Risk Management

Policy

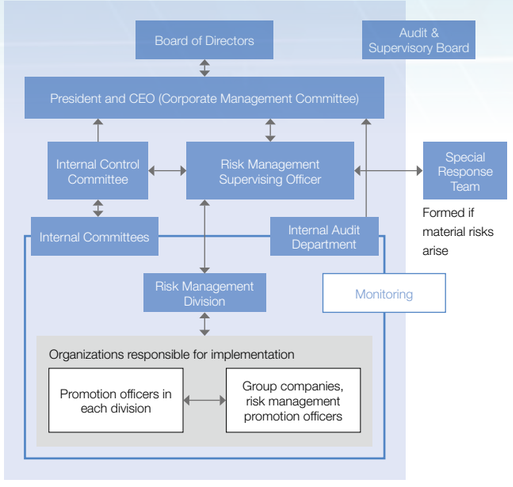
The NTT DATA Group seeks to ascertain all risks associated with business activities to minimize the frequency of occurrence of these risks and limit their impact on operations should they materialize. To facilitate this effort, in 2002 we appointed an officer in charge of supervising and promoting risk management from a Companywide perspective.

In addition, risk management promotion officers were appointed to the Risk Management Division as well as other divisions and Group companies to enable them to respond proactively and independently to various risks.

NTT DATA defines material risks, and reviews progress toward addressing these and achieving related targets, with the results of such reviews being reflected in various measures.

The Internal Control Committee convenes twice a year to discuss measures pertaining to the reduction of risks and evaluate their effectiveness. The results of these evaluations are reported to the Corporate Management Committee as well as the Board of Directors.

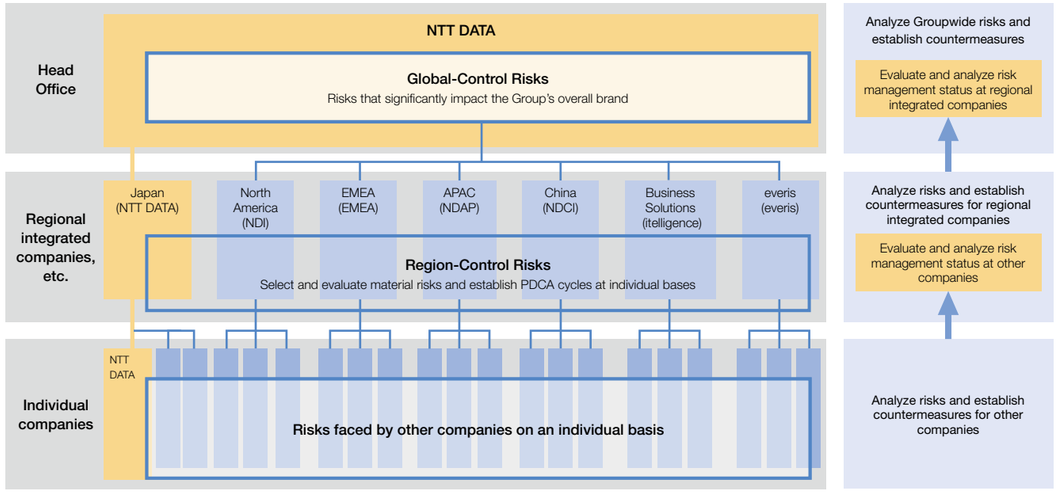
Since the NTT DATA Group provides various services worldwide to a wide range of clients and industries, each business unit has its own unique business environment. Therefore, the Board of Directors decided to delegate considerable power to sector heads. This measure allows proper understanding of and prompt responses to risks relating to client relationships and market environments.



Management Structure

NTT DATA identifies risks that may impact its Head Office, regional integrated companies, etc., and other companies on an individual basis, and formulates countermeasures accordingly. High-level divisions effectively manage the measures in place at organizations under their jurisdiction by analyzing and evaluating their implementation status. Groupwide measure implementation status is analyzed, evaluated, and monitored by the Risk Management Division. In addition, risks determined to have the potential to impact the entire Group are defined as "global-control risks," and are managed on a Groupwide basis. In this manner, the Company is practicing stringent and comprehensive risk management.

Risk Management Categories



Global-Control Risks

Global-control risks with the potential to impact the entire Group are identified by the Internal Control Committee by incorporating input from outside specialists and adopting a broad perspective that encompasses factors such as changes in social trends.

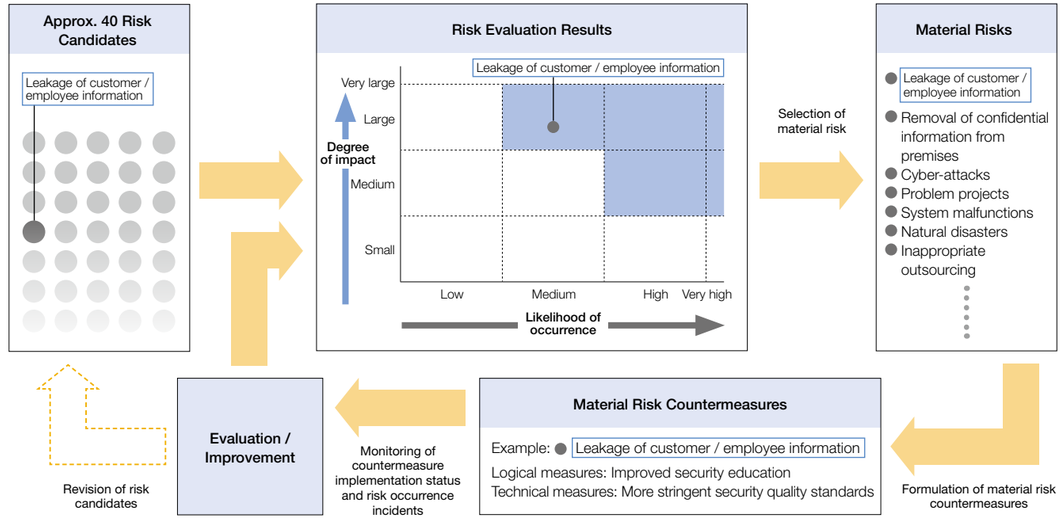
In 2016, we will continue selecting the same risks as in the previous fiscal year as a medium- to long-term effort spearheaded by NTT DATA's Head Office to strengthen our response to auditing deficiencies and the auditing of alliances, among other initiatives.

Material risks	Major improvements, etc.	Initiatives
Information leakage (personal / confidential information) Cyber-attacks	• Continue enhancing countermeasures for ever-increasing security risks • Strengthen preparedness for advanced cyber-attacks focused on public institutions	• Promote Companywide security measures (targeted attack emails, etc.), conduct cyber-attack response drills, review response to malware mass infection, and provide shared infrastructure for security • Expand security personnel training / qualifications
Accounting fraud (including window dressing)	• Expand global unified auditing, connect to risk indication auditing	• Review and implement global unified auditing items • Implement full-scale risk indication auditing, deploy in Group companies • Promote introduction of unified rules related to accounting, check mechanisms and operations • Stimulate awareness through training
Bribery	• Continue strengthening compliance education	• Conduct training related to overseas bribery regulations • Organize approach related to handling of gifts, etc.

Region-Control Risks

Region-control risks managed independently by regional integrated companies define material risks based on approximately 40 risk candidate items in each region that are evaluated and improved in light of material risk countermeasure implementation and risk occurrence status.

<Process of Selecting Region-Control Risk>



WEB This section introduces basic approaches and characteristic initiatives taken from our Information Security Report 2016. For details on our efforts in this area, please see Information Security Report 2016.
http://www.nttdata.com/global/en/csr/security/index.html

Negligence with respect to cyber-attacks and other information security response issues can increase the direct damage to businesses and seriously impact society. The NTT DATA Group focuses efforts on information security in accordance with information security policies.

Basic Approach Regarding Information Security

The Information Security Policy was established in 1998 as guidance for appropriately handling information assets and protecting information security, and the Personal Information Protection Policy was formulated in 2001. These policies were revised and improved in response to information technology progress and societal changes. Group companies also formulated information security policies based on the NTT DATA Group Security Policy (GSP) in an effort to ensure the secure distribution of information throughout the entire Group.

The objectives of the GSP, ensuring safety of information and actively utilizing and sharing information, are essential as a partner that supports customers' efforts to create new businesses. To realize these objectives, we are promoting initiatives including logical measures covering the formulation of rules and provision of training and educational activities related to information security, and technical measures to prevent information leaks as well as the introduction of thin-client PCs.

Safe Groupwide Application of Knowledge

Information Security Management System

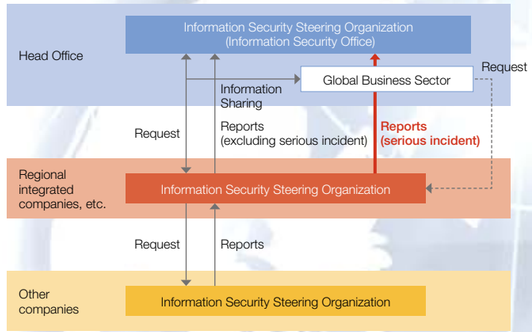
The Information Security Committee ascertains the Companywide status of information security activities and areas requiring improvement and formulates necessary initiatives. In addition, NTTDATA-CERT was established as a specialized organization for preventing information security incidents*1 and responding to any incidents that might occur. NTT DATA also joined the Nippon CSIRT Association as well as Forum of Incident Response and Security Teams (FIRST)*2, a global computer security incident response team (CSIRT)*3 community. Through our participation in these organizations, we are collecting a wide range of information on security trends, which we then utilize to improve security. The information security governance structure comprises three levels of information security steering organizations located at the Head Office, regional integrated companies, and other companies on an individual basis to ensure thorough global information security governance. The information security steering organizations at each level cooperate closely to maintain and develop information security policies, monitor information security measures, respond to emergencies, and engage in preventive measure activities to prevent incidents.

*1. The term information security incidents refers to the actualization of security threats related to information management and system operation, such as computer virus infection, unauthorized access and information leakage.
*2. FIRST is a global community consisting of approximately 350 CSIRTs from government agencies, educational institutions, companies and other organizations.
*3. A CSIRT is an incident response team comprised of security specialists. These teams collect and analyze information on security incidents, security-related technologies and vulnerabilities, and conduct activities including implementing effective countermeasures and training.

Global Information Security Governance Points

- Created a structure to promote the establishment of three levels of information security steering organizations located in the Head Office, regional integrated companies, and other companies on an individual basis
- Close cooperation among information security steering organizations
- Head Office conducts quarterly monitoring of control status at integrated companies

Structure of Information Security Governance



Ensuring the Security of Commercial Systems

NTT DATA thoroughly engages in enhancing its ability to respond to cyber-attacks on information systems, including unauthorized access via the Internet, internal intrusions by means of malware (so-called targeted attacks), and internal fraud. Specifically, we promote (1) building appropriate security measures starting from the development stage, (2) conducting periodic vulnerability checks (security diagnosis) for operating systems, (3) strengthening our framework for promptly responding to detected critical vulnerabilities, and (4) ensuring sound operational management of important information. In addition, we strive to provide systems that can be used safely and securely by promptly sharing information on the latest security technology trends and vulnerability information.

Initiatives Focused on the Future of Information Security

By quickly anticipating the future of information security, NTT DATA strives to create well-balanced systems that make people's lives more convenient while ensuring safety through efforts to automate cybersecurity measures and develop network technologies for Internet of Things (IoT) autonomous self-protection.

2020 will be a watershed year for the world of information security. The physical plane of people and devices will merge with cyberspace, thus NTT DATA is committed to developing new technologies in view of this novel concept of protecting every aspect of such an environment. Among the myriad of new technologies, the key to the future of information security is artificial intelligence (AI). AI will play a central role, not only in security information and event management (SIEM) and IoT self-protecting network technology but also in security technologies related to automatic vehicle operation and inter-company global cooperation on threat intelligence. We are also engaged in research and development focused on the medium to long term, including interlinking with AI to protect against the leakage of information by automated responses, the utilization of wearable terminals, reliable authentication, and the improvement of forensic technologies.

Future Aspects of Information Security

Latest Initiatives	Vision for 2020
Cybersecurity measure enhancements	Protecting the physical plane (people and devices) and cyberspace
Internal fraud countermeasures, internal measure enhancement	Automation of incident detection control using big data and AI
	Network technology for IoT autonomous self-protection
	Inter-company global cooperation on threat intelligence

Latest Challenges	Medium- to Long-Term Initiatives for 2020
Strengthening cybersecurity measures against targeted attacks	Use of wearable terminals
Information leakage resulting from internal fraud	Detection technology enhancement (use of AI, etc.)
Protection of specific personal information including "My Number" data	Incident response enhancement (use of automated technologies, etc.)
	IoT security