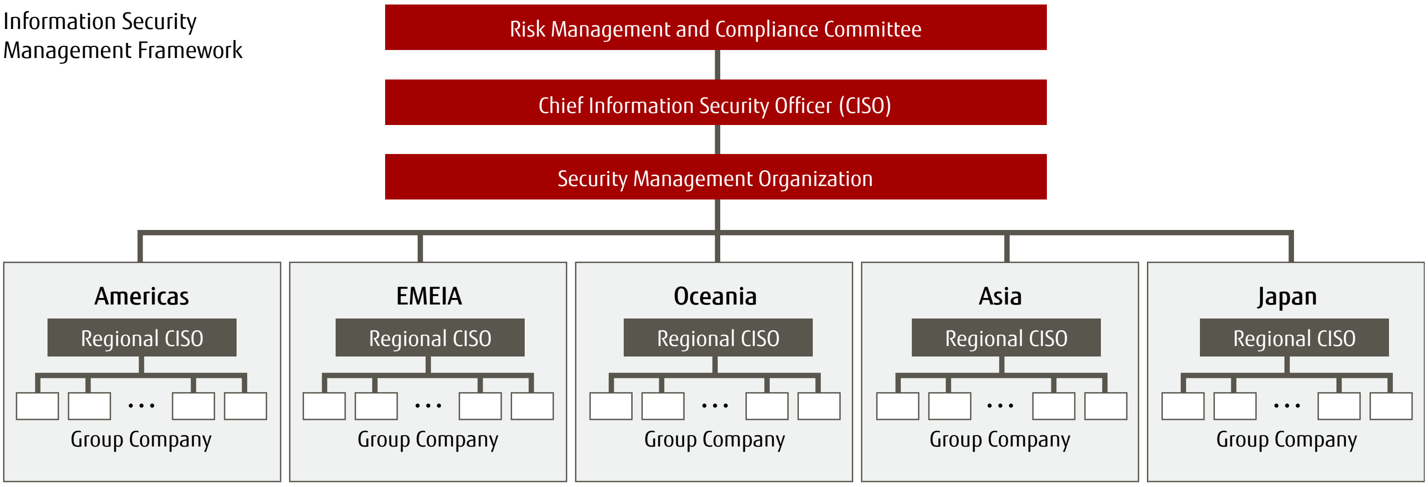
### ■ Chief Information Security Officer (CISO)

The chief information security officer (CISO) is appointed from the Risk Management and Compliance Committee, and is granted the responsibility and powers to manage global information security within the Fujitsu Group. The CISO reports regularly and as necessary to the Risk Management and Compliance Committee regarding the execution status of security measures.

### ■ Regional CISO

The regional CISOs are the chief security officers located in each of the five regions, and are granted the highest powers and responsibilities to manage information security within their region of authority. These officers formulate information security measures for the regions under their authority, and promote the thorough execution and reporting of information security as implemented by each group company's security team.

Information Security Management Framework



# Management Frameworks

### Security Management Organization

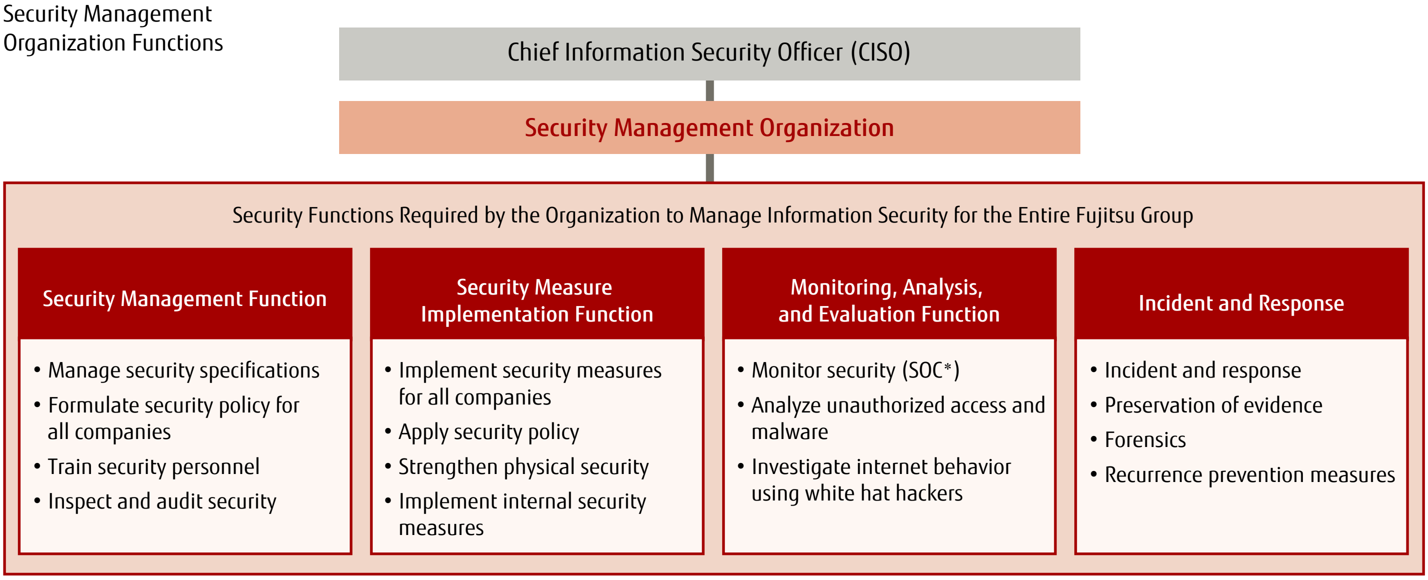
The Security Management Organization reports directly to the CISO for the purposes of strengthening Fujitsu Group information security, and plans common group rules and measures to promote unified management. This organization has four major functions designed to manage the Fujitsu Group security management function; security measure implementation function; monitoring, analysis, and evaluation function; and incident and response function.

## 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 in Japan. For overseas group

Security Management Organization Functions



Chief Information Security Officer (CISO)

Security Management Organization

Security Functions Required by the Organization to Manage Information Security for the Entire Fujitsu Group

**Security Management Function**
- Manage security specifications
- Formulate security policy for all companies
- Train security personnel
- Inspect and audit security

**Security Measure Implementation Function**
- Implement security measures for all companies
- Apply security policy
- Strengthen physical security
- Implement internal security measures

**Monitoring, Analysis, and Evaluation Function**
- Monitor security (SOC*)
- Analyze unauthorized access and malware
- Investigate internet behavior using white hat hackers

**Incident and Response**
- Incident and response
- Preservation of evidence
- Forensics
- Recurrence prevention measures

*SOC: Security Operations Center

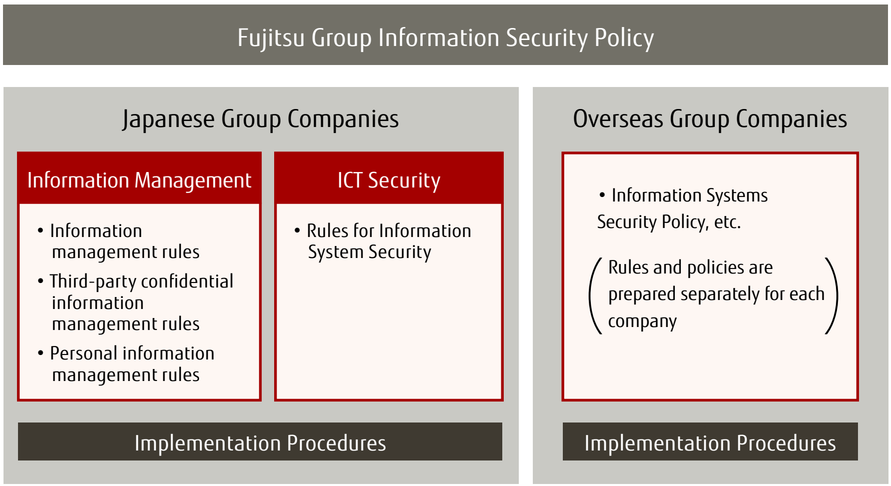
Information Security Policy Framework

**Information Management Rules**
Rules for appropriately handling information for work

**Third-party Confidential Information Management Rules**
Rules for appropriately handling third-party confidential information

**Personal Information Management Rules**
Rules for appropriately handling personal information based on personal information protection policy principles

**Rules for Information System Security**
Management rules for maintaining the confidentiality, integrity, and availability when using information devices, information systems, and networks



Fujitsu Group Information Security Policy

Japanese Group Companies

**Information Management**
- Information management rules
- Third-party 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.

(Rules and policies are prepared separately for each company)

Implementation Procedures

companies, they create and prepares rules and policy in accordance with the regulations of the respective country.

## ■ Security Screening 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 perform audits at the time public servers on the internet go on-line, as well as regular vulnerability audits in Japan.

In accordance with ISO 27001-compliant security requirements, we utilize assessment tools to evaluate the management of overseas group companies. 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 only 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 overseas information security managers with the required security training for managers.

e-Learning Screen

## ■ Information Security Awareness Development

Fujitsu Group companies in Japan formulated and raised a 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 its group companies in Japan we place sticker 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

Declaration for complete
information management!
Information management is the
lifeline of the Fujitsu Group

情報管理 徹底宣言!
情報管理は富士通グループの生命線

## ■ Information Management Handbook Publication

In Japan we publish the Information Management Handbook to deepen the understanding of internal policies regarding information management. This handbook can also be viewed on the intranet so that policies can be checked immediately whenever there is a question regarding information management.

### Information Management Handbook

—Enhancing Security Thinking and Skills—

1. Purpose of this handbook
2. What is information?
3. Handling confidential information
    - 3.1 Handling confidential Fujitsu information
    - 3.2 Handling third-party confidential information
    - 3.3 Provision of confidential information through service contracting
4. Handling personal information
5. Daily check points
    - 5.1 Do not leak internal information
    - 5.2 Common personal information
    - 5.3 Taking confidential information out of the business office
    - 5.4 Disclosing confidential information outside of the company
    - 5.5 Discarding confidential information
    - 5.6 Password settings
    - 5.7 Malware countermeasures
    - 5.8 Important matters during network use
    - 5.9 Important matters during e-mail sending and receiving
    - 5.10 Important matters during fax use
    - 5.11 Using personal IT equipment for work
    - 5.12 Using tablets, smartphones, and mobile phones
    - 5.13 Business office information security
    - 5.14 On using Fujitsu PKI
6. Handling accidents

## Collaboration with Partners

### Partner Information Security Management (selection, status evaluation, verification)

When selecting new partners, we verify the partner's information security condition and limit partners to those who have consented to agreements regarding important matters for information security management and handling of personal information during work contracting.

In regard to existing partners, we also conduct an annual written survey of the partner's information security status and select contractors based on required matters, such as the Act on the Protection of Personal Information. We also provide the results of the written survey, including the overall status and evaluation tools, as feedback to our partners so that they can implement initiatives to improve security.

Once a partner has been selected, we conduct annual information security audits. We visit our partners and inspect their information security compliance status based on any agreements. When the results of the inspection reveal a need for correction, we draw up a rectification plan and provide implementation guidance.

Information Security Audits (FY 2016):
Approximately 190 companies

### Information Security Training Sessions

Recently, rapid changes in the ICT environment has led to a greater risk of information leaks than in the past, which in turn has led us at the Fujitsu Group to hold information security training sessions for both group employees and our partners to which software development and services are contracted.

Given that preparing for advanced persistent threats(APTs) and ensuring other cybersecurity measures is an urgent matter for our partners, as well, in FY 2016 we held training sessions under the main theme of "Security Risk Response."

At the request of our partners, we also conducted on-site training sessions to which we dispatched lecturers. In addition, for partners that requested leader class skill training, we conducted on-site workshops in which group exercises and discussions were used to improve risk response skills. So that the workshop style training sessions could be attended by many of our partners, we planned and conducted collective workshops to which even single individuals could apply.

Information Security Training Session Details (FY 2016)

Approx. 900 companies/approx. 1,200 attendees (Sendai, Tokyo, Kawasaki, Chiba, Nagoya, Osaka, Takamatsu, Fukuoka, Okinawa)

- On-site Training Sessions: Approx. 80 companies/approx. 1,300 attendees
- On-site Workshops: Approx. 10 companies/approx. 180 attendees
- Collective Workshops: Approx. 20 companies/Approx. 30 attendees

### Information Sharing and On-site Support Tool Provision

Awareness Poster

こんなことしてませんか?
STOP 個人Webメール閲覧
>マルウェア感染ファイル ダウンロード →標的型攻撃
STOP 情報流用
>関係者外へ他プロジェクトの情報漏えい
Y市様向け システム更新提案
X市様向け システム更新提案
STOP ちょっとだけ自宅作業
>受託情報運搬中の 紛失・盗難
STOP 議事メモ撮影
>管理できない個人機器からの情報漏えい
今日、Y市さんへシステム更新の説明。緊張したよ…(^ ^)v
STOP SNSへ投稿
>お客様からの指摘 →出入り禁止

Since 2009, we have provided "Information Security Plazas" and "Awareness Posters" to our partners as a way of sharing and providing the latest information regarding information security.

Moreover, we provide project specific "Project Information Security Plans" to which all employees consent as a means of sharing information security requirements at the start of each project, and which serves as a means of aiding early discovery and response to problems. In addition, we also provide a "Compliance Status Check Sheet" as a self-inspection tool.

### Overseas Partner Response

For the purposes of responding to the globalization of our customers, reducing development costs, and securing personnel, we have been increasing business cooperation with overseas partners.

Fujitsu, as do in Japan we conclude Information Manage-

On-site Workshop

Information Security Training in India

ment Guidelines for Contractors agreements with our overseas partners, which provide for handling of entrusted information in accordance with the conditions of the specific country. We also conduct regular information security audits and provide information security training.

### Personal Information Protection

Fujitsu acquired the PrivacyMark in August 2007, and has continuously worked to strengthen our personal information protection framework, which includes annual personal information handling training and audits. Our group companies in Japan also acquire the PrivacyMark when necessary, and work to ensure personal information management. On the public websites of our overseas group companies, we post privacy policies designed to meet the laws and social requirements of each country. The Fujitsu Group companies are working on reinforcement of personal information protection system for a more secure and smooth protection of personal information in an ever-evolving state of global data circulation.

たいせつにしますプライバシー

10300034

## Security Measure Implementation Function

In accordance with the security policies, we implement the following security measures to the entire group companies.

### Network Security

We have installed firewalls between the external internet environment and the Fujitsu Group internal information network to protect against unauthorized access, and have adopted an unauthorized intrusion detection system to maintain the safety of our intranet. Our Security Operations Center (see page 12) monitors detection information 24 hours a day, 365 days a year.

### E-mail Security

Our e-mail gateways for handling external threats include spam mail and malware (virus) countermeasures, such as IP reputation and sender domain authentication. In addition, we automatically reverify all transmissions sent outside the company using automated e-mail recipient identification and automatically verify external transmission eligibility, thereby preventing any user who does not need external e-mail communication from transmitting e-mails or leaking information outside of the company.

### Web Security

As a means of providing safe internet access procedures, all access to the internet necessarily passes through proxy servers, which check for malware and filter URLs to prevent access to malicious websites. In addition, proxy utilization is limited by user authentication, which both prevents unintended access and records user access logs.

### Remote Access

We provide a remote access environment that allows work to be conducted safely when connecting to the intranet from outside the company via personal computer or smart device. We encrypt communications over the access routes and utilize two-factor authentication to prevent unauthorized access. In addition, as an initiative to innovate working-styles, we have introduced virtual desktops and provide an environment that allows for work to be carried out remotely while ensuring security by preventing data from remaining on the personal computer being used.

### Endpoint Security

We automatically apply OS and application security updates, as well as renew malware definition files on employee computers. In addition, we utilize thin clients for terminals on which data cannot be saved to strengthen our information leak prevention measures. Similarly, we are continuing to install standard personal computers and thin clients equipped with these endpoint security measures. As a result, we have been able to reduce the burden required of each individual employee for implementing different security measures on personal computers, and at the same time have improved the level of security by implementing standardized endpoint security in a systematic, unified manner.

### Authentication Security

We have introduced IC security cards for employee authentication and other purposes. The face of the security card is printed with the name and photograph of the employee, and the IC chip is loaded with the name, employee number, employee public key infrastructure (PKI) certificate, and key. These cards which are managed by the human resources department, guarantee the card user is the proper employee. These cards can be used for both system login authentication via secure identity verification and electronic document settlement, which is as effective as stamping a sanctioned seal on paper documents.

## 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 has 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 comprises 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.

## Incident and Response Function

### Incident and Response

The Fujitsu Group has established a dedicated incident and response team. When an incident occurs, the team cooperates with the SOC to identify the location of occurrence and affected terminals, after which the team uses specialized devices to appropriately preserve evidence*. In addition, the team employs measures to prevent secondary damage and to reduce the spread of damage.

*Preservation of evidence: Rapidly collecting traces of the cyberattack and analyzing these is essential to identifying the cause of the incident as well as any damage. To ensure these traces are not lost, electromagnetic evidence (hard disks, logs, etc.) from the equipment related to the incident is preserved (copied, etc.).

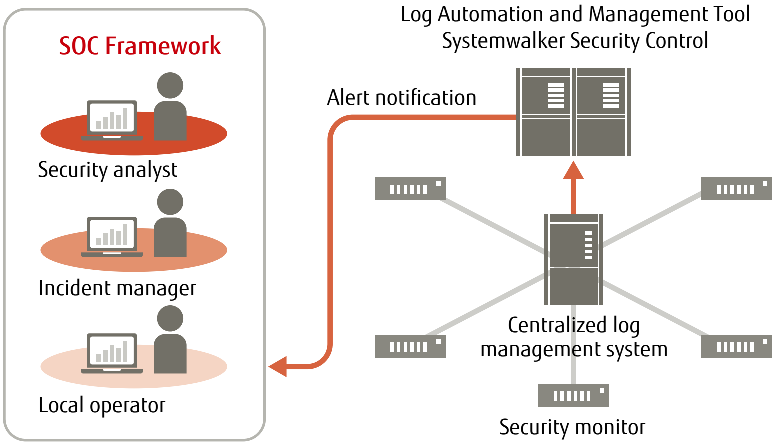
### Forensics

We analyze the preserved evidence, as well as the alerts and logs acquired by the SOC. We then identify the damage, cause, and affected scope to rapidly bring the situation to a close.

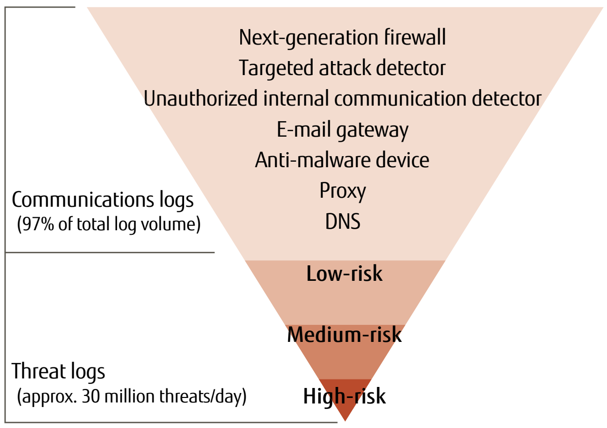
### Recurrence Prevention Measures

We then report the risk discovered by the investigation to the Risk Management and Compliance Committee. Under the CISO, we further investigate whether similar incidents have occurred, and deploy recurrence prevention measures to all companies in cooperation with the related departments.

Security Monitoring (SOC) Framework



Security alert classifications


Next-generation firewall
Targeted attack detector
Unauthorized internal communication detector
E-mail gateway
Anti-malware device
Proxy
DNS
Communications logs
(97% of total log volume)
Low-risk
Medium-risk
Threat logs
(approx. 30 million threats/day)
High-risk