



Fundamental approach

Nomura Group has established processes to accurately identify risks arising from all types of operations and trading, and is working to bolster risk evaluation and the risk management framework.

Key risk types



Risks taken by Nomura Group differ by divisions or businesses. We have established a risk management framework based on risk profiles. Nomura Group has adopted a multi-faceted risk evaluation process to avoid risks that may be damaging to our reputation. Risk management oversight is carried out by the committees comprising members of senior management. The Global Integrated Risk Management Committee (GIRMC) and the Global Risk Management Committee (GRMC), for example, deliberate and decide on risk management issues material to the firm.

Unavoidable risks

Operational risk	Risk of suffering losses due to internal administrative processes, people, or systems being either inappropriate or not functioning properly.
Model risk	Risk of loss arising from model errors, incorrect or inappropriate model application with regard to valuation models and risk models.
Liquidity risk	Risk of losses arising from a potential lack of access to funds or higher cost of funding than normal levels due to deterioration in Nomura's creditworthiness or deterioration in market conditions.

Selective risk taking

Market risk	Risk of loss in the value of financial assets and liabilities, as a result of market move in risk factors including interest rates, foreign exchange, and price of securities.
Credit risk	Risk of suffering losses when a borrower is unable to make payment and fail to meet a contractual obligation.

Risks that must not be taken

Compliance risk	Risk that can lead to administrative punishment, economic losses, and reputational damage when Nomura executives or employees violate laws and regulations. Compliance risk also includes risk of losses caused by violating Nomura Group's Code of Ethics and other internal policies and guidelines, including harassment.
-----------------	--

Risk Management

Risk culture

Fostering a sound risk culture is essential for Nomura Group to maintain its social credibility and sustain its business activities. At Nomura Group, all employees, irrespective of their function or geographic location, must understand their specific responsibilities related to risk management, and actively work to manage risks.

Risk management policy

Our business activities are exposed to various risks including market risk, credit risk, operational risk and liquidity risk. Properly managing these risks is one of management's top priorities. It is important for us to maintain capital adequacy and achieve business plans under any type of economic environment, to protect our clients, and to comply with laws and regulations. Nomura Group has defined the types and maximum levels of risk that the firm is willing to take, as documented in the Risk Appetite Statement. Our Risk Appetite Statement and risk appetite are approved by the Executive Management Board, and the risk is monitored daily against a set of risk appetite. If by any chance risk amount exceed risk appetite, the senior management consults with stakeholders and takes actions to solve such excess.

Risk management approach at Nomura Group

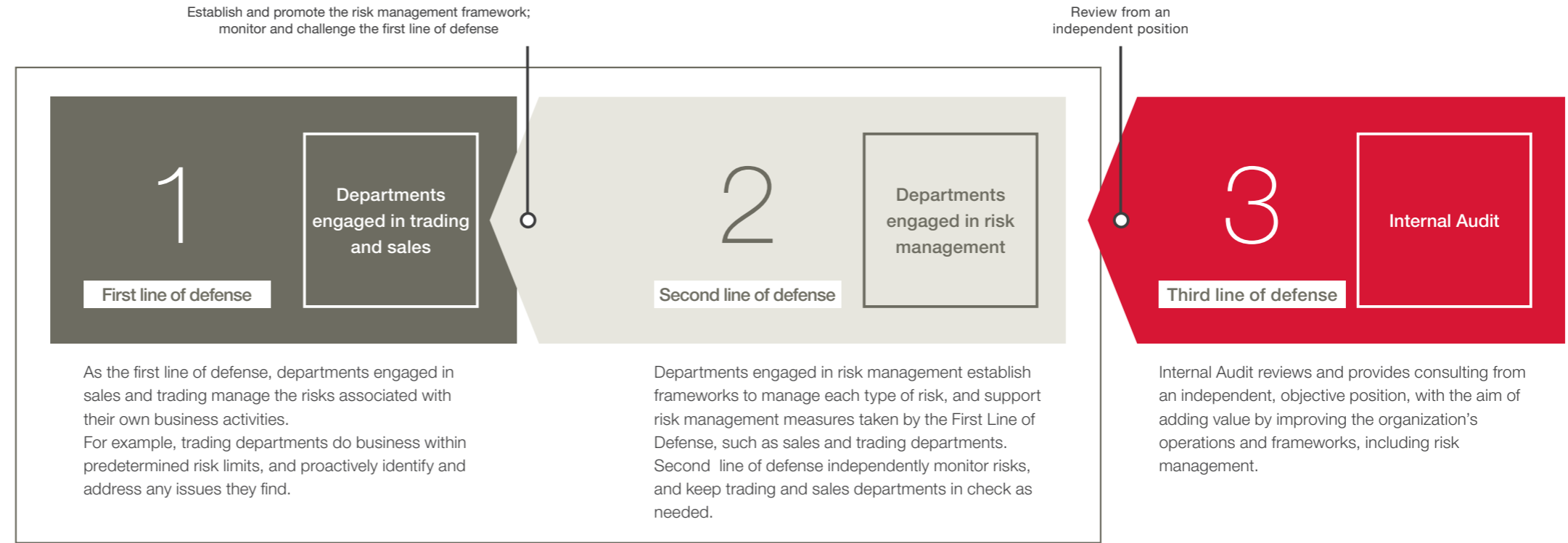
- Implemented frameworks to evaluate and control the possibility of risks arising from the firm's operations and transactions.
- Quantifying risks as much as possible.
- Taking a prudent approach to risks which are outside the area of experience and knowledge, and those that are difficult to control by hedging or other mitigating actions.

Setting risk appetite and guidelines for:

Capital adequacy and balance sheet measures	to comply with capital regulations imposed on financial institutions and to maintain a strong financial base in continuing to conduct businesses under various economic conditions.	Market risk and credit risk	to manage market risk and credit risk within wholesale businesses.
Liquidity risk	to maintain sufficient liquidity to survive a severe liquidity situation and to comply with regulatory requirements.	Operational risk	to understand and mitigate the impact and likelihood of operational risk events assumed in the course of conducting business.
		Compliance risk	to promote proper understanding and compliance with the letter and spirit of all applicable laws, rules and regulations and avoid misconduct.

The three lines of defense in risk management

Nomura Group has adopted the following layered structure on the grounds that all employees are accountable for proactively managing risk.



Chief Risk Officer Message



Risk Culture In Nomura

Lewis O'Donald
Chief Risk Officer (CRO) (based in London)

In Nomura we have a significant reliance on strengthening risk management. What do we mean by this in practice? First to define our goals in risk management for Nomura: it is to make sure Nomura is resilient to market shocks and unexpected threats and that we have hence have enough capital to continuously run our business. It is also to make sure the returns we make on this capital – our shareholders capital – are appropriate and in alignment with our strategic goals. The terminology of Risk can be intimidating. But at its core it is simple. At Nomura, – the executives and the board as the firm's representatives – defines a risk capacity: the maximum amount of risk the firm would want to take. Then it sets a risk appetite: the amount of risk the firm wants to use – of its capacity – in pursuit of its strategies. This appetite is allocated

into the divisions and sub-divisions of the firm in accordance with its business plans. What we mean by risk here can be many things – but risk management tries to use measures – think a ruler to tell which risk is larger than another – which distil many risks into one number. The actual methodology used in this measurement has a degree of complexity and can be technical, but it is important for all our employees to be aware of the risks they take on for Nomura in the course of business. This is one of the most important tenets of risk management at Nomura – that we are all risk managers, and we have responsibility for the actions we take when we expose – knowingly or unknowingly – Nomura to risk. This idea that we are all risk managers is an intrinsic part of our risk culture. Culture can be a hard idea to encompass, so what do I mean by Nomura's risk culture: I

mean how we see and experience people in Nomura reacting and interacting with each other over risk outcomes. We want our risk culture to be strong and control focused and to permeate the organization organically, and to influence our people when they must take decisions which affect the firm. It is difficult to measure, and it is hard to change, but we try to develop ours through training, through incentives, through mentoring and good practice and through leadership. Our culture is built from our Corporate philosophy and the values we espouse: Entrepreneurial leadership, teamwork and integrity. We try to continuously remind our employees both of their legal requirements as well as their obligations to the firm through training; we also hold "Nomura Founding Principles and Corporate Ethics Day" each year where we re-inforce our message and why it is


important for all of us. Lastly we work hard at giving a clear 'tone from the top' showing that our senior managers live and breathe the highest standards of conduct and ethics every day. By continuing to emphasize our culture and our conduct in the markets and to our customers we believe we will continue to build a firm with the highest standards in the marketplace, to the benefit of our clients and our stakeholders.

Stress testing

Nomura Group conducts stress testing to address risks that may spread globally, and to identify risks that are difficult to recognize with statistical methods alone, as well as to prepare for unprecedented risk events. Stress testing uses stress scenarios to assess the impact


on our business and financial soundness should those adverse events occur. These scenarios may include severe deterioration in the economic environment, geopolitical conflicts and natural disasters.

Examples of stress scenarios




Assessment of capital adequacy under the scenario that a serious economic situation that occurred in the past happens again (Example: Financial crisis)

Assessment of the impact on Nomura's earnings of extreme economic conditions that could occur in the future (Example: Economic collapse in a particular country or region)




Assessment of the impact on Nomura's portfolio of political events in Japan or overseas (Example: UK referendum on leaving EU)

Assessment of the impact on Nomura's earnings of a large-scale natural disaster (Example: earthquake directly under the Tokyo metropolitan area)



Chief Risk Officer Message

Risk is a possibility of suffering unexpected losses caused by any number of reasons. Then what is risk management? In short, I think the risk management is an approach of how to reduce this uncertainty. In many financial institutions including Nomura, risk management starts with understanding the risks by quantifying them. Needless to say, no one can predict the future, so the banks collect data from past events, and use some statistical techniques to estimate what to expect in the future. As history repeats itself, looking back on the past may have positive implication for future prediction. That said nothing can be estimated with 100% accuracy.

Yuji Nakata

Executive Managing Director
Head of Group Entity Structure and Co-CRO



So, what can be done to reduce the unexpected? Let inspirations and imaginations run at every possible direction and get prepared. That is the basics of risk management. At the same time, prepare for the worst on the premise that no matter how

hard we try to predict, unexpected things will happen. In financial institutions we prepare for the worst, or turning unexpected into expected, by maintaining adequate capital levels.

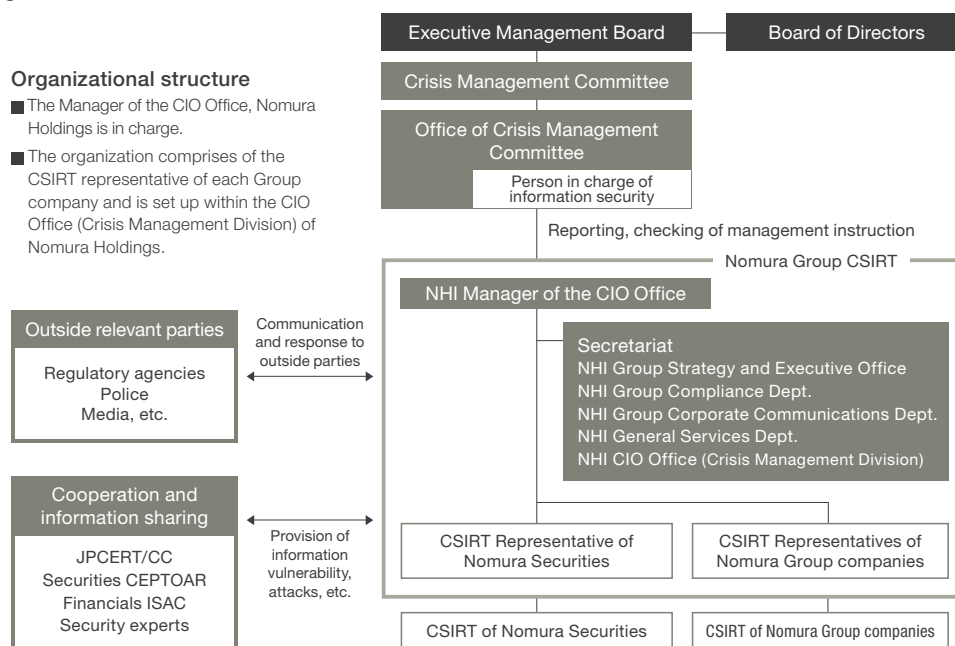
Cyber security measures

Nomura Group has for some time been undertaking security measures to protect systems against cyber-attacks. However, in light of the increasingly serious cyber security threats throughout the world, we recognize that our current countermeasures may not be sufficient in the future.

In order to ensure that clients' information and assets are securely protected from these increasingly challenging cyber security threats, and to enable clients to conduct transactions with peace of mind, Nomura Group is working to strengthen its cyber security platform, using the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc of the Financial Services Agency, the Cybersecurity Management Guidelines of the Ministry of Economy, Trade and Industry based on ISO27001 and ISO27002 as a reference.

Cyber security system

Nomura Group, as a whole, has established a global organizational structure to deal with incidents stemming from cyber-attacks and to minimize potential damage. The Nomura Group Computer Security Incident Response Team (CSIRT), formed within Nomura Holdings, has spearheaded the formation of a CSIRT in Nomura Securities and other Group companies, and governs the CSIRT in each Group company. Each CSIRT works to protect its company's operational and information assets, as well as systems, promoting cyber security measures from four factors: organizational management, system security measures, human-level response, and coordination with outside organizations.



Organization management

We continuously strive to enhance our cyber security platform at “normal times” by taking measures such as participating in drills to protect against cyber-attacks, by having the effectiveness of our measures evaluated by outside cyber security experts, and by knowing the status of measures taken by outside vendors. In the case of an incident such as dangerous, vulnerability information or detection of a cyber-attack, the CSIRT 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

Based on the Nomura Group Information Security Policy, relevant seminars and training programs are regularly provided to all executives and employees in order to raise their awareness and knowledge.

Cooperation with outside organizations

Nomura Group has established information collection and sharing systems related to cyber-attackers and attack methods, through information sharing organizations such as Financials ISAC Japan and Nippon CSIRT Association, as well as FS-ISAC (U.S.) and other overseas organizations.