Resilience Risk Management and Crisis Management

Risk Management enhancement including to foster Risk Culture remains one of our important focuses over the medium-to-long term. Nomura pursues continuous efforts to further promote and maintain Risk Culture as well as to appropriately manage risks under a robust and sophisticated risk management governance and framework, in order to add value to our clients and all other stakeholders.

On the other hand, on the back of financial instability in recent years, there has been increasing attention to ensuring "Resilience" including the elaboration of Recovery and Resolution Planning. Nomura has established a new team to lead and supervise the Group's resilience and related responses, aiming to accelerate the enhancement of overall Crisis Management. Under heightened uncertainty, we remind ourselves that it is an important perspective, which all of our businesses should keep in mind, to ensure and enhance our own resilience (the ability of financial institutions to continue to provide important business services at the minimum level of resilience that should be maintained in crisis).

〉〉Risk Management

2021

2022

2023

Risk Management Enhancement Program kicked off

CONDUCT for OUR PEOPLE

07 Managing risks appropriately

We will deepen our knowledge and understanding on risks, properly recognize and evaluate them, and actively engage in risk management. We will assume appropriate risks to pursue the improvement of Nomura Group's corporate value and provide the highest quality of services to our clients. Each employee is accountable and will work together to prepare for all possible contingencies.

Managing risks appropriately: ✓

- □ We understand we are accountable, have ownership in risk management and will be proactive in mind and action without leaving things to others
- □ In order to maintain trust from all of our stakeholders, we will not only comply with the rules and regulations concerning risk management but also take appropriate actions with integrity, based on understandings of the purpose and background of the rules, and with the highest expertise and ethical standards required of financial institutions
- □ We acknowledge we may underestimate risks or take wrong actions. In case we recognize any risk management concerns or issues, we have a responsibility to proactively and promptly escalate concerns to our managers and relevant departments, even when not directly involved in the business
- □ We will strive to create a psychologically safe workplace, respecting each other's opinions and do not treat in disadvantageous manners. As an organization we will recognize risks correctly and make appropriate decisions

31
CODE of CONDUCT

CHALLENGE
建設的な牽制

ESCALATE
報連相の徹底

RESPECT
尊重しあえる関係

The Steering Committee for Enhancement of Risk Management integrated into the Group Risk Management Committee

For history details, please refer to the Nomura Report 2023 (page 73-74)
https://www.nomuraholdings.com/investor/library/ar/2023/pdf/nomura_report_73_74.pdf

On December 25, 2025, the Nomura Group will celebrate 100th Anniversary. We continue to focus on enhancing risk and crisis management as important initiatives to strengthen the Group's foundation for the next 100 years.

2024

2025

〉〉Crisis Management

Resilience Department established

Nomura Group Crisis Management Committee reorganized

Typical examples that fall between Risk Management and Crisis Management are Business Continuity Management and cybersecurity measures.

Business Continuity

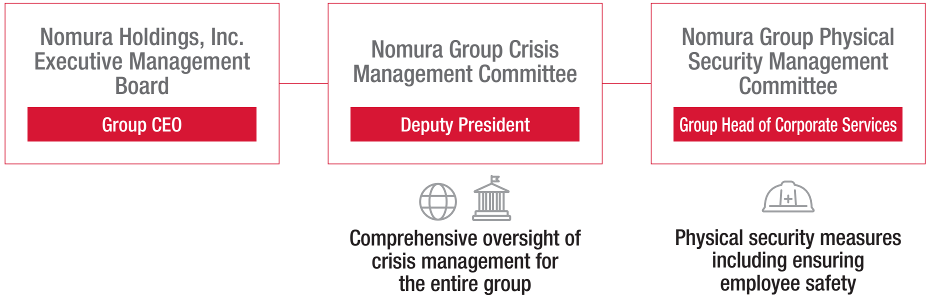
To prepare for crises such as natural disasters like earthquakes and typhoons, human disasters like fires and terrorism, and infectious diseases, we continue to review and reconsider business continuity plans, conduct multifaceted assessments, and provide training to ensure the protection of human life, physical security, and mitigate the impact and ensure swift recovery in the event of business interruption.

Basic Idea

The purpose of the business continuity management within the Nomura Group is to ensure the continuation of Nomura Group's operations in the event of a crisis, while ensuring the following items are reliably executed. Our clients are at the heart of everything that we do, and being available to our clients, particularly in times of crisis, is essential. Equally, we cannot serve our clients unless we protect our people. Group Resilience is an important business function that ensures our staff and assets are prepared for any disruption, and able to serve our clients.

- **Ensuring the safety of executives and staff**
- **Protection of material information and assets**
- **Minimization of losses, risks, and business interruptions**
- **Protection of reputation and brand**
- **Compliance with supervision and instructions from regulatory authorities**

Management Structure



Nomura Holdings, Inc. Executive Management Board

Group CEO

Nomura Group Crisis Management Committee

Deputy President

Comprehensive oversight of crisis management for the entire group

Nomura Group Physical Security Management Committee

Group Head of Corporate Services

Physical security measures including ensuring employee safety

In April 2024, we reorganized the Nomura Group Crisis Management Committee and are accelerating efforts to strengthen the resilience across the Group. The Nomura Group Physical Security Management Committee will continue to be responsible for responding to natural disasters and other events as before.

Key Initiatives

In terms of disaster prevention, we conduct evacuation drills and initial fire extinguishing training using fire extinguishers in the office, assuming a scenario where a fire actually occurs after a large-scale earthquake to prepare for disasters. For emergency stockpiling, we have prepared more than three days' worth of drinking water, food, blankets, and portable toilets so that employees can stay in the facility in cases where it is difficult to return home due to disasters such as earthquakes. Regarding business continuity, we have established backup offices in anticipation of the scenarios where major headquarters are damaged and rendered unusable by earthquakes. We also conduct tests for business continuity at the backup offices assuming actual disasters have occurred. For systems, we strive to ensure quick recovery in case of malfunctions by setting up backup data centers in remote locations. We have also strengthened infrastructure such as private power generation equipment to prepare for systemic risks and continue important operations from the standpoint of avoiding local disasters as well as wide-area disasters such as Tokyo Inland Earthquake.

Cybersecurity

In order to protect our clients' data and assets from increasingly serious cybersecurity threats and to ensure that our stakeholders can continue business with us with confidence, Nomura continues the efforts to maintain and strengthen our cybersecurity measures through teamwork and leadership of Group Chief Information Officer (CIO) as well as Nomura Group Crisis Management Committee and Group Risk Management Committee.

Basic Principles

» Organization management

At normal times, we take part in cybersecurity drills, conduct Threat-Led Penetration Test, assess cyber risks and monitor actions taken by overseas subsidiaries and outside contractors in a constant effort to heighten our readiness. In the case of an incident such as obtaining dangerous vulnerability information or detecting a cyber-attack, the CSIRT(Computer Security Incident Response Team) leads the efforts to analyze the cause, minimize damage, and quickly restore systems.

» System security measures

We adopt a multi-layered defense system, which includes multiple detection and defense mechanisms against unauthorized access and malicious programs such as computer viruses. We review these countermeasures as appropriate to deal with new threats.

» Human-level response

In accordance with the Nomura Group Information Security Policy, relevant seminars and training programs are regularly provided to all executives and employees and they are kept alert in order to raise their awareness and knowledge about cybersecurity.

» Cooperation with outside organizations

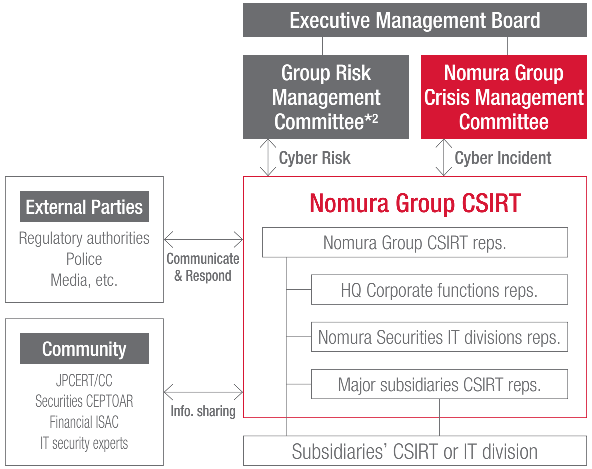
Nomura is cooperating with information sharing organizations such as Financial ISAC Japan and FS-ISAC and cybersecurity vendors to gather and share information on the cyber attackers and their approaches.

※1 ISAC: Information Sharing and Analysis Center

Governance

The Group Risk Management Committee (or its subordinate committee chaired by Group CIO), based on a delegation from the Executive Management Board, covers critical security topics such as resources in cybersecurity risk mitigation and governance, cybersecurity risks, as well as security incidents and cyber tabletop simulations.

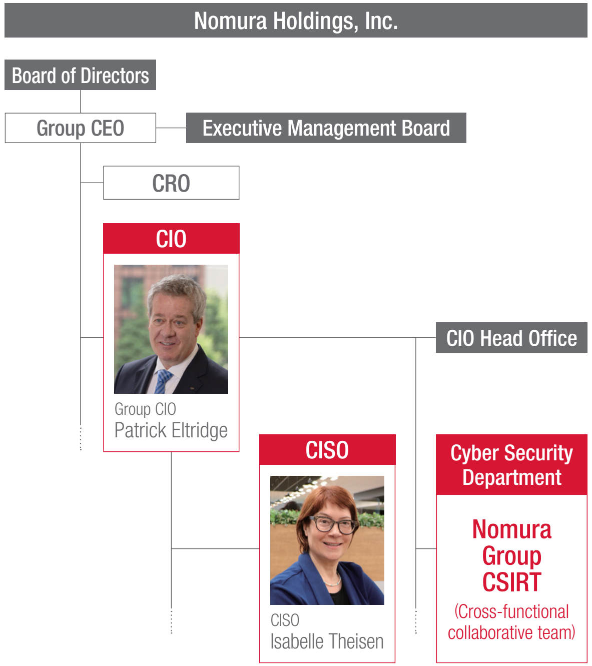
In addition, immediate escalation will be taken for potentially material cybersecurity events according to Nomura's security incident response process including Crisis Management perspectives.


Executive Management Board
Group Risk Management Committee*2
Nomura Group Crisis Management Committee
Cyber Risk
Cyber Incident
External Parties
Regulatory authorities
Police
Media, etc.
Communicate & Respond
Nomura Group CSIRT
Nomura Group CSIRT reps.
HQ Corporate functions reps.
Nomura Securities IT divisions reps.
Major subsidiaries CSIRT reps.
Community
JPCERT/CC
Securities CEPTOAR
Financial ISAC
IT security experts
Info. sharing
Subsidiaries' CSIRT or IT division

*2 On practice, periodic report after detailed deliberation by a subcommittee chaired by the Group CIO

Organizational Structure

Cyber Security Department was established in April 2024 as a specialized unit to analyze and respond to growing threats. A Chief Information Security Officer (CISO) was also hired to drive the cyber risk mitigation and control improvement program.



Major Initiatives

» Technical measures

Nomura's cybersecurity programs are designed to be in line with industry best practice standards and include core capabilities such as Security Governance, Security Awareness and Training, Threat Intelligence & Management, Security Operations Management, Vulnerability Management, Application Security, Data Security, and Identity and Access Management.

Nomura is regularly engaging various external service providers to perform independent assessments of our cybersecurity programs and controls. The results from these independent engagements are integrated into updates to our cybersecurity strategy as appropriate. We also conduct our own regular internal security assessments, such as penetration testing, vulnerability scanning, red teaming, and tabletop cyber attack simulations.

From Risk Management perspectives, Nomura has developed a Third-Party Security Risk Management program that monitors and assesses the cybersecurity controls of our third-party vendors, which include, among others, service providers, SaaS providers, contractors, consultants, suppliers, etc. This program provides a consistent, controlled, cross-divisional approach to managing the services provided by third-party vendors. We perform various risk identification activities including onsite reviews for critical suppliers. Security risks and exceptions observed are monitored per our global Operational Risk Management framework.

» Training and culture for cybersecurity

Nomura recognizes that in order to ensure cybersecurity and information security on an ongoing basis, it is essential to embed a culture that reflects the daily awareness and actions by each and every employee on the ground, not just by those in specialized units such as IT, and not just by strengthening technical measures and infrastructure.

Therefore, we have a variety of initiatives within the Group to ensure that all officers and employees have a necessary vigilance against the threats of cyber attack and ability to take actions as needed.

For example, we provide mandatory training for all employees and targeted attack email training, and we plan a campaign to promote proactive awareness, such as an event inviting cybersecurity expert as external lecturer as an opportunities to learn about the latest threats and the key points of data security, and providing awards to those with a high awareness of cybersecurity.

Furthermore, we continue our organization-wide efforts to strengthen the effectiveness of management and controls, for example by participating in exercises organized by supervisory authorities and conducting internal global exercises on cybersecurity.