Analytical Report on IT Resilience in the Financial Sector
Executive Summary（July 2026）

- Since 2019, the Financial Services Agency (FSA) has continuously published analytical reports on system failures occurring at financial institutions. In June 2025, the FSA reorganized the report and published it as the "Analytical Report on IT Resilience in the Financial Sector". This year, the FSA has prepared this report, with a view to contributing to the enhancement of IT resilience in the financial sector, taking into the account of the growing geopolitical, cyber, and third-party risks, as well as the increasing reliance of financial institutions' operations and customer services on IT and digital infrastructure.

Report Structure

Part I: Analysis of System Failures

Part II: Assessment of IT Governance Maturity

Part III: Cybersecurity

- ✓ Key issues identified through inspections and monitoring, together with illustrative practices
- ✓ Evolving cyber threats posed by AI and its implications for the financial sector
- ✓ Outsourced study on strengthening third-party cybersecurity risk management
- ✓ Unauthorized access to and fraudulent transactions involving customer's accounts

Part IV: Conducting Cloud Resilience Exercises

Appendix 1 : Collection of System Failure Cases

Appendix 2 : Basel Committee on Banking Supervision (BCBS) Principles for the Sound Management of Third-Party Risk

Column : Migration to Post-Quantum Cryptography

Key Messages

IT environments in the financial industry are becoming increasingly complex. Financial institutions are also relying more heavily on third parties, while cyberattacks continue to grow in sophistication. As a result, risks that could affect the management of financial institutions are increasing. These risks could ultimately have an impact on the stability of the financial system.

In light of these developments, the management of financial institutions needs to recognize IT risk and cyber risk as top management priorities. They should continuously review and strengthen their governance, risk management frameworks, investments, human resource development, and third-party risk management.

At the same time, financial institutions should assume that disruptions and cyber incidents may still occur despite preventive measures. Based on this assumption, they need to strengthen their IT resilience to ensure the continuity of critical operations, the timely recovery of services, and the mitigation of customer impact.

To promote stronger IT resilience across the financial sector, the FSA will continue to encourage both individual efforts by financial institutions and collaborative initiatives across the industry. In addition to inspections and monitoring, the FSA will support these efforts through information sharing, the provision of guidance, and the organization of exercises and other resilience-building initiatives.