

SFC Cybersecurity Guidelines for Internet Trading

Hong Kong SFC guidelines set cybersecurity requirements for licensed internet securities traders to protect clients and market integrity.



What it is

Hong Kong SFC — Cybersecurity Guidelines for Internet Trading is a regulatory framework that establishes baseline cybersecurity requirements for securities firms offering internet trading services. The guidelines aim to strengthen the security and resilience of online trading platforms, helping firms protect client assets and maintain market integrity.

Issued by the Securities and Futures Commission (SFC) of Hong Kong, these guidelines apply to licensed corporations conducting internet-based securities trading activities. The framework sets expectations for cybersecurity controls such as user authentication, system monitoring, incident response, and access management, ensuring firms address operational risks and data protection challenges unique to online trading.

At a glance

PUBLISHER

Securities and Futures Commission (SFC)

TYPE

Guidance

VERSION

Current SFC Cybersecurity Guidelines for Internet Trading

EFFECTIVE

2017

DOMAIN

Cybersecurity

FAMILY

Other

REGION

Hong Kong

INDUSTRY

Financial Services

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

Moderate

Source: <https://www.sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf?rev=eb44681c436548c1bb37092f2145f45c>

Why it matters

- **Strengthen cybersecurity governance** Help organizations implement clear policies and robust controls tailored to internet trading risks, improving oversight across critical systems and processes.
- **Enhance regulatory alignment** Facilitate alignment with local SFC requirements and international cybersecurity standards, minimizing gaps during audits and supervisory reviews.
- **Improve incident detection capabilities** Enable earlier identification and response to cyber threats through mandated monitoring, logging, and proactive vulnerability management measures.
- **Protect client assets and data** Reduce the risk of unauthorized access and data breaches, safeguarding sensitive financial information and client holdings.

How SmartSuite supports SFC Internet Trading Cybersecurity Guidelines

Technology Risk Requirement Library Track cybersecurity and technology risk expectations with ownership and evidence.	Secure Configuration and Access Governance Manage hardening, access controls, and privileged access evidence.	Monitoring and Incident Readiness Capture monitoring proof, incident workflows, and escalation documentation.
Internet-Facing System Controls Track controls for online services and trading systems with verification evidence.	Vendor and Outsourcing Oversight Manage provider risk, contracts, monitoring, and contingency planning evidence.	Exam Readiness Reporting Report posture, gaps, and evidence coverage for supervisory expectations.

Common framework mappings

EU DORA

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27018

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

SWIFT CSCF

Official resources

Hong Kong SFC Cybersecurity Guidelines
Provides official guidelines for reducing and mitigating hacking risks in internet trading.
sfc.hk/-/media/EN/assets/components/codes/files-current/web/guidelines/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading/guidelines-for-reducing-and-mitigating-hacking-risks-associated-with-internet-trading.pdf

Frequently asked questions

- What is the purpose of the Hong Kong SFC — Cybersecurity Guidelines for Internet Trading?**
The guidelines are designed to establish minimum cybersecurity standards for licensed firms providing internet trading services in Hong Kong. Their primary aim is to reduce and mitigate hacking risks, protect client assets, and strengthen the security and resilience of online trading platforms.
- Are the SFC Cybersecurity Guidelines mandatory for all organizations?**
Yes, the SFC Cybersecurity Guidelines are mandatory for licensed corporations conducting internet-based securities trading activities in Hong Kong. Compliance with these guidelines is a regulatory requirement, and firms may face regulatory action if they fail to meet the prescribed standards.
- Who must comply with the SFC Cybersecurity Guidelines for Internet Trading?**
All licensed corporations regulated by the Hong Kong Securities and Futures Commission (SFC) that offer internet trading services are required to comply. This includes firms involved in the online trading of securities, derivatives, and associated financial products.
- What are the key cybersecurity controls required by the guidelines?**
The guidelines require controls including strong user authentication, secure system access management, real-time system monitoring, incident detection and response processes, and regular system vulnerability assessments. Firms are also expected to manage third-party risks and ensure data protection for all online trading activities.

How should organizations implement the SFC Cybersecurity Guidelines?

Implementation should start with a cybersecurity risk assessment tailored to online trading operations. Organizations must map the guideline controls to their business and technology environments, deploy required technical and procedural measures, and establish ongoing processes for monitoring, documentation, and incident readiness.

How do the SFC Cybersecurity Guidelines relate to other cybersecurity frameworks or standards?

The SFC Cybersecurity Guidelines complement broader frameworks such as ISO 27001 and global financial sector standards. They provide sector-specific requirements while encouraging alignment with recognized best practices for governance, risk management, and operational resilience.

What are the ongoing compliance requirements for organizations subject to the guidelines?

Organizations must maintain up-to-date control documentation, conduct regular self-assessments, and be prepared for supervisory review by the SFC. Ongoing compliance also requires continuous monitoring for security events, regular training, periodic incident response exercises, and timely remediation of identified risks.

How would SmartSuite support Hong Kong SFC — Cybersecurity Guidelines for Internet Trading?

SmartSuite enables organizations to operationalize the SFC guidelines by providing centralized risk registers, control libraries, and customizable workflows. It supports the collection of evidence, tracking of compliance activities, and preparation for audits through role-based dashboards, automated reporting, and remediation management, helping teams maintain audit readiness and demonstrate regulatory compliance.

License included / downloadable: Yes The SFC Cybersecurity Guidelines for Internet Trading are publicly available through the Hong Kong Securities and Futures Commission.

Full framework page and mappings: smartsuite.com/frameworks/hong-kong-sfc-cybersecurity-guidelines-for-internet-trading