How Do We Identify and Respond to Risks?

To achieve sustainable business growth, a solid foundation is essential for appropriately managing increasingly diverse and complex risks and maintaining the trust of customers and society. This section explains our initiatives in areas such as risk management, information security, and AI governance. In addition, the CISO describes our efforts to enhance security governance across the entire Group.

Risk Management

At SoftBank, we work to mitigate and prevent risks by building an organizational structure to identify risks throughout the Company, implementing preventive measures, and executing periodical risk management cycles.

Risk management structure

In order to identify Company-wide risks from various angles and prevent the materialization of risks, we have established a management system based on the concept of a "three-line model." The first line is where each department in the head office conducts reviews that includes risks when devising various measures and policies on the ground, while also carrying out risk management in their own departments. The second line is where the Risk Management Division, an organization independent from business departments, headed by a the head of the Risk Management Division charged with overseeing risk management, conducts Company-wide and comprehensive identification of risks and confirmation of the status of measures taken (conducted twice a year), and reports to the Risk Management Committee. The Risk Management Committee, which includes the President & CEO, COO, CFO, etc. as members and in which the Audit & Supervisory Board members and heads of the relevant departments also participate, determines the level of importance and the risk manager (risk owner) for each risk, gives instructions to take measures, etc. and through the head of the Risk Management Division, reports the status to the Board of Directors. The committee also supervises risks that may have a significant impact on the Group (including telecommunications service risk, information security risk, and information systems risk) with a Director experienced in information security (President & CEO Junichi Miyakawa) playing a central role.

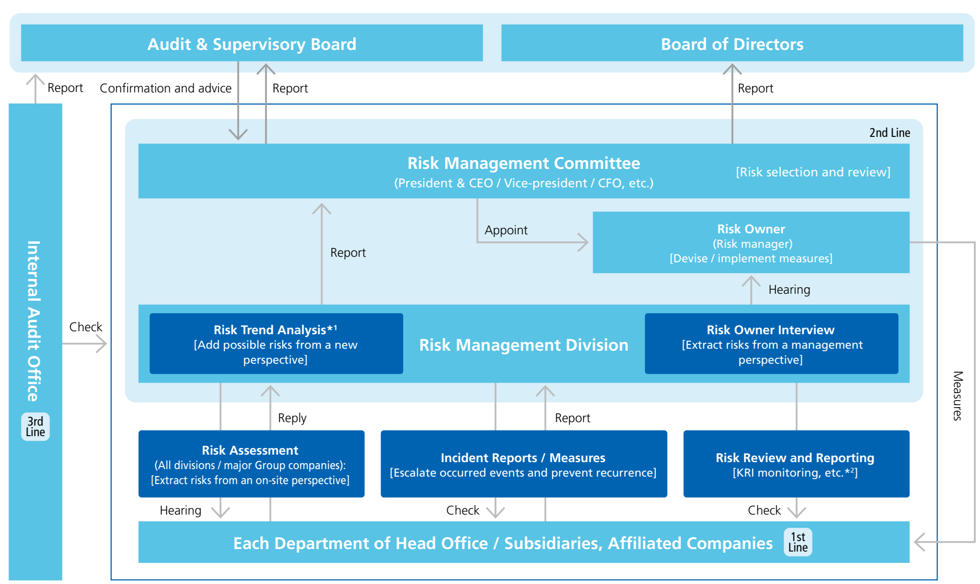
The Internal Audit Office conducts an independent audits the entire risk management system and situation from a position independent from the first and second lines.

The head of the Risk Management Division reports the content of reviews by the Risk Management Committee, including the risk identification process, to external (non-executive) directors who supervise the execution of company operations. In addition, the division head reports to the Audit & Supervisory Board and reflects the confirmations and advice on risk management methods and areas for improvement received from external (non-executive) directors and the Audit & Supervisory Board members in our risk management measures.

In addition, we establish a reporting system for subsidiaries and affiliated companies, and conduct periodic checks of business-related risks identified by each subsidiary and affiliated company and countermeasure status, from the standpoint of risk management for the Group overall.

We strive to prevent any incidents, but in the unlikely event that one does occur, the department where the incident occurred acts as the first line in identifying the details and impact of the incident and reporting to the Risk Management Division in accordance with the reporting standards stipulated by the incident impact determination criteria. The Risk Management Division evaluates the impact of each incident and promptly reports any incidents that may have a significant impact on the management of the Group to management, external directors (non-executive), and the Audit & Supervisory Board members, etc.

Furthermore, in terms of considering and implementing measures to reduce the impact of incidents and prevent recurrence, each department in the head office, as the first line, proactively reviews and implements specific measures, while the Risk Management Division has established a system as the second line to verify and evaluate the content of these measures and the status of their implementation, and provide advice and guidance as necessary. While promoting highly effective response measures by the first line that are suited to the actual situation on the ground, the second line provides appropriate supervision based on the risk management framework and rules, working to prevent the recurrence of incidents and minimize their impact.



*1 Risk trend analysis: a technique where the latest news and public information is analyzed to provide material for identifying risks from new perspectives.

*2 KRI: Key Risk Indicators

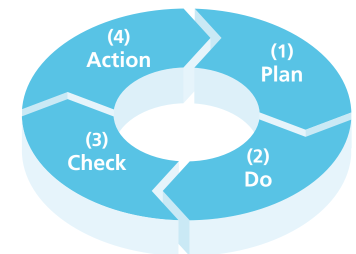
(Note)1 The head of the Risk Management Division and the head of the Internal Audit Office independently report on risk management and audits to the Board of Directors based on their respective capacities.

2 We are working to further improve our risk management system through by outside evaluation of risk management by a third-party organization. This includes an annual evaluation of internal control in accordance with the internal control reporting system stipulated by the Financial Instruments and Exchange Act and SSAE18.

3 Please refer to "Risk Management" on our website for details.

Risk management methods

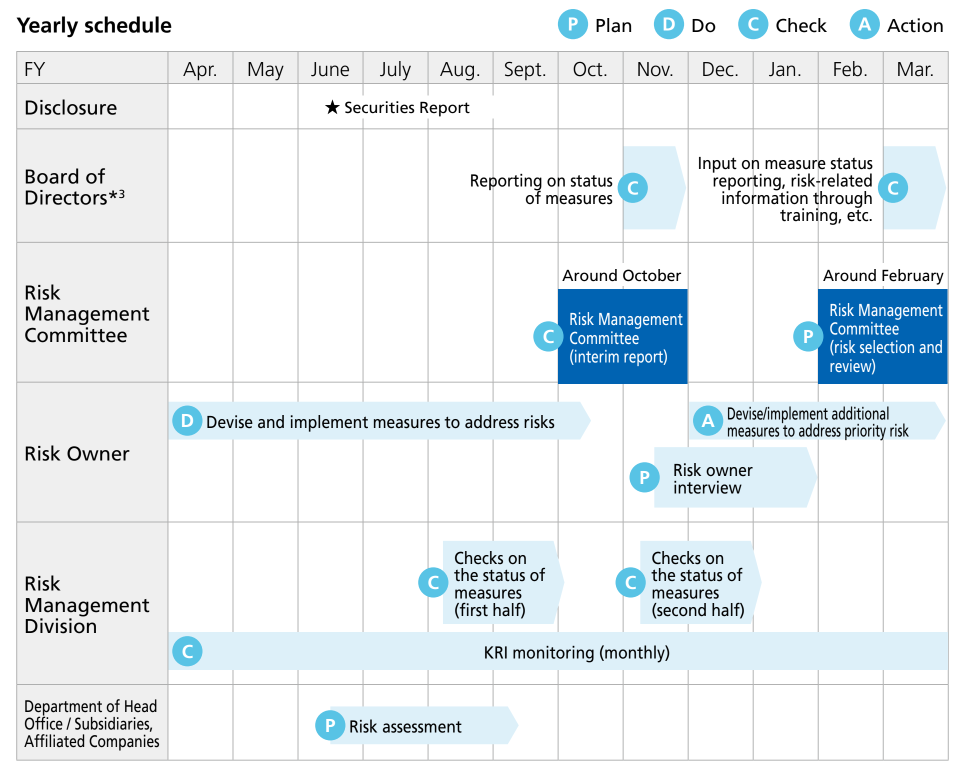
When devising various policies and measures, not only are we reviewing potential risks in conjunction with business opportunities, we are also implementing a PDCA cycle, as illustrated below, on a regular basis to identify, select, and assess a wide range of risks for the Group, through which we are working to uncover, mitigate, and prevent increasingly complex and diverse risks before they occur.



PDCA cycle

(1) Plan	The Risk Management Division conducts risk assessments using a risk classification table (compiled from risk scenarios relevant to SoftBank and its subsidiaries and associates), interviews with the heads of each division in the Company and the management of our principal subsidiaries and associates, interviews with each risk owners for the fiscal year, and the Risk Management Committee identifies risks that have a significant impact on the Company based both on perspectives from the field and from the perspective of management and appoints risk owners. We do this to conduct a more multifaceted risk analysis aimed at identifying risks from various viewpoints by collecting information by means of providing information beforehand, such as external environment reports that include risks and opportunities, and raising questions that include short-term and medium- to long-term viewpoints.
(2) Do	Risk owners review and implement measures, etc. for risks based on those that the Risk Management Committee has determined to have a significant impact on the Company.
(3) Check	The Risk Management Division monitors the status of measures by risk owners on a monthly basis, and reports to management and the Risk Management Committee. Based on these reports, the Risk Management Committee checks the implementation status, etc. of measures, reviews risks, and checks the necessity, etc. of additional measures.
(4) Action	Risk owners examine and implement improvements and additional measures, etc. for any additional measures that are determined to be necessary by the Risk Management Committee.

Yearly schedule



*3 Includes advance briefings for External Directors and Audit & Supervisory Board Members.

We have implemented a system to broadly identify risks and opportunities, assess their significance and priority, and incorporate them into countermeasures and various initiatives.

During risk assessments and interviews, we not only consider traditional risks but also include opportunities. Additionally, we evaluate their impact by establishing time horizons: short-term (within a few years), medium-term (approximately 3 to 5 years), and long-term (approximately 10 to 30 years), aiming for a more accurate analysis.

Consolidated risks are addressed through countermeasures led by the Risk Management Committee. Meanwhile, information on opportunities is shared across departments and utilized in the development of sustainability strategies and the establishment of materiality.

Addressing Risks That Have Significant Impact on the Company

Based on the likelihood of occurrence and the magnitude of potential effect, we assess and identify risks that have a significant impact on our Company by classifying them into four levels in the matrix on the right. Furthermore, from the identified risks, we comprehensively evaluate and prioritize the risks that require immediate attention and take appropriate countermeasures to reduce risks and prevent issues before they occur.

Impact

Level		Definitions
4	Significantly high	Tremendous impact on entire business/Group
3	High	Tremendous impact on business
2	Medium	Impact on execution of business
1	Low	Minor impact on business

Probability

Level		Definitions
4	Significantly high	Likely to occur multiple times a year
3	High	May occur once every year
2	Medium	May occur once every few years
1	Low	May occur once every 10 years

Risk related to management strategy

Risk items	Typical risk examples	Risk reduction measures
a. Changes to economic conditions, regulatory or market environments, and competition with other companies		
▪ Domestic political conditions ▪ Competitors' situations ▪ Customer expectations ▪ Amendments to laws ▪ Economic fluctuations ▪ Demographic changes ▪ Product/ service defects	▪ Risk of increased competition in the telecommunications industry due to new entrants from other industries and the rapid spread of services from startups competing with the Group's services ▪ Risk of providing products or services with major defects that cause damage to customers	▪ Adopt services, products, and sales methods that suit consumer orientation ▪ Thorough quality control during manufacturing and development stages
b. Adapting to technology and business models		
▪ Technological innovation	▪ Risk of the Group being unable to respond appropriately or in a timely manner to changes in the market such as the emergence of new technologies (including generative AI and AI agents) or business models	▪ Research the newest technology and market trends, conduct verification testing to introduce technically superior services, consider alliances with other companies, etc.
c. Leakage or inappropriate use of information (including privacy information) and inappropriate use of products and services provided by the Group		
▪ Leakage or loss of information due to cyber attacks ▪ Inappropriate use of information assets ▪ Inappropriate use of products/services	▪ Risk of information leakage, loss, etc. due to intentional or negligent actions of the Group or unauthorized access such as cyber attacks by a third party ▪ Risk of losing society's confidence and trust in the Group due to an error arising from inadequate management and utilization of our information assets resulting in social criticism ▪ Risk of lowered confidence and trust due to misuse (crimes such as fraud, etc.) of apps or payment services provided by the Group	▪ Limit work areas related to confidential information and establish access control rules; monitor and prevent unauthorized access due to cyber attacks from outside the company; separate and isolate access and networks according to information security levels ▪ Establish guidelines and conduct training ▪ Periodic monitoring of unauthorized use
d. Destabilization of the international situation		
▪ Procurement of equipment, facilities, etc.	▪ Risk of delays in transportation of telecommunications business equipment and facilities due to regulations and restrictions imposed on aircraft, ships, and so forth by countries in conflict or other countries involved	▪ Monitoring, information gathering, decentralization and diversification of suppliers
e. Stable provision of network services		
(a) Telecommunication network failures	▪ Risk of being unable to maintain telecommunications service quality due to increased network traffic or an inability to secure necessary frequency bands	▪ Bolster the telecommunication network based on predictions of future traffic
(b) Unpredictable circumstances such as natural disasters	▪ Risk of a natural disaster, pandemic, etc. preventing normal operation of telecommunication networks or information systems	▪ Introduce network redundancy, establish an emergency recovery system, and implement countermeasures for power outages at network centers and base stations

(Note) Please refer to "Addressing risks that have significant impact on the company" on our website for details.

Risk related to management strategy

Risk items	Typical risk examples	Risk reduction measures
f. Corporate acquisition, business alliances, establishment of joint ventures, organizational restructuring within the Group		
▪ Investment and loans	▪ Risk of investee companies being unable to perform as expected; risk of business partnerships and joint ventures not producing expected results	▪ Conduct sufficient due diligence when considering each investment to make investment decisions in accordance with the prescribed approval process
g. Dependence on other companies' management resources		
(a) Outsourcing ▪ Inappropriate management of information by outsourced companies	▪ Risk of outsourced companies being unable to perform work as expected ▪ Risk of infringing on customers' human rights as a result of an outsourced company fraudulently acquiring Group and customer information or using it for other purposes	▪ Conduct periodic audits of outsourced companies' work ▪ Evaluate and select the supplier in accordance with our purchasing rules
(b) Use of other companies' facilities ▪ Other companies' management resources	▪ Risk of becoming unable to continue using communication line facilities owned by other operators	▪ Use multiple operators' communication line facilities
(c) Procurement of various equipment ▪ Supply disruptions ▪ Delivery delays	▪ Risk of supply disruptions, delivery delays, etc. in the procurement of telecommunication equipment, etc.	▪ Build networks by procuring equipment from multiple suppliers
h. Use of the *SoftBank* brand		
▪ Brand use	▪ Risk that our actions negatively impact the trust or interests of SoftBank Group Corp. and we become unable to use the *SoftBank* brand	▪ Bolster the system for checking prior to using the brand, release materials related to brand use, and conduct training
i. Service interruption or degradation due to related system failure		
▪ System failures	▪ Risk of becoming unable to continuously provide service for customer-facing systems, the *PayPay* cashless payment service etc. due to human error, equipment/system problems, cyber attack by a third party, hacking, or other unauthorized access	▪ Add redundancy to the network and clarify recovery procedures in case of failure or other accidents
j. Training and securing human resources		
▪ Human resources (hiring, training) ▪ Labor management (overwork, etc.) ▪ Human rights ▪ Diversity	▪ Risk of being unable to secure engineers or other human resources necessary for business operation as planned ▪ Risk of reducing society's trust and confidence in SoftBank due to being unable to meet social demands for consideration for basic human rights ▪ Risk of reducing society's trust and confidence in SoftBank due to being unable to meet social demands for respecting diversity and demonstrating their full potential	▪ Adopt a remuneration system that considers the expertise of human resources with high market value ▪ Establish a human rights policy and human rights due diligence process; conduct risk assessments ▪ Ensure Company-wide awareness of efforts related to diversity; conduct training
k. Climate change		
▪ Increasing damage from natural disasters ▪ Biodiversity	▪ Risk of higher restoration and maintenance costs due to an increase in disaster-affected facilities and worsening of damage ▪ Risk of financial losses due to impacts on supply chains from the loss of biodiversity	▪ Promote redundancy of core networks and secure communications in the event of a disaster, etc. ▪ Conduct risk assessment on the impacts that business has on biodiversity

(Note) Please refer to "Addressing risks that have significant impact on the company" on our website for details.

Information Security

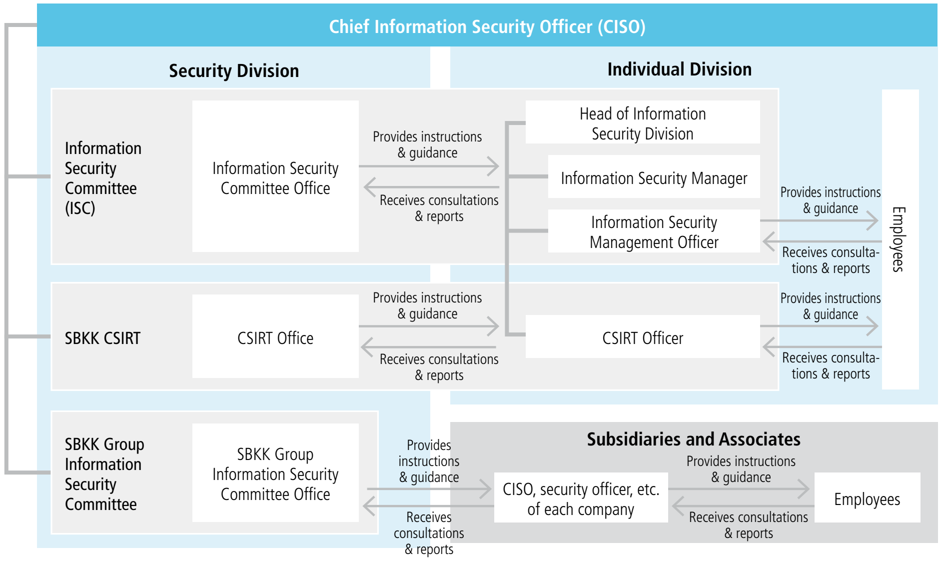
Information security

Policy

We have formulated and continue to adhere to our “Information Security Policy” so that we can keep the trust of our customers and the wider community by implementing sweeping and advanced solutions to counter the risk of information leaks. In addition, we take the utmost care in handling the personal data of our customers, in accordance with our “Privacy Policy,” and give due consideration to the rights of our customers. Furthermore, we have taken the initiative in protecting privacy by ensuring compliance with various laws and regulations, guidelines set by the government, and other standards, as well as by joining a certified personal information protection organization as a designated business operator.

Meanwhile, security risks have become increasingly diversified and advanced, highlighted by the sophistication of cyber attacks, the increase in persistent attacks by international hacker groups, attacks targeting teleworking environments, and cases of internal fraud. We constantly monitor and study these kinds of threats, but at the same time, we proactively employ cutting-edge technology to develop advanced security environments, while also working to further enhance our 24 hours a day, 365 days a year security surveillance and rapid response framework. Furthermore, we run training sessions to instill a heightened level of security awareness among all employees, while constantly keeping our security policies and rules up to date in step with the times.

Information security governance



We have established the Information Security Committee (ISC), chaired by the Chief Information Security Officer (CISO) and comprising managers of information security from each department, to promote information security measures across the entire Company. Moreover, through the creation of the SoftBank Computer Security Incident Response Team (SoftBank CSIRT), we are making every effort to prevent the occurrence of security incidents and to minimize damage by swiftly responding to incidents. We have also created the SBKK Group Security Committee, which is chaired by the CISO and comprised of the information security managers at affiliate companies in an effort to collaborate closely on the implementation of policies and various measures at each affiliated company.

Security measures

To protect the facilities that provide customer information and telecommunication services and to ensure the safe use of our products and services, we have established five levels of security areas in our facility environment and strictly manage them at each level. In addition, security analysts monitor security 24 hours a day, 365 days a year at the Security Operation Center (SOC). Furthermore, we are constantly advancing our information security measures by collaborating internally and with other organizations, and by reviewing our measures using the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework (CSF) and the Center for Internet Security’s (CIS) CIS Controls.

(Note) Please refer to “Information Security” on our website for details.

Continuous security enhancement

In response to the spread of digital devices, advances in AI and increasingly sophisticated cyberattacks, we strive to continuously strengthen security by adopting the latest technologies, improve the security mindset of our employees through education, and train specialists in the field of security.

[Technological measures]

(1) Monitoring technology

While the early detection of incidents is becoming increasingly difficult due to the growing complexity of attack techniques in recent years, the number of detected incidents is on the rise each day. SoftBank strives to improve the quality of monitoring by continuously upgrading detection methods, implementing analysis and solutions by referring to threat intelligence (information useful to detecting and blocking attacks), and automating response operations so that no signs of attack are missed.

(2) Monitoring of threats and attacks

By monitoring communication log data collected from digital devices, such PCs and smartphones, and machines such as servers, we anticipate and determine threats from multiple angles: suspicious communications inside or outside of our organization, potential malware infections, and others. We have built information sharing processes with security organizations we belong to and with security vendors to ensure we are aware of the latest trends by reviewing incidents at other companies and reports on vulnerabilities and attacks.

We aim to detect sophisticated and complex attacks as early as possible by implementing Security Information and Event Management (SIEM), a tool to detect the latest attacks, whereby various data logs can be collected and correlation analysis be performed.

(3) Monitoring of telecommunication networks security

Since telecommunications networks serve as social infrastructure, expectations for their reliability and quality are higher than ever before. SoftBank, as a telecommunications provider, performs different kinds of monitoring to provide a stable telecommunications network. Monitoring security is one part of this effort.

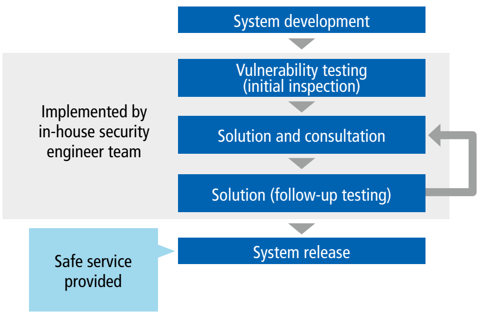
What 5G networks can bring include not only higher speeds but also ultra-low latency and massive device connectivity. It is expected that 5G will enable a variety of use cases like remote operations and autonomous driving. SoftBank is building an even more stringent security monitoring system to respond to changes in data traffic caused by DDoS attacks and to counter cyberattackers' attempts to access 5G equipment.

Use cases of 5G network features

Ultra-low latency	Remotely-controlled robots, autonomous driving, telemedicine - all previously considered difficult due to latency.
Massive device connectivity	Accelerated power of IoT that will revolutionize industries and society, with more things and sensors connected to networks.

(4) Security testing

If SoftBank launches services with deficient equipment or latent vulnerabilities, our network and system could be subject to attacks, potentially resulting in harm to customers. Our security engineer team carries out complete vulnerability testing and issues instructions to address any vulnerabilities detected so that we can provide safe services.



Since new vulnerabilities can emerge even after the release of a service we continue vulnerability testing and follow-ups to minimize security risks.

(5) Enhancement of internal security environment

We are responding to sophisticated attacks by utilizing various security solutions including MDM (Mobile Device Management) and EDR (Endpoint Detection and Response). Additionally, we carry out simulation exercises on targeted attack e-mails, to help strengthen our internal network security.

Some solutions and technologies that we have internally implemented and verified effectiveness are offered to enterprise customers as security services.

[People-led enhancements]

(1) Employee training

In order to ensure appropriate handling of information at the workplace as well as to raise awareness of information and cyber security, we provide classroom training, e-learning programs, security drills to executives and employees while constantly updating security rules.

At our internal training, we place particular importance on the "protection of personal information" and "secrecy of communications," and we continue to work on improving our employees' knowledge and ethics.

Useful materials and educational videos on information security are available on the company intranet portal for employees to access at any time.

(2) Training of security experts

Our security experts work hard not only to collect and share information on threats and solutions but also to improve their technical skills and knowledge so that they can guard against ever-changing security threats. SoftBank encourages them to obtain security qualifications to build their expertise.

Qualifications held by our security experts	CISSP, Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Registered Information Security Specialist (RISS), GIAC qualifications, CEH, AWS Certified Security - Specialty, among others.

CISO Interview

Continuously strengthening Group-wide security governance to protect corporate value

Q In November 2023, our subsidiary, LY, publicly announced a data breach incident caused by unauthorized access, which subsequently led to administrative guidance from Japan's Ministry of Internal Affairs and Communications. As a parent company, how do you view the challenges in security governance?

SoftBank and NAVER Corporation (hereinafter "NAVER") each hold a 50% stake in A Holdings Corporation, the parent company of LY. This incident originated from unauthorized access to a system of a NAVER-affiliated company, leading to the leak of some user information from the *LINE* app. In response, the Japan's Ministry of Internal Affairs and Communications issued administrative guidance stating that "LY's outsourcing partner was a NAVER-associated company with strong capital influence over LY, and adequate management of the outsourcing partner was not carried out." We take this matter very seriously as well.

Going forward, we will accurately and swiftly revise our security policies in line with changes in the business environment surrounding SoftBank and Group companies. We will also more rigorously monitor compliance status across all Group companies. Furthermore, we will step up efforts to strengthen security across the entire Group by implementing continuous risk reduction measures.

Q LY is currently implementing measures to prevent a recurrence in response to the administrative guidance. As the parent company, how do you evaluate these efforts and their progress to date?

LY has positioned security enhancement as a top management priority. The company has secured a budget of ¥15 billion for FY2024 and is steadily implementing the following recurrence prevention measures.

Measures to prevent recurrence:

- Ending outsourcing to the NAVER group and completely separating the network and authentication platforms previously shared with the group
- Thoroughly implementing technical countermeasures, such as strengthening access control and monitoring systems under its own leadership
- Raising the standards for the entire LY Group to a level equivalent to SoftBank's security governance policies and countermeasures
- Implementing employee security education using common training materials and conducting regular audits

We highly commend these initiatives as they demonstrate LY's strong risk management awareness and implementation capabilities.

In addition, LY holds a "Group CISO Board" every two weeks*, consisting of CISOs from its key group companies. As the CISO of the parent company, I attend every meeting. I closely examine the scope and security level of each initiative and provide detailed feedback and ask in-depth questions as needed. This meeting is generally held online to accommodate participating group companies located overseas. However, we created an opportunity at the end of 2024 for all related parties to meet in person at LY's head office to engage in deeper discussions. I feel this opportunity has further strengthened collaboration and allowed various measures to proceed more smoothly than before.

*As of June 2025, the frequency of the meeting has been changed to once a month.

Q What lessons have you learned from this incident?

We previously minimized intervention in security governance for LY, respecting its autonomy and independence as a listed company. However, this incident served as a catalyst for us to realize that as a parent company, we should be more deeply involved in the following issues that could significantly impact the corporate value of the entire Group, regardless of whether a company is listed or not.

Issues that could significantly impact the corporate value of the entire Group:

- Confirming the presence of personal information and confidentiality of communications handled at overseas offices
- Assessing the degree of dependence on service providers in specific countries
- Verifying that systems comply with domestic regulations and guidelines

Going forward, we will implement more rigorous security measures across all Group companies and further enhance the overall level of security governance within the organization.

Q Going forward, how do you plan to strengthen security governance for the entire Group, not only for LY but also for other listed subsidiaries?

First, we believe it is essential to further strengthen and maintain close communication channels with each Group company.

To quickly identify important issues and take action before potential risks materialize, it is crucial to establish smooth information sharing and good relationships based on trust, even during normal times. Therefore, we will create multi-layered communication channels, from executives and security officers to mid-level managers and front-line staff, to deepen mutual understanding more than ever.

This will create a system that enables early exchange of information and consultation not only when incidents occur, but also when there are signs or potential risks. In the future, we will also unify security governance frameworks, policies, and risk visualization methods across the Group and establish a mechanism to grasp the risk status of the entire company in real time.

Q What initiatives are in place for SoftBank's unlisted subsidiaries?

For unlisted Group companies, we provide more practical support compared to those of the listed Group companies and involvement based on each company's business characteristics and risk profile, as follows.

Practical support and involvement for unlisted Group companies:

- Conducting risk assessments and audits for each company, and establishing reporting systems and response procedures for when incidents occur
- Providing security awareness training programs for all employees, as well as specialized training programs for security personnel and system developers
- Assisting in the implementation of various security solutions to protect devices and systems
- When necessary, seconding our specialists to support building in-house capabilities for continuous improvement of security posture

Through these initiatives, we are further strengthening the information security foundation of the entire Group and helping each company establish a robust security framework while maintaining its independence.

Q Could you share your aspirations for the future?

As our *Beyond Carrier* strategy has deepened, our Group has expanded its business beyond telecommunications into diverse fields such as media, e-commerce, and payment/finance. We are now advancing the development of "Next-generation Social Infrastructure" to support a society that coexists with AI. I believe that for this to be realized, it is essential for us to uphold security and earn unwavering trust of society.

Based on the lessons learned from this incident, we are determined to continuously strengthen security governance while respecting the autonomy and independence of each company, and to steadfastly protect our corporate value.

AI Governance

As the use of AI rapidly advances across various fields in Japan and overseas, companies are responsible for handling AI appropriately to provide safe and reliable services. We are actively building our AI governance through discussions in the "AI Ethics Committee," an advisory board for appropriate AI development and operations, to advance the practice of responsible AI.

Basic policy

Under our *Beyond Carrier* strategy, we are working to provide innovative services and promote DX by going beyond just being a traditional telecommunications carrier and leveraging cutting-edge technologies such as AI and IoT. Among these cutting-edge technologies, AI has been widely used in all industries in recent years and is expected to see more diverse applications and become increasingly sophisticated in the future. On the other hand, depending on how it is used, it is possible that AI could yield discriminatory assessments or selection, disseminate misinformation or false information, and infringe on the rights of others. This highlights the need for ethical considerations and caution when using the technology.

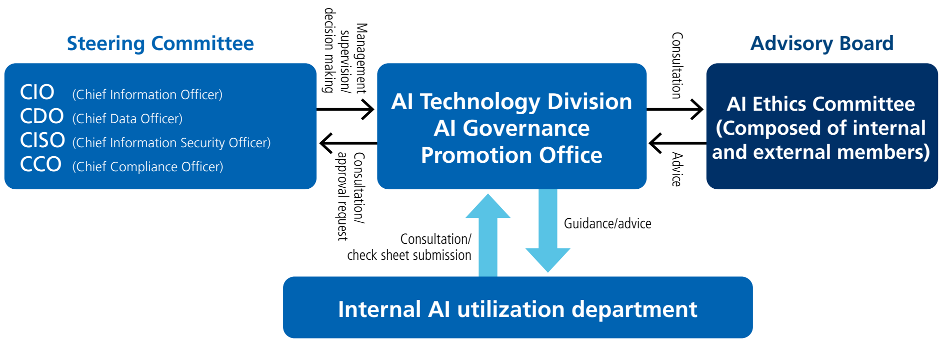
In light of this, in July 2022, we formulated the "SoftBank AI Ethics Policy" for the purpose of ensuring the appropriate use of AI and delivering safe and reliable services to customers. More specifically, the policy sets out six main guidelines: (1) human-centeredness, (2) respect for fairness, (3) pursuit of transparency and accountability, (4) ensuring safety, (5) privacy protection and security, and (6) development of AI human resources and literacy. We will operate our business and develop services in accordance with these guidelines.

In addition, we have put in place a framework to adopt this policy throughout the Group, and as of April 2025, 75 Group companies have decided to implement it.

Promotion system

AI governance is promoted by the AI Technology Division, the strategic division for our AI business.

AI governance promotion and execution system



We have established the AI Governance Promotion Office as an independent, specialized department within this division to oversee governance related to internal AI utilization. The Steering Committee, which includes our CIO (Chief Information Officer), CDO (Chief Data Officer), CISO (Chief Information Security Officer), and CCO (Chief Compliance Officer), performs management and supervision.

In addition, the "AI Ethics Committee," composed of members from both inside and outside the Company, provides advice as an advisory board.

AI Ethics Committee

To address ethical issues in AI and implement "responsible AI*," we established the AI Ethics Committee in April 2024 as an advisory board on overall AI ethics. The committee is chaired by our Senior Vice President & CISO and consists of six external experts with a wide range of expertise in areas such as AI ethics, technology, data governance, finance, law, and ESG, along with five internal executive officers and employees.

The committee met four times in FY2024 to exchange information on a wide range of topics, including the status of AI utilization at SoftBank, our AI governance initiatives, AI regulatory trends in Japan and overseas, and AI ethics from an ESG and institutional investor perspective. As AI technology rapidly evolves and its associated challenges become more complex on a global scale, we will continue to incorporate the diverse perspectives and insights of external experts to achieve objective and highly effective AI governance based on the perspectives of users.

AI Ethics Committee FY2024 agenda

Meeting month	Agenda
1st meeting: July 2024	▪ Status of SoftBank's AI utilization ▪ SoftBank's AI governance initiatives
2nd meeting: October 2024	▪ Trends in AI regulation in Japan and overseas and corporate requirements ▪ SB Intuitions' initiatives in developing homegrown LLMs ▪ Current status and challenges of large-scale data crawling in LLMs
3rd meeting: December 2024	▪ AI ethics from ESG and institutional investor perspectives ▪ Initiatives for the safety of large language models
4th meeting: March 2025	▪ Fair cultural representation in LLMs ▪ SoftBank's risk-based approach and risk assessment case studies

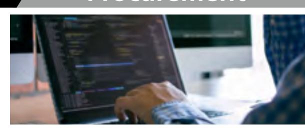
* Enterprises and organizations responsibly address issues and potential risks such as ethics, privacy, and security related to AI, and develop and provide reliable and fair AI services.

Major initiatives

Establishing AI governance operations to support business implementation

We have established processes to be followed at each stage of AI-related business: “planning/design,” “development/procurement,” and “operation.” During planning/design, we assess the severity and impact of risks using a proprietary risk assessment framework based on references such as the EU AI Act. We also conduct discussions based on a predefined checklist to identify potential risks such as unethical information, copyright infringement, and data bias. For high-risk projects in particular, we hold review meetings that include executive officers. After development, we use the checklist again to confirm the status of responses to potential risks and ensure safety, transparency, and accountability, and also hold council meetings with departments involved in AI risk and governance. After the start of operations, we continuously monitor for issues such as deterioration in prediction accuracy, trends in laws and regulations, and the need for system policy revisions, and prepare for unexpected risks by providing appropriate information to users. Through this consistent process, we achieve a balance between innovation and governance.

Overall process

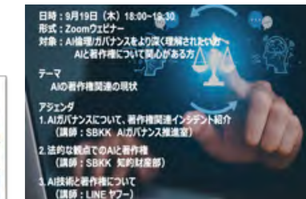

Planning/Design	Development/Procurement	Operation
Consultation/Guidance	**Check/Guidance**	**Review/Evaluation**
▪ Unethical information ▪ Copyright infringement ▪ Data bias	▪ Safety ▪ Transparency ▪ Accountability	▪ Prediction accuracy degradation ▪ Regulatory trends ▪ System policy review

Implement **risk-based measures (risk-based approach)** for each project

Promotion of AI ethics and governance education

In our AI governance promotion strategy, we position “AI ethics and governance education” as a top-priority measure. We conduct ongoing awareness-raising activities for all employees, including executive officers, through annual e-learning training, biannual study sessions, and monthly email newsletters. The training focuses on key themes such as AI incident case studies from Japan and overseas, points to consider when using generative AI (such as bias, information leakage, copyright infringement, and hallucinations), and social trends surrounding AI ethics, aiming to improve the AI literacy and ethical awareness of all employees.

Various initiatives

e-learning	Online study session	Email newsletter delivery
		
Once a year, e-learning on AI ethics and governance is provided for all employees. The content is explained in an easy-to-understand manner using manga and other materials.	Study sessions on themes related to AI ethics and governance are held **twice a year**.	Company-wide newsletter on themes related to AI ethics and governance is distributed **monthly**.

Participation in the “Hiroshima AI Process Reporting Framework” to achieve responsible AI

The “Hiroshima AI Process” is a G7-led framework for international rule-making on generative AI. In this process, “International Guiding Principles” for all AI stakeholders and an “International Code of Conduct” for organizations developing advanced AI systems were established. Furthermore, a “Reporting Framework” (hereinafter, “the Framework”) has been created for AI development companies and others to self-assess and report on their level of compliance with this Code of Conduct. This has established a system to promote responsible AI development throughout the international community.

We have endorsed the purpose of this international consensus-building and announced our participation in the Framework. Going forward, we will utilize the Framework to self-assess and report on our governance status, including risk management and ensuring transparency based on our AI Ethics Policy. By doing so, we will fulfill our accountability to society and promote responsible AI development as a member of the international community.