Module	**Japan – Cybersecurity**
Jurisdictions	**Japan**

Module Application

Does your organisation have adequate cybersecurity measures in place to meet legal obligations, mitigate cyber risks, and ensure compliance with Japanese laws, regulations, and government-issued guidelines?

Is your organisation classified as a 'critical infrastructure operator' or a 'cyberspace-related service provider' required to cooperate with government cybersecurity policies?

Does your organisation have an internal controls system designed to safeguard against cybersecurity risks, breaches, and protect the organisation's data, assets, and reputation?

Are the cybersecurity measures, policies, and practices of your organisation consistent with Japanese government-issued standards and core cybersecurity principles?

Module Scope

The module provides comprehensive guidance to organisations operating in Japan on their cybersecurity obligations. This module addresses compliance requirements under key legislative frameworks, including the Basic Act on Cybersecurity, Act on the Prohibition of Unauthorized Computer Access, and Act on the Protection of Personal Information (APPI), among others. It focuses on establishing effective internal controls, developing a robust cybersecurity framework, and ensuring cooperation with government policies concerning cybersecurity. The module aims to assist organisations in mitigating cyber threats, protecting critical infrastructure, and safeguarding sensitive data while maintaining compliance with applicable laws and regulations.

Key requirements

Organisations in Japan must comply with various obligations to ensure the security of their systems, data, and operations against cybersecurity risks. These include:

1. Development and implementation of an internal controls system:
    - Organisations must establish an internal controls system to ensure legal compliance and protection from cybersecurity risks. Directors are responsible for maintaining and continuously improving these controls to adapt to changes in the cyber threat landscape.
2. Compliance with cybersecurity laws:
    - The Basic Act on Cybersecurity which applies to critical infrastructure operators, cyberspace service providers, and other relevant entities, requiring cooperation with government cybersecurity policies.

- The Act on the Prohibition of Unauthorized Computer Access which ensures protection against unauthorised system access and imposes penalties for violations.
- The Act on the Protection of Personal Information (APPI) which mandates organisations to safeguard personal data, notify relevant authorities of data breaches, and implement robust data protection measures.

3. Cybersecurity risk management and training:
   - Develop a cybersecurity risk management framework to address, mitigate, and respond to identified risks.
   - Conduct regular training and awareness programs for employees on cybersecurity policies, legal obligations, and data protection measures.
4. Incident response and emergency preparedness:
   - Establish a Computer Security Incident Response Team (CSIRT) to handle and respond to security incidents effectively.
   - Develop and maintain an emergency response plan and conduct periodic simulations and reviews to ensure preparedness for cybersecurity breaches or other emergencies.
5. Supply chain security and vendor management:
   - Organisations must regularly review the cybersecurity measures of business partners and third-party vendors to ensure compliance with agreed standards and protect the organisation's overall security posture.
6. Risk assessment and business continuity planning:
   - Conduct comprehensive risk assessments to identify vulnerabilities, evaluate risks, and develop strategies to maintain business continuity in case of cyber incidents.
   - Coordinate with senior management to assess the acceptability of security risks and implement appropriate mitigation measures.
7. Cooperation with government agencies and information sharing:
   - Certain organisations, especially those operating critical infrastructure, must cooperate with government agencies and comply with any special cybersecurity guidelines or directives.
   - Share relevant information on cyber threats, vulnerabilities, and countermeasures with industry peers and government bodies.

Key practices:

- Security policy development: Document a security policy that outlines goals, strategies, and procedures for cybersecurity risk management.

- Employee training and awareness: Ensure employees understand their roles and responsibilities related to cybersecurity.
- Regular reviews and audits: Continuously assess and improve cybersecurity measures to align with emerging threats and regulatory requirements.

Compliance sources

- Basic Act on Cybersecurity (Act No. 104 of 2014)
- Act on the Prohibition of Unauthorized Computer Access (Act No. 128 of 1999)
- Act on the Protection of Personal Information (APPI) (Act No. 57 of 2003)
- Civil Code (Act No. 89 of 1896)
- Companies Act (Act No. 86 of 2005)
- Penal Code (Act No. 45 of 1965)
- Unfair Competition Prevention Act (Act No. 47 of 1993)

Consequences of non-compliance

Failure to meet cybersecurity obligations can result in:

- Theft, financial loss, damage to intellectual property, and increased costs for remedying systems and public relations.
- Liability on directors for damages resulting from inadequate cybersecurity controls, and organisations may face regulatory action from bodies such as the Personal Information Protection Commission (PPC).
- Reputational damage, harm to customer relationships, investors, and business partners, affecting market value and profitability.
