

Code of Practice

Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance

For Authorized Institutions designated by the Monetary Authority as Critical Infrastructure Operators

A Code of Practice issued by the Monetary Authority under Section 8(1)(b)

2 June 2026

TABLE OF CONTENTS

1. INTRODUCTION.....	3
1.1 Purpose and scope.....	3
2. DEFINITIONS AND CONVENTIONS.....	4
2.1 Definitions.....	4
3. DESIGNATION OF CRITICAL COMPUTER SYSTEMS	7
3.1 Designating critical computer systems	7
4. INFORMATION REQUIRED FOR DESIGNATION.....	8
4.1 Requiring information for designating critical computer systems.....	8
5. OBLIGATIONS OF DESIGNATED AIS – DIVISION 1.....	9
5.1 Obligation to maintain office in Hong Kong	9
5.2 Obligation to notify operator changes.....	9
5.3 Obligation to set up and maintain computer-system security management unit	10
6. OBLIGATIONS OF DESIGNATED AIS – DIVISION 2.....	11
6.1 Obligation to notify material changes to certain computer systems	11
6.2 Obligation to submit and implement computer-system security management plan	11
6.3 Obligation to conduct computer-system security risk assessments	20
6.4 Obligation to arrange to carry out computer-system security audits	21

1. INTRODUCTION

1.1 Purpose and scope

- 1.1.1 This Sectoral Code of Practice (this Code) is published by the Monetary Authority (the MA) in consultation with the Commissioner of Critical Infrastructure (Computer-system Security) (the Commissioner) pursuant to section 8 of the Protection of Critical Infrastructures (Computer Systems) Ordinance (the Ordinance).
- 1.1.2 This Code is applicable to an Authorized Institution (AI) designated by the MA as a Critical Infrastructure (CI) operator (Designated AI).
- 1.1.3 This Code provides practical guidance on how a Designated AI complies with category 1 obligations and category 2 obligations. A Designated AI should refer to guidance published by the Commissioner in relation to category 3 obligations, which can be found in section 7 of the Code of Practice (Generic) published on the website of the Office of the Commissioner ([hyperlink to https://www.occics.gov.hk/en/industry/code-of-practice/index.html](https://www.occics.gov.hk/en/industry/code-of-practice/index.html)).
- 1.1.4 A Designated AI should refer to relevant sections and/or schedules of the Ordinance at all times when applying guidance provided in this Code to ensure compliance with legal obligations.
- 1.1.5 This Code is not subsidiary legislation, nor would failure to comply with the provisions of this Code in itself constitute an offence. However, the MA may issue written directions to require a Designated AI to take appropriate actions in relation to the compliance with category 1 obligations and category 2 obligations if there has been non-compliance or defective compliance with such obligations, which may be considered with reference to this Code. Failure to comply with such directions would be an offence.
- 1.1.6 A Designated AI should provide information, which is accessible in or from Hong Kong, to the MA upon request in relation to the compliance with category 1 obligations and category 2 obligations.
- 1.1.7 This Code sets the baseline requirements for protecting critical computer systems (CCSs) of Designated AIs, and does not target personal data nor trade secrets of Designated AIs. A Designated AI should apply enhanced security measures, appropriate to its circumstances and commensurate with the computer-system security risk of its CCSs.
- 1.1.8 The MA may, in consultation with the Commissioner and industry stakeholders, from time to time review and amend the requirements stipulated in this Code according to the latest technological development and industry best practices.

2. DEFINITIONS AND CONVENTIONS

2.1 Definitions

2.1.1 The terms defined in the Ordinance are applicable to this Code.

2.1.2 The terms used in Section 2 to 6 of this Code are defined as follows –

access control	means the control feature that ensures that access to assets is authorised and restricted based on business and security requirements;
accessible from Hong Kong	means a computer system which can be accessed from an entry point in Hong Kong regardless of the physical location of that system;
accessible in Hong Kong	means a computer system which is physically reachable within Hong Kong;
availability	means the property of being accessible and usable on demand by an authorised entity;
Code	means this Sectoral Code of Practice for the Protection of Critical Infrastructures (Computer Systems) Ordinance published by the MA;
Commissioner	means the Commissioner of Critical Infrastructure (Computer-system Security) appointed under section 3(1) of the Ordinance;
compromise	means the violation of the security of an information system;
computer-system security risk	means the risk that a vulnerability in a computer system may be exploited by a malicious actor thus resulting in a computer-system security incident. It refers to the likelihood of the risk event occurring and the resulting impact;
confidentiality	means the property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems;
C-RAF	means Cyber Resilience Assessment Framework;

encryption	<p>means a cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption”, which is a transformation that restores encrypted data to its original state.</p> <p>Practical examples:</p> <ul style="list-style-type: none"> • Data at-rest: applicable to data on disk rather than in-memory. May consider disk encryption, file or folder level encryption, data encryption, etc. • Data in-transit: applicable to end-to-end data transfer from one endpoint to another. May consider HTTPS (SSL, TLS), IPsec VPN, etc. • Data in-use: applicable to data stored in memory, CPU cache, or CPU register. May consider full memory encryption to limit clear text data to the CPU internal cache;
malware	<p>means software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to computer systems;</p>
patch management	<p>means systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hotfixes, and service packs;</p>
regulating authority	<p>means the Commissioner or a designated authority;</p>
remote connection	<p>means access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g. the Internet);</p>
removable storage media	<p>means portable electronic storage media such as magnetic, optical, or flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard disks or solid-state drives, floppy disks, zip drives, optical disks, tapes, memory cards, flash drives, and USB storage devices;</p>
sensitive digital data	<p>means any electronically stored, processed, or transmitted information which unauthorised access, disclosure, alteration, or loss could cause significant harm to individuals, organizations or society;</p>

SPM	means Supervisory Policy Manual;
supplier	means an individual or an organization that enters into an agreement with the acquirer for the supply of a product or service. A supplier can be a vendor, contractor, seller, producer (collectively known as “external service provider”), or a party that is in the same organization;
supply chain	means a linked set of resources and processes between multiple tiers of developers that begin with the sourcing of products and services and extend through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer;
vulnerability	means a weakness in the design, implementation, or operation of an asset or the internal controls of a process, which may expose the computer system to computer-system security risks.

3. DESIGNATION OF CRITICAL COMPUTER SYSTEMS

3.1 Designating critical computer systems

- 3.1.1 The MA will engage bilaterally with each Designated AI when determining which of its computer systems should be designated as a CCS under the Ordinance. As Designated AIs would be required to provide related information and assessments, this chapter aims to provide further information on the key factors that may be considered and discussed during the process. This chapter should be read in conjunction with section 13 of the Ordinance.
- 3.1.2 The MA will from time to time review the list of CCSs in consultation with Designated AIs.
- 3.1.3 A computer system will more likely be designated as a CCS if it meets any of the following criteria:
- (a) The system plays a material role in respect of the core function of the CI concerned. Whether a system is isolated from the Internet or whether the operation of the computer system, in full or in part, is being outsourced to a Group entity or affiliate or a third-party service provider is irrelevant.
 - (b) The disruption or destruction of the system would cause severe impact to the core function of the CI. Whether the core function of the CI could be switched to manual processing as a failover solution is irrelevant.
 - (c) The system stores or processes sensitive digital data that are used directly in the provision of essential services, e.g. a full set of personal data (such as name, identity document number, phone number and residential address) used in banking services. Whether there is a sophisticated mechanism for data protection or recovery is irrelevant.
 - (d) The system is highly related to other CI operator(s), which may or may not be a Designated AI. Regulating authorities will provide guidance as and when necessary. Examples of these computer systems include centralised processing or data exchange systems within the same sector or across multiple sectors.
 - (e) Systems directly strengthening the resilience of the CCSs described in paragraph 3.1.3(a)-(d) above (e.g. backup facilities in high-availability systems).
- 3.1.4 The underlying IT infrastructures of a Designated AI's CCSs, such as network components, operating platforms, middleware, may also be regarded as components of the CCS.

4. INFORMATION REQUIRED FOR DESIGNATION

4.1 Requiring information for designating critical computer systems

4.1.1 Examples of information required by the MA for ascertaining whether to designate a computer system as a CCS include, but are not limited to:

- (a) Facts and functions about the computer system, including upstream and downstream dependencies;
- (b) Architecture of the computer system;
- (c) Nature and volume of sensitive digital data processed by the computer system;
- (d) Network diagram of the computer system providing or supporting the core functions of the CI;
- (e) Manufacturers and models of computer hardware and software providing or supporting the core functions of the CI;
- (f) External information technology or telecommunication services subscribed for providing or supporting the core functions of the CI;
- (g) Resilience features, including the design and actual setup of the computer systems providing or supporting the core functions of the CI; and
- (h) Documentation illustrating the design and operations of the computer system, such as diagrams or system function descriptions.

5. OBLIGATIONS OF DESIGNATED AIS – DIVISION 1

5.1 Obligation to maintain office in Hong Kong

5.1.1 For the purpose of section 19 of the Ordinance, “office in Hong Kong” generally means any office maintained by the Designated AI in Hong Kong. This office may, but does not have to be, the “principal place of business in Hong Kong” as reported to the MA under section 20 of the Banking Ordinance (Cap.155) (BO). In any case, such office should serve not only as the location to which notices or other documents may be given or sent, but also as the location where a Designated AI conducts its business, operations or activities, such as managing daily operations, making business decisions, interacting with stakeholders, or maintaining business records.

5.1.2 Although there are similar (and not exactly the same) requirements for a Designated AI regarding the maintenance and notification of its certain address relating to a particular purpose under another ordinance, such as “the address of the principal place of business in Hong Kong” as referred to in section 20(1)(a) of the BO, a Designated AI is nonetheless obligated to notify the MA in writing of its “office address in Hong Kong” within the specified period as required under section 19(1) of the Ordinance for compliance purpose.

5.1.3 When there is a subsequent change to the “office in Hong Kong” that has been notified to the MA under section 19(1) of the Ordinance, a Designated AI is obligated to notify the MA in writing of the change to the “office address in Hong Kong” within the specified period as required under section 19(3) of the Ordinance. If and when such obligation under the Ordinance arises at the same time as another similar obligation under a different ordinance (e.g. for notifying the MA under section 20(4) of the BO of a change to “the address of the principal place of business in Hong Kong” which is the same address as the “office in Hong Kong” under the Ordinance), the Designated AI may:

- (a) notify the MA under separate notifications, each referring specifically to fulfilment of the obligation under section 19(3) of the Ordinance or section 20(4) of the BO, as the case may be; or
- (b) notify the MA under one composite notification, provided that the composite notification must set out clearly the fulfilment of the corresponding obligations under the specific sections in the respective ordinances, i.e. section 19(3) of the Ordinance or section 20(4) of the BO.

5.1.4 Where a composite notification is given, the Designated AI remains obligated to adhere to the respective time limits for which the notifications must be made under the respective ordinances.

5.2 Obligation to notify operator changes

5.2.1 While the question of whether an event may constitute an “operator change” (as defined in section 20(4) of the Ordinance) will be determined by the MA based on the facts and circumstances of each particular case, it is the MA’s present expectation that the below non-exhaustive scenarios would generally result in an operator change:

- (a) a Designated AI ceases to provide, partially or entirely, essential service(s) in the banking and financial services sector due to events, such as a sale or

disposal of its business, mergers, restructuring, resolution, or any other reason(s); or

(b) a Designated AI transfers its banking licence to another organization.

5.2.2 Notification by a Designated AI to the MA under section 20(1) of the Ordinance should be given in the form and way as specified by the MA under section 10 of the Ordinance.

5.2.3 A Designated AI is obligated to notify the MA of the operator change under section 20(1) of the Ordinance, regardless of whether the MA has already had knowledge of such operator change or whether the operator change is occasioned by the MA's decision. For instance, in the event of the MA revoking the Designated AI's banking authorization in accordance with section 22 of the BO, the obligation under section 20(1) of the Ordinance continues to apply, unless the designation of the Designated AI as a CI operator is revoked.

5.3 Obligation to set up and maintain computer-system security management unit

5.3.1 For the purpose of section 21(1) of the Ordinance, a computer-system security management unit need not be based in Hong Kong.

5.3.2 For the purpose of section 21(4) of the Ordinance, the employee supervising the computer-system security management unit need not be based in Hong Kong. Besides, having adequate professional knowledge in relation to computer-system security generally means possessing appropriate professional qualifications (e.g. Certified Information Security Professional (CISP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), etc.) and professional experience in computer-system security commensurate with the risk of their CCSs to discharge the duties effectively. Notification by a Designated AI to the MA of the appointment of the employee supervising the computer-system security management unit should be given in the form and way as specified by the MA under section 10 of the Ordinance.

5.3.3 For the purpose of section 21(6) of the Ordinance, while the date of the change pertains to the date of assumption of duty, a Designated AI is encouraged to proactively inform the MA as soon as the contract of employment is signed. Notification by a Designated AI to the MA of any change in respect of an appointment after it is made should be given in the form and way as specified by the MA under section 10 of the Ordinance.

6. OBLIGATIONS OF DESIGNATED AIS – DIVISION 2

6.1 Obligation to notify material changes to certain computer systems

- 6.1.1 For the purpose of section 22(1) and section 22(2) of the Ordinance, the date on which the event occurs generally refers to the moment when a change is deployed to production environments. If the deployment is conducted in phases, the date on which the event occurs should be applicable to each individual phase of the change deployment. A Designated AI may opt to notify the MA of all subsequent changes collectively at the initial phase of the change deployment.
- 6.1.2 For the purpose of section 22(3) of the Ordinance, a Designated AI should report any material change in a CCS that has high security risk implications to the CI's core function, as identified through a risk assessment process that adheres to relevant control principles outlined in the C-RAF maturity assessment matrix sections 2.2.2 and 3.5.3. Material changes in a CCS (non-exhaustive) may occur in the events below:
- (a) Platform migration;
 - (b) Server virtualisation;
 - (c) Major version upgrade of a core component (e.g. database);
 - (d) Changes to the computing platform or hardware;
 - (e) Application re-design;
 - (f) Significant code changes;
 - (g) Changes to the underlying infrastructure that supports the CCS;
 - (h) Integration with or change in interdependency on external systems or networks;
 - (i) Changes of mission or major functions that alters the system's operational scope, intended purpose or requirements in security, resources or functions; or
 - (j) Any system modification that fundamentally alters the characteristics or nature of the CCS.
- 6.1.3 For the purpose of section 22(1), notification by a Designated AI to the MA of material changes to certain computer systems should be given in the form and way as specified by the MA under section 10 of the Ordinance.

6.2 Obligation to submit and implement computer-system security management plan

- 6.2.1 A computer-system security management plan should cover all matters necessary to fulfil the statutory obligation to protect the computer-system security of the CCSs in accordance with Schedule 3 of the Ordinance. In relation to matters specified in Schedule 3 Part 1 of the Ordinance, a Designated AI should fulfil the requirements stipulated in sections 6.2.5 – 6.2.27, 6.3 and 6.4 of this Code, which provide relevant practical guidance. In relation to matters specified in Schedule 3 Part 2 of the Ordinance, a Designated AI should refer to guidance published by the Commissioner.

- 6.2.2 A Designated AI should ensure that the computer-system security management plan and any subsequent changes (other than contact point or editorial updates such as reformatting or typographical corrections) submitted to the MA are endorsed by the Board of Directors (the Board), or a functional sub-committee delegated by the Board, or the senior management overseeing the operation of the concerned CI (e.g. Chief Executive Officer, Chief Operating Officer, or their equivalent). The plan should be reviewed as circumstances require, and, in any case, at least once every two years, to ensure its effectiveness and validity.
- 6.2.3 In the event that the computer-system security management plan consists of a collection of policies, standards and guidelines, a Designated AI should provide a clear cross-reference that maps each applicable requirement between relevant sections of the plan and sections 6.2.5 – 6.2.27, 6.3 and 6.4 of this Code.
- 6.2.4 If a Designated AI cannot fulfil any of the requirements stipulated in sections 6.2.5 – 6.2.27, 6.3 and 6.4 of this Code, the Designated AI should implement alternative security controls that achieve comparable results. The alternative controls should be documented in the computer-system security management plan, with a detailed description showing how they effectively mitigate the relevant risks.
- 6.2.5 Computer-System Security Management Unit
- (a) When setting up the computer-system security management unit for the purposes described in section 21(1) of the Ordinance, a Designated AI should adhere to relevant control principles outlined in the C-RAF maturity assessment matrix section 1.3.1.
- 6.2.6 Policies, Standards and Guidelines
- (a) A Designated AI should define and enforce computer-system security policies, standards and guidelines that provide management direction and support for protecting CCSs in accordance with business needs and security requirements, and enable the Designated AI to satisfy requirements and/or guidance stipulated in sections 6.2.5 – 6.2.27, 6.3 and 6.4 of this Code.
- (b) When drafting its policies, standards and guidelines, a Designated AI should consider its own requirements on security, this Code, the relevant supervisory requirements and applicable national and international computer-system security standards.
- (c) A Designated AI should establish a mechanism to ensure the policies, standards and guidelines are effectively communicated to and easily accessible by all personnel involved in the operation of CCSs.
- 6.2.7 Computer-System Security Risk Management Approach
- (a) A Designated AI should formulate and implement an approach to identify, assess, mitigate and monitor computer-system security risks of CCSs, adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 1.3.2 and subdomain 2.2.

- (b) In addition, when formulating the computer-system security risk management approach, a Designated AI should also refer to nationally or internationally recognised methodologies and standards for computer-system security risk management.

6.2.8 Security by Design

- (a) A Designated AI should implement a secure development process to ensure the security of the CCS throughout the system development life cycle, adhering to relevant control principles outlined in the C-RAF maturity assessment matrix subdomain 3.4.

6.2.9 Asset Management

- (a) A Designated AI should define and document the identification approach, selection criteria, and the regular review mechanism for CCSs based on guidance provided by the MA for the designation of CCSs.
- (b) A Designated AI should maintain up-to-date inventories and conduct regular reviews of the inventories, adhering to relevant control principles outlined in the C-RAF maturity assessment matrix subdomain 2.1.
- (c) A Designated AI should ensure that access to the inventories is restricted and on a need-to-know basis. Where applicable, the following information should be included in the inventories:
 - (i) descriptions, major functions, physical / logical locations, and owners or key personnel of CCSs; and
 - (ii) the associated assets, including hardware assets (name, manufacturer, model, firmware version, etc.), software assets (name, publisher, version, etc.), applications, valid warranties, service agreements and legal / contractual documents.

6.2.10 Access Control and Account Management

- (a) A Designated AI should ensure proper access and account management of CCSs by implementing measures adhering to:
 - (i) relevant control principles outlined in the C-RAF maturity assessment matrix subdomain 3.1.1; and
 - (ii) relevant requirements outlined in SPM TM-G-1 sections 3.2.1, 3.2.2 and 3.3.1.
- (b) Furthermore, a Designated AI should:
 - (i) define and document procedures for password delivery and password reset;
 - (ii) review user privileges and data access rights at least once per year, with records for access rights approval and review maintained; and

- (iii) arrange for a notification message (in the form of a system notification or physical notice) that provides appropriate security notices (e.g. system usage may be recorded and monitored, unauthorised use is prohibited) to be displayed to the users of CCSs before they are authenticated to use the CCSs.

6.2.11 Privileged Access Management

- (a) A Designated AI should manage privileged access by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.1.2, and relevant requirements outlined in SPM TM-G-1 section 3.2.3.
- (b) A Designated AI should prevent unauthorised devices from connecting to the internal network by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.2.1, and allow only authorised devices equipped with security controls to access privileged accounts by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix sections 3.3.1 and 4.1.1.

6.2.12 Cryptography

- (a) A Designated AI should ensure proper and effective use of cryptography for the protection of data-at-rest, data-in-transit and data-in-use by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix sections 3.1.1, 3.1.5, 3.1.6, 3.2.1, 3.3.1, 3.3.2 and 7.1.1.
- (b) A Designated AI should manage cryptographic keys by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.1.8 and relevant requirements outlined in SPM TM-G-1 section 3.1.4, and referencing to the latest international standards.
- (c) Commensurate with the risk, keys used to process sensitive digital data should be stored and distributed separately from the corresponding encrypted information.
- (d) A Designated AI should refer to the latest national or international computer-system security standards regarding the use of cryptographic algorithms and methods.

6.2.13 Password Management

- (a) A Designated AI should manage passwords by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.1.1 and relevant requirements outlined in SPM TM-G-1 section 3.2.2.
- (b) Furthermore, a Designated AI should ensure that all passwords are promptly changed if they have been or are suspected of being compromised. In addition, where a password is the single authentication factor used by suppliers for maintenance and support, the password should be changed after every use.

6.2.14 Physical Security

- (a) A Designated AI should implement physical access management by adhering to:
 - (i) relevant control principles outlined in the C-RAF maturity assessment matrix sections 3.1.1, 3.1.4 and 4.3.1; and
 - (ii) relevant requirements outlined in SPM TM-G-1 sections 3.6.1 and 3.6.3.
- (b) Furthermore, a Designated AI should:
 - (i) protect the deployed surveillance systems from unauthorised access or interruption;
 - (ii) protect the power and communication cables of CCSs against damage and interception; and
 - (iii) label the power and communication cables of CCSs to facilitate physical identification and inspection.

6.2.15 Configuration Management and System Hardening

- (a) A Designated AI should implement configuration management and system hardening controls by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.2.2 and relevant requirements outlined in SPM TM-G-1 section 3.4.1.
- (b) Both the least functionality principle and the least privilege principle should be adopted when performing system hardening.

6.2.16 Change Management

- (a) A Designated AI should implement change management controls by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.5.3, and relevant requirements outlined in SPM TM-G-1 sections 4.2.4 and 4.3.

6.2.17 Patch Management

- (a) A Designated AI should implement patch management controls by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix sections 3.5.1 and 3.5.2, and apply appropriate change management controls with reference to section 6.2.16 Change Management of this Code when deploying the patches.
- (b) A Designated AI should adopt a risk-based approach to determine an appropriate patch management strategy for CCSs, adhering to relevant control principles outlined in the C-RAF maturity assessment matrix subdomain 2.1 and section 2.2.3.

6.2.18 Remote Connection

- (a) When implementing security measures for remotely accessing the CCS from outside a Designated AI's premises, a Designated AI should adhere to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.1.5 and relevant requirements outlined in SPM TM-G-1 sections 3.5.2.
- (b) Where a Designated AI permits the use of privately-owned equipment for remote access, it should, in addition to section 6.2.18(a) specified above, establish relevant policies and procedures, require user acknowledgement of security responsibilities before use, support the separation and protection of sensitive digital data on the equipment, and consider enabling location tracking of equipment and remote data wiping.

6.2.19 Storage Media

- (a) For any storage media of CCS that store sensitive digital data, a Designated AI should:
 - (i) ensure proper authorisation for the disclosure, modification, removal and destruction of sensitive digital data;
 - (ii) apply relevant encryption controls described in section 6.2.12 Cryptography of this Code; and
 - (iii) completely erase and destroy the sensitive digital data from storage media before disposal or re-use. A suitable deletion method, such as degaussing, electronic overwriting or cryptographic erasure, should be employed to avoid data leakage.
- (b) In addition, where a portable computing device or removable storage media is used, a Designated AI should:
 - (i) protect sensitive digital data stored on portable computing devices and removable storage media by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix sections 3.2.2, 3.3.1 and 3.3.2;
 - (ii) perform malware scans on portable computing devices and removable storage media to prevent a CCS from malware infection; and
 - (iii) protect the portable computing devices and removable storage media that store or process sensitive digital data directly involved in the provision of essential services from unauthorised access or misuse.

6.2.20 Backup and Recovery

- (a) A Designated AI should implement backup and recovery measures for its CCSs and associated data by adhering to:
 - (i) relevant control principles outlined in the C-RAF maturity assessment matrix sections 5.1.2 and 5.2.3;
 - (ii) relevant requirements outlined in SPM TM-G-1 section 5.1.2; and

- (iii) relevant requirements outlined in SPM TM-G-2 sections 4.6.2 and 5.2.1.
- (b) Furthermore, a Designated AI should:
- (i) implement a secure tertiary data backup (STDB) taking into account the principles stipulated in the Hong Kong Association of Banks's STDB Guideline. For any CCS component where a Designated AI determines, with justification, that onboarding to the STDB is technically infeasible, the Designated AI must establish a backup copy that is physically disconnected from the CCS;
 - (ii) ensure off-site data backups are stored at a secure and remote location and at a distance sufficient to escape from disasters at the main site; and
 - (iii) restrict access to the backup media to authorised personnel in accordance with the established mechanism. Unauthorised access to the media library or off-site storage room should not be permitted.

6.2.21 Network Security

- (a) A Designated AI should implement network security controls by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.2.1.
- (b) Access to CCSs via wireless communications should be carefully planned to mitigate security risks. Where the use is justified by operational necessity, a Designated AI should assess the relevant security risks and implement compensatory security measures by adhering to relevant control principles outlined in C-RAF maturity assessment matrix sections 3.1.6 and 3.2.1, and implement logging practices with reference to section 6.2.23 Log Management of this Code.

6.2.22 Application Security

- (a) When developing or making changes to any application in relation to CCSs, a Designated AI should implement a secure development process described in section 6.2.8 Security by Design of this Code and apply change management controls described in section 6.2.16 Change Management of this Code. In addition, a Designated AI should ensure only authorised software are installed by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 2.1.
- (b) A Designated AI should protect the source code that it owns, maintains or customises from unauthorised access by implementing proper access control and account management.
- (c) Data used for testing should be carefully selected, protected and controlled. In particular, a Designated AI should adhere to relevant control principles outlined in the C-RAF maturity assessment matrix section 3.3.2 and relevant requirements outlined in SPM TM-G-1 section 4.2.4.

6.2.23 Log Management

- (a) A Designated AI should properly retain and manage system logs that support detection and response to computer-system security incidents concerning CCSs with reference to section 6.2.26 Monitoring and Detection of this Code, and adhere to relevant control principles outlined in the C-RAF maturity assessment matrix sections 5.3.1.
- (b) Furthermore, a Designated AI should define policies for logging activities and retaining logs of CCSs to facilitate computer-system security incident investigations. The policies should include but not be limited to the requirement to log:
 - (i) Log-on attempts;
 - (ii) Password change attempts;
 - (iii) Access attempts to critical files (e.g. software configuration files, password and key files, etc.);
 - (iv) Use of privileged rights, such as addition and deletion of user accounts;
 - (v) Changes to user access rights;
 - (vi) Modifications to audit policies; and
 - (vii) Activation and de-activation of protection systems, such as anti-malware systems and intrusion detection systems.
- (c) The logs should be retained for a minimum period of 6 months. Such logs should be secured so that they cannot be deleted or altered, and can be read only by authorised persons.
- (d) Retained logs should contain sufficient information to support after-the-fact investigation of computer-system security incident(s), including the effectiveness of security measures.

6.2.24 Cloud Computing Security

- (a) There has been a growing trend of AIs adopting cloud computing via the engagement of third-party Cloud Service Providers (CSPs), and the scope of function and cloud deployment models varies across different AIs. In light of this, a Designated AI should take note of relevant guidance, such as the Practice Guide on Cloud Adoption dated 8 January 2026, issued by the HKMA from time to time, as well as internationally recognised standards and best practices, and implement controls for CCSs commensurate to the nature and criticality of its cloud adoption.
- (b) In addition, a Designated AI should take into account security requirements and guidance stipulated in section 6.2.25 Supply Chain Management of this Code when managing risks associated with cloud adoption.

6.2.25 Supply Chain Management

- (a) A Designated AI should manage supply chain risks of CCS arising from the engagement with suppliers by adhering to:
 - (i) guidance provided under sound practices 1, 2 and 3 of the Circular on Managing Cyber Risk Associated with Third-party Service Providers and its Annex, dated 21 December 2023; and
 - (ii) relevant control principles outlined in the C-RAF maturity assessment matrix section 2.1 and domain 7.
- (b) A Designated AI should implement appropriate measures, commensurate with the identified supply chain risk and geopolitical risk, to avoid over-dependence on a single or a few suppliers and better enable management of risks arising from drastic events such as an unplanned vendor exit or product / service unavailability.

6.2.26 Monitoring and Detection

- (a) A Designated AI should implement measures to detect computer-system security incidents affecting CCSs by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix sections 4.2.1, 4.2.2, 4.3.1 and 4.3.2.
- (b) A Designated AI should monitor and analyse threat intelligence in relation to CCSs, and take appropriate actions, adhering to relevant control principles outlined in the C-RAF maturity assessment matrix subdomains 4.4 and 6.1.
- (c) A Designated AI should implement procedures to authorise, control and monitor the use of mobile codes (e.g. JavaScript, VBScript, ActiveX controls, Microsoft Office macros) and scripts within the CCS.

6.2.27 Computer-System Security Training

- (a) A Designated AI should formulate and implement a training programme by adhering to relevant control principles outlined in the C-RAF maturity assessment matrix section 1.5.2, and regularly evaluate the effectiveness of training activities via user feedback and post-training assessments.
- (b) A Designated AI may require an external service provider involved in CCS operation through contractual agreements to provide training to its personnel.

6.3 Obligation to conduct computer-system security risk assessments

- 6.3.1 For the purpose of section 24(1) of the Ordinance, a Designated AI should refer to nationally or internationally recognised methodologies and standards for computer-system security risk assessment.
- 6.3.2 The computer-system security risk assessment should include, but not be limited to, all applications, hosts, and network devices of the CCSs.
- 6.3.3 After conducting the computer-system security risk assessment, a Designated AI should document the identified risks to the CCSs, including the likelihood and severity, the level of risks that the CCSs can tolerate, and the required risk mitigation measures and monitoring.
- 6.3.4 The computer-system security risk assessment should include a vulnerability assessment and a penetration test which, among other steps, identify security and control weaknesses.
- 6.3.5 The vulnerability assessment in the computer-system security risk assessment should involve various vulnerability identification activities, including but not limited to vulnerability scanning, source code reviews (for internally developed and vendor-provided custom applications), and configuration reviews, to identify potential security loopholes and vulnerabilities. The vulnerability assessment should be conducted under the supervision of a qualified security professional having suitable knowledge, relevant experience and appropriate professional qualifications.
- 6.3.6 The penetration test in the computer-system security risk assessment should be carried out from the position of a potential attacker or based on threat intelligence, and can involve active exploitation of possible vulnerabilities of the CCSs. The test should include, but not be limited to, the areas of network security, system software security, client-side application security and server-side application security. The penetration test should be conducted by a tester having suitable knowledge, relevant experience and appropriate professional qualifications.
- 6.3.7 The computer-system security risk assessment report, covering both vulnerability assessment and penetration test, should include at least the following information:
- (a) Assessment scope, objectives, methodology, time of assessment, and assumptions for what is and is not covered;
 - (b) Detailed findings of identified vulnerabilities, including potential impacts, exploitability and priority of each vulnerability, as well as any weakness relating to security control; and
 - (c) Treatment plan for each finding, with timeline and responsible party for executing and monitoring the implementation of the plan.
- 6.3.8 When preparing the computer-system security risk assessment report, a Designated AI may leverage the results of similar assessment(s) conducted with a different scope or performed at different times, provided that:
- (a) the leveraged assessment(s), collectively, covers all CCSs;

- (b) the leveraged assessment(s) can achieve the objectives stated in Schedule 4 of the Ordinance;
 - (c) the leveraged assessment(s) fulfil the requirements and guidance stipulated under sections 6.3.1 to 6.3.7 of this Code; and
 - (d) the assessment frequency aligns with the specified period stated in section 24(1) of the Ordinance.
- 6.3.9 A Designated AI leveraging the result(s) of similar assessment(s) per section 6.3.8 of this Code should supplement an analysis justifying the applicability of the leveraged assessment(s) in relation to section 6.3.8(a) to (d).
- 6.4 Obligation to arrange to carry out computer-system security audits**
- 6.4.1 A computer-system security audit should assess whether a Designated AI's computer-system security management plan is implemented and whether the security controls and measures comply with the computer-system security management plan.
- 6.4.2 A Designated AI should appoint an assessor to conduct the computer-system security audit for their CCSs and adhere to relevant principles outlined in C-RAF Chapter 1 section 1.2.4.
- 6.4.3 Nationally or internationally recognised methodologies and standards, or computer-system security best practices should be referenced when conducting a computer-system security audit.
- 6.4.4 The assessor should include at least the following in its conclusion of the audit report:
- (a) whether and to what extent the computer-system security management plan is implemented;
 - (b) whether and to what extent the security controls implemented adhere to the requirements / guidance stipulated in this Code, including the reasonableness and efficacy of any alternative controls employed; and
 - (c) with respect to items (a) and (b) and findings identified, the overall condition of the computer-system security for the CCSs.
- 6.4.5 When preparing the computer-system security audit report, a Designated AI may leverage similar assessment(s) conducted with a different scope, provided that:
- (a) the leveraged assessment(s), collectively, cover all CCSs;
 - (b) the leveraged assessment(s) fulfil the requirements stipulated under sections 6.4.1 to 6.4.4 of this Code; and
 - (c) the assessment frequency and period align with the frequency and specified period stated in sections 25(1) and 25(13), respectively, of the Ordinance.

*** ENDS ***