中銀香港(控股)有限公司
BOC HONG KONG (HOLDINGS) LIMITED

Technology Risk Management Policy (Extract)

Purpose

The purpose of this policy is to establish the technology risk management framework and to enhance the technology risk management level, to promote safe, continuous and stable operations, as well as to strengthen core competitiveness and sustainable development.

Technology Risk Management Principles

The Group categorizes technology risk management into different domains, including IT governance, information asset management, use of cryptography, security management, physical and personnel security, system development and change management, information processing, communications networks, management of service providers, cyber security controls, etc.

Core Principles

- Technology risk management shall cover all departments / RPC units, positions, personnel and their daily activities, to ensure that all technology risk can be identified, assessed, monitored, controlled and reported.
- Review and enhance technology risk management on an on-going basis, with respect to the rise of new technology risk management areas and changes in the Bank's business goal and objectives, so as to ensure that the Bank's technology risk management function is able to cover all technology risk areas and support the Bank's business goal and objectives.

IT Governance

- Ensure all staffs are aware of and comply with various technology risk management policy, administrative measures and relevant standards, guidelines and rules.

Information Asset Management

- Establish information assets classification and protection standards.

Use of Cryptography

- Use proper and effective cryptography to protect the confidentiality, authenticity and / or integrity of information

System Security Management

- Information system security shall be managed according to its classified security level. The level of security protection and control shall be adopted in accordance with its security requirements and importance of the system.

Physical and Personnel Security

- Establish and implement appropriate security controls to prevent unauthorized physical access, damage and interference to the Bank offices, facilities, networks, and systems.

System Development and Change Management

- Information systems encompass infrastructure, business applications, off-the-shelf products and services. All information systems shall comply with the Bank's security framework and system development standards to ensure that security and recovery requirements are addressed at the appropriate time in the development cycle.

Information Processing

- Establish complete control plan and proper management procedures to manage technology risk during the process of acquisition, development, operation and maintenance. Information facilities and equipment shall be subject to preventive and corrective maintenance periodically.

Communications Networks

- Establish network infrastructure and security standards. All connecting points between internal and external networks shall be appropriately protected and monitored to prevent unauthorized access.

Management of Service Providers

- Establish management measures to ensure deliverables and services provided by service providers comply with the Bank's information security standards, and set up processes for on-going monitoring, assessment and testing of service providers.

Cyber Security Controls

- Implement necessary measures to protect against cyber attacks, intrusion, interference, damage, illegal use and unexpected events. Ensure network is operated in stable and reliable conditions, and protect the confidentiality, integrity, and availability of information during transmission, processing and storage. Develop threat intelligence processing framework, enhance the collection, analysis, sharing and reporting of threat intelligence and adopted appropriate measures to mitigate the relevant cyber risks.