Economic Security as a New Priority for AI Governance

Jun Tsutsumi

11 November 2026

Iakyara vol.422

Nomura Research Institute, Ltd.



Jun Tsutsumi
Senior Chief Researcher
Financial Technology Solution Division

Executive Summary

Use of AI to identify and rectify cybersecurity vulnerabilities has increased sharply following the revelations surrounding Claude Mythos. Looking ahead, economic security risk assessment will become essential, alongside existing measures to address more familiar risks such as hallucinations and information leaks. Particular attention should be paid to establishing governance frameworks that account for export controls on AI models.

AI governance through model risk management

The revelations following Anthropic's release of a preview version of its Claude Mythos model have accelerated the use of AI to assess cybersecurity vulnerabilities. At the same time, they have heightened awareness of the risk that AI itself could be weaponized by malicious hackers.

Against such a backdrop, Japan's Financial Services Agency (FSA) published an updated version of its 2025 *AI Discussion Paper* in March 2026. The paper presented examples of AI use cases and identified challenges to be addressed based on survey responses and other input from financial institutions.

Japanese financial institutions are using AI not only to improve their day-to-day operating efficiency but also for a wide variety of other use cases such as credit screening and AML/CFT. The paper also highlighted initiatives to establish AI governance frameworks. It reported that many financial institutions are taking a trial-and-error approach to using AI responsibly, adjusting their practices as AI applications expand in scope and sophistication. The paper's inclusion of such content implies that regulatory authorities are keenly interested in development of AI governance.

As generative AI technology advances at a rapid pace, Japanese financial institutions' approach to AI governance as AI users is in a state of flux. In Europe and the US, AI governance is commonly incorporated into model risk management (MRM) frameworks. This is because AI, broadly defined to include generative AI, generally fits the definition of a "model" used in MRM: a quantitative method, or a combination of such methods, that processes input data according to specified

©2026 Nomura Research Institute, Ltd. All Rights Reserved.

logic or assumptions to produce outputs such as estimates, forecasts, scores or classifications.

Examples include the Basel Committee on Banking Supervision's *Digitalisation of finance*, published in May 2024, and the US Treasury Department's *Artificial Intelligence in Financial Services*, both of which base AI governance on MRM frameworks. However, the *Supervisory Guidance on Model Risk Management* (SR Letter 26-2), jointly issued by the US Federal Reserve Board and other regulators in April 2026, refrained from prescribing rules for the time being. Instead, it allows financial institutions to individually make their own AI governance decisions in light of the uncertainties surrounding the ultimate outcome of AI's rapid evolution.

Europe and the US thus recognize the need for AI governance and broadly favor incorporating it into MRM. Nevertheless, the rapid pace of technological change has prevented the establishment of uniform governance practices across the financial sector, even in the US. At the same time, as AI is increasingly used to enhance conventional models, including financial, valuation, credit risk and credit screening models, it is becoming difficult in practice to separate AI governance from existing MRM frameworks.

Export controls are an essential AI-governance consideration

In November 2021, Japan's FSA published its *Principles for Model Risk Management*, setting out eight principles and several key concepts, including the three lines of defense. Designed to apply to a broad range of models rather than specific categories, these principles could also provide a foundation for AI governance.

Putting them into practice would require financial institutions to establish MRM frameworks that encompass not only conventional models enhanced by AI, such as financial, valuation, credit risk and credit screening models, but also AI models themselves, given the variation in their behavior across different AI models.

For example, the model approval function (Principle 4) would be assigned to the risk management department, which serves as the second line of defense under the FSA's three-lines-of-defense framework. Explicit criteria for reviewing and approving AI models are currently lacking in Japan but pertinent reference resources are available, including the Ministry of Economy, Trade and Industry and

©2026 Nomura Research Institute, Ltd. All Rights Reserved.

the Ministry of Internal Affairs and Communications' jointly issued *AI Guidelines for Business* and the AI Safety Institute's *Guide to Evaluation Perspectives on AI Safety.*

Another important consideration is AI's dual-use nature: the technology has applications in both commercial and military or national security contexts. Financial institutions must therefore ensure that their AI model review and approval processes account for compliance with export controls, an area that has generally fallen outside their traditional scope of concern.

AI-related technology, software and hardware are subject to US export controls, reflecting tensions between the US and China, currently the two leading countries in terms of AI models' development and evolution. US export controls apply extraterritorially to Japan to the extent that Japanese entities use US products or technologies in their products or services. If a Japanese financial institution were to hypothetically be blacklisted by the US government for violating US export controls, it would face existential risks such as loss of access to US products. Japanese financial institutions consequently cannot avoid complying with US export controls.

The US restricts exports of certain high-performance GPUs, including those manufactured by Nvidia, and various AI models to designated countries. Meanwhile, the US Congress is now deliberating on a bill named the Remote Access Security Act (RASA), which is based on the premise that restrictions on physical exports of technology and software are insufficient.

If the bill passes, remote access would be legally deemed equivalent to an export. Having passed the House of Representatives, the bill is awaiting a Senate vote, although the timing remains uncertain. In the meantime, financial institutions would be well advised to proceed on the assumption that the US already treats remote access as effectively equivalent to an export.

Under this interpretation, any instance where an AI system hosted in Japan is accessed by a foreign company located in a country subject to US export controls, or even by a Japanese company with a beneficial shareholder located in such a country, could be within the purview of US export controls even if no actual physical transfer of hardware, software or other technology takes place.

©2026 Nomura Research Institute, Ltd. All Rights Reserved.

As a safeguard against such legal compliance risk, US AI models' license agreements exhaustively list the countries where the model is permitted to be used based on a broad interpretation of US export controls.

Accordingly, the model approval process under the FSA's MRM framework (Principle 4) must include verification that the intended users of an AI model do not include group companies or service providers, including subcontractors, with a physical presence or beneficial shareholder outside the geographic scope permitted by the license agreement. Appropriate security settings must also be implemented to ensure compliance with these geographic restrictions.

That said, it would not be realistic to expect an existing model management unit within a financial institution to be solely responsible for vetting everything from export controls to high-level security settings' adequacy. Financial institutions should therefore lay the necessary groundwork for cross-organizational collaboration before appropriately integrating AI governance into their MRM frameworks. This could involve establishing committees with representatives from relevant departments, drawing on external expertise, or combining both approaches.

©2026 Nomura Research Institute, Ltd. All Rights Reserved.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $5.1 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including Tokyo, New York, London, Beijing and Sydney, with over 16,800 employees.

For more information, visit https://www.nri.com/en

The entire content of this report is subject to copyright with all rights reserved.
The report is provided solely for informational purposes for our UK and USA readers and is not to be construed as providing advice, recommendations, endorsements, representations or warranties of any kind whatsoever.
Whilst every effort has been taken to ensure the accuracy of the information, NRI shall have no liability for any loss or damage arising directly or indirectly from the use of the information contained in this report.
Reproduction in whole or in part use for any public purpose is permitted only with the prior written approval of Nomura Research Institute, Ltd.

Inquiries to : Business Planning Department, Financial Technology Solution Division
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

https://www.nri.com/en/knowledge/publication/list.html#lakyara

©2026 Nomura Research Institute, Ltd. All Rights Reserved.