BITSIGHT

DATASHEET

Japan’s Guidelines on Cybersecurity in the Financial Sector

Japan’s Financial Services Agency (FSA) recently published new “Guidelines on Cybersecurity in the Financial Sector.” These Guidelines provide detail about basic and desirable cybersecurity measures that financial organizations should implement. They are based on results of past inspections and monitoring by the FSA along with changes in the cybersecurity environment. **Bitsight’s cyber risk management solutions enable organizations to implement a robust cybersecurity program and meet many of the measures outlined by the FSA.**

1. Cybersecurity Management Structure

OVERVIEW OF REQUIREMENTS	BITSIGHT VALUE
• Financial institutions must establish a coherent cybersecurity management system across the organization – including accounting for subsidiary groups and companies, regardless of geography. • Management and the board of directors are responsible for creating and maintaining an effective structure and tracking key performance indicators and risk indicators. • Aim for earliest possible recovery in the event of an incident, coordination must be established amongst departments such as Operations, Planning, Public Relations, Compliance, Risk Management and Audit together with Management. • Cybersecurity risk shall be considered as part of overall risk management of the organization and basic policies for cybersecurity management must be established. • The Board of Directors must establish a Cybersecurity Framework and continuously and dynamically review organizational and technical response measures, and proactively allocate resources.	• Bitsight helps organizations establish strong cybersecurity governance and oversight by providing continuous monitoring, objective metrics that are easily understood and communicated, and reporting. • Its real-time security analytics allow management and the board to track security performance across critical areas of risk and complex business environments. • Bitsight helps management and the board identify strengths and gaps in the security program and ensure the cybersecurity framework aligns with business goals and regulatory requirements. • Reports are easy to create and leverage with internal and external stakeholders; many organizations leverage Bitsight to publicly disclose information about their security programs.

2. Cyber Risk Assessment

OVERVIEW OF REQUIREMENTS	BITSIGHT VALUE
• Financial institutions must have procedures to classify and manage information assets based on their importance, including internal and external systems across different departments. Threats such as perimeter breach, internal misconduct across internal network segments must be considered. • They must have procedures for identifying and assessing cybersecurity risks to the organization and its infrastructure, based on likelihood for cyber attacks and potential impact to the organization's business and information assets. • They must have procedures to manage vulnerabilities to hardware and software and set patching timeframes based on asset importance, risk and severity of the vulnerability. Systems operated by subsidiaries or third parties must be included. • They must properly manage data and networks, including external and third party connections.	• Bitsight's Enterprise Performance and Benchmarking Reports allow organizations to gain a clearer picture of their risk exposure across their entire cyber ecosystem, which is critical for risk identification and effective management of information assets as required by the guidelines. • Bitsight provides cybersecurity performance data and insights based on continuous monitoring of Internet-facing resources, enabling organizations to understand critical risks to their infrastructure and assets across a multitude of risk vectors. • Bitsight provides automated vulnerability assessments and helps organizations maintain strong security postures by continuously scanning for vulnerabilities across systems and infrastructure – including third parties and subsidiaries – helping to uncover issues and minimize cyber risks. • Bitsight's Security Risk Rating and Risk Vector grades provide an objective universal metric for communicating ongoing improvement activities across lines of businesses and geographies.

3. Third-Party Risk Management (TPRM)

OVERVIEW OF REQUIREMENTS

- Due to increasing reliance on third parties, financial institutions need to properly manage risks of their supply chains and establish a cybersecurity management system for the entire third party lifecycle. This includes an organizational structure to manage third-party risk.
- Financial institutions must have a deep understanding of the scope of the cloud services they are using.
- For third-party risk management, financial institutions should conduct diligence (including leveraging external evaluations) and clarify cyber requirements in contract.
- Financial institutions should continuously monitor the cybersecurity risk posed by third-parties and their products and services.
- It is desirable for organizations to consider dependencies on fourth parties and regularly monitor the ability of third parties to manage their fourth/Nth party risks.

BITSIGHT VALUE

- Bitsight is a leader in Third-Party Risk Management. Offering a suite of capabilities that enable organizations to manage the cyber risks across complex supply chains, assess third-party risks, continuously monitor entities, and ensure transparency between service providers and institutions.
- Bitsight enables organizations to perform scalable third-party risk assessments, onboarding, and overall third-party management, while access complementing security artifacts and objective and dynamic security performance data.
- Bitsight's continuous monitoring capabilities provide immediate warnings of changes in third-party security status, including cloud security risk and emergence of 0 day vulnerabilities in the third party and Nth ecosystem.
- Bitsight's fourth-party data helps identify risk concentration and other critical dependencies.
- Bitsight's third-party risk management capabilities ensure the security and integrity of external partnerships.
- Combining the above mentioned with the Security Performance Management use case, Bitsight offers a single universal metric and platform that will allow key decision makers an effective point of reference for cyber risk across their cybersecurity attack surface.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE

BITSIGHT