White Paper

IT Security Guidance for Hong Kong Monetary Authority (HKMA)

avanade

What is the Hong Kong Monetary Authority (HKMA)?

What is it?
The Hong Kong Monetary Authority (HKMA) is the government authority in Hong Kong responsible for maintaining monetary and banking stability.[1] Hong Kong is one of the main financial hubs for the Asia Pacific region. The Hong Kong stock exchange alone has a market capitalization of $27.76 trillion HK Dollars (approximately USD 3.5 trillion). The HKMA was established on April 1, 1993, by merging the Office of the Exchange Fund with the Office of the Commissioner of Banking. The is governed by the Exchange Fund Ordinance and the Banking Ordinance, and it reports to the Financial Secretary.

- **Maintaining currency stability** within the framework of the Linked Exchange Rate system
- **Promoting the stability and integrity of the financial system,** including the banking system
- Helping to maintain **Hong Kong's status as an international financial center**, including the maintenance and development of Hong Kong's financial infrastructure
- **Managing the Exchange Fund**, the reserve that backs Hong Kong's currency

Hong Kong's banking structure is comprised of three tiers:[2]

- **Licensed Banks** may provide current and savings accounts; accept deposits of any size and maturity from the public, pay or collect checks; and use the name "bank" without restriction. According to the Deposit Protection Scheme Ordinance, only licensed banks can, and are required to, join the Scheme as Members
- **Restricted License Banks**, many of which are engaged in wholesale and capital market activities, may only take deposits from the public in amounts of HK$500,000 or above without restriction on maturity
- **Deposit-taking Companies** are restricted to taking deposits of HK$100,000 or above with an original term to maturity of at least three months. These companies are mostly owned by, or otherwise associated with, banks and engage in a range of specialized activities, including consumer and trade finance, and securities business.

Securities and Futures Commission
The Securities and Futures Commission is an independent Hong Kong statutory body set up to regulate Hong Kong's securities and futures markets.[3] The HKMA and SFC work closely together to ensure that there is an open market with a level playing field for all intermediaries in the securities industry of Hong Kong.[4] We will discuss both HKMA and SFC guidelines on security and risk management in this document.

Why does HKMA matter?
Cybersecurity threats in Hong Kong continue to rise. Financial losses in Hong Kong totaled HK$1.8 Billion in 2015 alone, and are expected to rise over the next few years.

HKMA places cybersecurity at the forefront of Hong Kong's financial sector Information Technology (IT) defensive strategies. In parallel with the Cybersecurity Fortification Initiative (CFI), HKMA has also launched its Enhanced Competency Framework on Cybersecurity (ECF-C) for banking operations in Hong Kong. While the ECF-C is not mandatory, authorized institutions (AIs) are highly encouraged to adopt the EFC-C and institute its practices to conduct financial operations within the banking sector of Hong Kong.[5]

HKMAs risk management and guidelines are detailed in three main circulars published and circulated by the HKMA amongst their AIs. These circulars are:

1. Enhanced Competency Framework on Cybersecurity[6]
2. Cyber Security Risk Management[7]
3. Cyber Security Fortification Initiative[8]

SFC have also published a list of high level guidelines in their circular to all Licensed Corporations on Cybersecurity.[9]

HKMA Enhanced Competency Framework on Cybersecurity (EFC-C)

The ECF-C is focused on "relevant practitioners," who conduct 1.) IT Security Operations, 2.) IT Risk Management, and 3.) IT Audits.

Formal Qualifications
Relevant practitioners must possess formal qualifications that are recognized by certifications listed in the ECF-C, section 5.1. Formal qualifications are broken down by Core Level, less than five years, and Professional level, more than five years in the cybersecurity functional role. The qualification structure is based upon the three lines of defense concept under cyber risk governance:

- First line of defense: IT Security Operations and Delivery
- Second line of defense: IT Risk Management and Security Controls
- Third line of defense: IT Audits

Key Tasks for Roles under ECF-C
Key tasks are broken down by Core Level and Professional Level roles in the ECF-C. The responsibilities for each role are provided under the headings:

1. IT Security Operations and Delivery
2. IT Risk Management and Control and
3. IT Audit

Further, the ECF-C document details out the certification requirements and the paths to certifications for Core Level and Professional Level Roles.

Recognized Certificates			
	First Line of Defense	**Second Line of Defense**	**Third Line of Defense**
Recognized Certificates	IT Security Operations & Delivery	IT Risk Management & Security Controls	IT Audits
Core Level			
CSX Fundamentals Certificate	✓	✓	✓
CSX Practitioner Certificate (CSX-P)	✓	✓	✓
GIAC Information Security Professional (GIAC GISP)	✓	✓	✓
GIAC Security Essentials (GSEC)	✓	✓	✓
ISC² Systems Security Certified Practitioner (SSCP)	✓	✓	✓
Professional Level			
CSX Specialist Certificate (CSX-S)	✓	✓	✓
CSX Expert Certificate (CSX-E)	✓	✓	✓
ISACA Certified Information Systems Auditor (CISA)	✓	✓	✓
ISACA Certified Information Security Manager (CISM)	✓	✓	✓
ISACA Certified in Risk and Information Systems Control (CRISC)	✓	✓	✓
ISACA Certified in the Governance of Enterprise IT (CGEIT)	✓	✓	✓
ISC² Certified Information Systems Security Professional (CISSP)	✓	✓	✓
ISC² Certified Cloud Security Professional (CCSP)	✓	✓	✓

HKMA Cyber Security Risk Management

Client Data Protection (CDP) Program
This document highlights the need of an updated risk management plan and recommends to the senior management and board members of the member AIs to take cybersecurity seriously, particularly as they are responsible for protecting the critical assets and sensitive information of their customers. The document recommends that the following areas to be covered:

1. Risk ownership and management accountability
2. Periodic evaluations and monitoring of cybersecurity controls
3. Industry collaboration and contingency planning
4. Regular independent assessment and tests

HKMA have also prescribed a list of controls that are preventive or detective in nature:

a) Registration of authorized and restriction on unauthorized devices, software and networks;
b) Secure configuration and access controls of devices, software and networks;
c) Identification and remediation of vulnerabilities of devices, software and networks;
d) Controlled use of privileged user accounts of devices, software and networks;
e) Defenses against malwares and Advanced Persistent Threats (APTs);
f) Security and access controls of application systems;
g) Protection of customer data and sensitive information stored in, or accessible by, different media, devices, software and networks;
h) Security related to IT systems and networks accessible by mobile devices or devices outside the AI's physical security controls;
i) Detection of unusual activities of, and potential intrusions into, IT systems and networks;
j) Management of security related to service providers; and
k) User education and awareness.

Controls that are mainly for dealing with contingency scenarios:

a) Incident responses and management, including controls for digital forensic if appropriate;
b) System resilience, including protection against DDoS; and
c) Data recovery capability.

It is interesting to note that although HKMA have the above prescribed list of controls, there are no specific common framework that has been established for security and risk management. HKMA instead recommend the AIs to adopt the standards set out by international organizations including:

- Control Objectives for Information and Related Technology (COBIT)
- SANS Top 20 Critical Security Controls (CSC)
- Information Security Forum – Standard of Good Practice for Information Security
- ISO/ISEC 27001, 27002 and 27035

HKMA Cybersecurity Fortification Initiative (CFI)

The CFI is a new scheme launched by the HKMA in collaboration with the banking industry to enhance the resilience of HK banks to cybersecurity attacks. The main pillars of this initiative are:

1. Cyber Resilience Assessment Framework (C-RAF) – risk based approach for banks to assess, and
2. Benchmark resilience against cybersecurity attacks.
3. Professional Development Programme (PDP) - a training programme designed to increase the number of qualified cybersecurity professionals.
4. Cyber Intelligence Sharing Platform (CISP) - a platform for banks to share intelligence and to collaborate on cyber attacks.

Cybersecurity controls suggested by Securities and Futures Commission (SFC)

The SFC has also suggested a list of cybersecurity controls to the licensed corporations (LCs) to further enhance their cybersecurity framework

i. Establish a strong governance framework to supervise cybersecurity management;
ii. Implement a formalized cybersecurity management process for service providers;
iii. Enhance security architecture to guard against advanced cyber-attacks;
iv. Formulate information protection programs to ensure sensitive information flow is protected;
v. Strengthen threat, intelligence and vulnerability management to pro-actively identify and remediate cybersecurity vulnerabilities;
vi. Enhance incident and crisis management procedures with more details of latest cyber-attack scenarios;
vii. Establish adequate backup arrangements and a written contingency plan with the incorporation of the latest cybersecurity landscape; and
viii. Reinforce user access controls to ensure access to information is only granted to users on a need-to-know basis.

Outsourcing guidelines for HKMA and SFC

Although the above guidelines and recommended controls are for the Authorized Institutions (AIs – in case of HKMA) and for the Licensed Corporations (LCs – in case of SFC) there are certain specific rules in case of outsourcing of any work related to HKMA and SFC.

For HKMA, the supervisory policy manual[10] has guidelines for the AIs to be followed when outsourcing any data processing or non-core business activities. The document pauses to make the AI aware of the legal obligations under the banking ordnance in relation to their outsourcing plans, which are summarized as:

- AIs to have adequate accounting systems and systems of control;
- Conduct their business with integrity, competence and in a manner, not detrimental to the interest of depositors and potential depositors;
- AIs should not enter into, or continue, any outsourcing arrangements if it results in their internal control systems or business conduct being compromised or weakened after the activity has been outsourced.

The document also lists supervisory concerns that the AI should take note before proceeding with an outsourcing agreement:

The Hong Kong Securities and Futures Commission (SFC) has not published its own guidelines on outsourcing. However, it has endorsed the Principles on Outsourcing of Financial Services for Market Intermediaries, published by the International Organisation of Securities Commissions for financial services firms under the SFC's jurisdiction. These principles cover seven areas of outsourcing:

- Due diligence process in selecting a service provider.
- Contract with a service provider.
- Business continuity issues.
- Client confidentiality.
- Concentration of outsourcing services.
- Termination procedures.
- Access to books and records.

Supervisory concerns that the AI should take note before proceeding with an outsourcing agreement	
Concern	**Detail**
Accountability	Reminder to the senior management that outsourcing can only allow them to transfer day-to-day managerial responsibility, but not accountability, for an activity or a function to a service provider.
Risk Assessment	Recommendation to the senior management to undertake a comprehensive risk assessment addressing: • Importance and criticality of the services to be outsourced • Reasons for outsourcing • Impact on AI's risk profile of the outsourcing Regular re-perform this assessment through the life of the contract.
Ability of the service provider	To perform appropriate due diligence considering the provider's financial soundness, reputation, managerial skills, technical capabilities, operational capability and capacity, compatibility with the AI's corporate culture and future development strategies, familiarity with the banking industry and capacity to keep pace with innovation in the market. To have appropriate controls in place and continuously monitor the performance of the service provider.
Outsourcing agreement	HKMA recommends that the outsourcing agreement be properly documented including contractual liabilities and obligations. This agreement to be regularly reviewed.
Customer data confidentiality	To address this concern, HKMA recommends that the outsourcing arrangement complies with relevant statutory privacy and other requirements by seeking legal advice. Controls to be in place for the staff of the service provider to abide by confidentiality rules. Document the contractual rights of the AI in case of breach of confidentiality. Segregation of AIs data from other customer data residing in the service providers network. Access rights to AI's data delegated to authorized employees of the service provider on a per need basis. In the event of termination of the outsourcing agreement, the document recommends that the service provider allow retrieval or destruction of customer data.
Control over outsourced activities	This concern addresses the outsourcing agreement's terms and conditions and set effective procedures for monitoring contract performance, material problems, regular review of the service providers financial condition and risk profile, and service provider's contingency plan. The document also recommends the above factors through regular internal audits.
Contingency planning	Contingency planning is addressed through recommendations of: • Maintaining and regularly testing them with the service provider; • Ensure that they have an adequate understanding of their service provider's contingency plan; • Consider the availability of alternative service providers or the possibility of bringing outsourced activity back in-house in an emergency.
Access to outsourced data	Stressing the importance of timely access to data this concern reminds the AIs that they should be able to retrieve data from the service providers and that data be accurate and available in HK on a timely basis. Access to the data by HKMA should not be impeded by outsourcing. The AIs should ensure that the outsourcing agreement allows for supervisory inspection of operations and controls of the service provider.
Additional concerns	HKMA lists additional concerns apart from the above: • Understand the risks from overseas outsourcing • Take into consideration that overseas authorities have right of access to customers' data. The AI needs to notify HKMA if overseas authorities seek access to their customers' data. • AIs should notify their customers of the country in which the service provider is located. • AIs should not outsource to a jurisdiction which is inadequately regulated. • Section 33 of PDPO (HK privacy ordinance) has restrictions on transferring of privacy outside HK. • The agreement with the service provider should preferably be governed by HK law. • To have a robust back-up system in an acceptable jurisdiction.

How Avanade help you comply with HKMA and SFC

Avanade understands financial services clients are deeply committed to both protecting their customers and maintaining a trusted reputation in the marketplace. With in-depth knowledge of compliance rules and deep experience with protecting information, Avanade helps organizations utilize robust technology solutions to enhance business operations, while also navigating the complex security and privacy guidelines put in place by HKMA and SFC.

Working with a variety of FIs, each with its own set of objectives and challenges, Avanade has created a broad library of data security best practices that form its **Client Data Protection (CDP) program**. Avanade assigns every engagement to the CDP and, in helping an FI protect its sensitive and personal data, uses a prevention-focused methodology built on the following foundational principles:

- **Senior-level oversight** responsibility for all engagements where client data is accessible
- **Clear communication and documentation** of all CDP requirements
- **Required controls** for secure handling of client data while in Avanade's custody
- **Service-specific controls** tied to vulnerabilities inherent to unique types of work, such as the needs of financial services clients
- **Technology controls** deployed to enforce mandatory baseline protection mechanisms
- **Tools, processes and subject matter specialist support** for project teams
- **Standardized data protection** tools and templates

Program execution begins with a risk assessment to determine each client's risk in relation to their precise project requirements. The second mitigation phase uses an implementation plan consisting of up to 24 control families operated by the project team.

Avanade requires that a CDP plan be established before any delivery tasks begin, and everyone working on behalf of the client engagement must adhere to the plan for the life of the engagement. Plan execution is periodically reviewed by independent internal teams to gauge both compliance and the effectiveness of the controls to manage the client's risk. Any identified gaps are tracked and escalated to the assigned Client Data Protection Executive (CDPE) for corrective action.

Avanade's knowledge of financial services regulations around the world – and its experience helping clients protect their systems and information – have enabled the company to develop effective approaches to security. Avanade knows, however, that every client is different, and each has its own set of requirements and challenges. That is why Avanade makes sure it understands these elements during the assessment process so that the company can develop and put in place the right security controls to fit a client's individual needs. Moreover, Avanade continues to reassess those needs throughout delivery, ensuring that the company provides services that its clients can count on to help keep data safe and systems protected.

Avanade's Client Security Team

Given that there are multiple requirements for both the AI and Avanade as an outsourcing service provider, we recommend for any potential engagements within the purview of HKMA or the SFC, the Client Security team be engaged early to discuss the various requirements. Avanade's internal processes and procedures are sufficiently advanced to cater to HKMA guidelines and a comprehensive and compliant response will be presented to all potential clients.

Summary

Takeaways
HKMA and SFC requirements and guidelines are quite complex due to the nature of various publications and circulars coming out at different times. In this paper, we have summarized all the requirements for a quick overview of the various guidelines as published.

It is important to note that although the AIs need to follow the guidelines and requirements set out in the publications, there are different set of requirements when outsourcing any work to service providers. Avanade understands these requirements, and we are confident that all the requirements can be met for any service provided to the client through us.

What you want the client to do next?
We encourage our clients to visit Avanade trust center at http://www.avanade.com/trust to check out our commitment to Security and protecting client data. We are a 13-time winner of the Alliance SI partner of the year award by Microsoft and recently won the award for the 10th year in a row. The award shows our commitment to work on the Microsoft suite of products and demonstrates our continued effort to work with the global leaders in the emerging governance framework across the globe.

About Avanade
Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation and has 30,000 professionals in 24 countries. Visit us at www.avanade.com

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Africa
Pretoria
Phone +27 12 622 4400
SouthAfrica@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
Asia-Pacific@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

[1] http://www.hkma.gov.hk
[2] Banking Supervision in Hong Kong, 2nd edition, page 19, August 2010, Background Brief Series, Hong Kong Monetary Authority
[3] http:/www.sfc.hk/web/EN/about-the-sfc/our-role/
[4] http://www.hkma.gov.hk/eng/key-functions/banking-stability/banking-policy-and-supervision/supervisory-co-operation.shtml
[5] Guide to Enhanced Competency Framework on Cybersecurity, page 4, December 2016, Hong Kong Monetary Authority
[6] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf
[7] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf
[8] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf
[9] http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=16EC17
[10] http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf