HONG KONG MONETARY AUTHORITY
香港金融管理局

CYBER RESILIENCE ASSESSMENT FRAMEWORK

December 2016

Contents

Chapter 1. Overview

1.1. Introduction

1.1.1. To further strengthen the cyber resilience of authorised institutions (AIs) in Hong Kong, the Hong Kong Monetary Authority (HKMA) has developed a Cyber Fortification Initiative (CFI), which comprises three components: (i) a Cyber Resilience Assessment Framework (C-RAF); (ii) a Cyber Intelligence Sharing Platform; and (iii) a Professional Development Programme (PDP). This document aims to explain the implementation of the C-RAF.

1.1.2. The C-RAF is a structured assessment framework for AIs to assess their inherent risks and the maturity levels of their cybersecurity measures against a set of principles set out in the C-RAF, called "control principles". Through this process, AIs will be able to better understand, assess, strengthen and continuously improve their cyber resilience.

1.1.3. The C-RAF comprises the following elements:

i. **Inherent risk assessment**;
ii. **Maturity assessment**; and
iii. **intelligence-led cyber attack simulation testing (iCAST).**

1.1.4. The overall workflow of the assessment process is set out below. First, AIs are required to assess and ascertain their inherent risk (i.e. the "inherent risk assessment" process) which will result in an inherent risk rating. The inherent risk rating is mapped to its respective maturity level of cyber resilience as expected by the HKMA. Then they assess and determine their actual maturity level of cyber resilience (i.e. the "maturity assessment" process). Any gaps between the expected level and the actual level of maturity of cyber resilience will then be identified for improvement, so that the AIs' cyber resilience will be brought to the appropriate level as expected by the HKMA.

1.1.5. The high-level process flow is shown in Figure 1. Details on the inherent risk assessment and maturity assessment are set out in Chapter 2 and Chapter 3 of this document respectively.

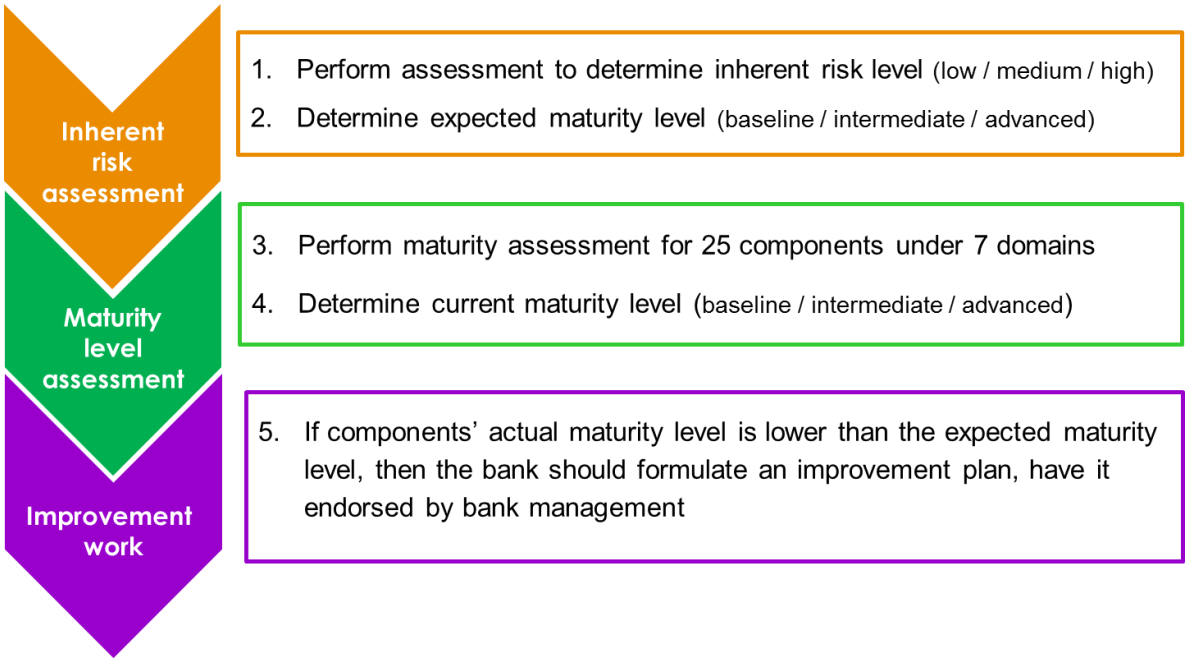

Figure 1: process flow of the C-RAF

1.1.6. The development of the C-RAF has also taken into account similar assessment frameworks of other regulatory authorities and certain international standards[1]

1.1.7. This document sets out the details of, and the process for conducting, the C-RAF. Please read this document carefully before completing the C-RAF data entry programme. The entry programme, prepared by the HKMA in Excel format, will be provided to your institution separately.

[1] Reference has been made, but not limited, to international guidelines or cybersecurity frameworks listed below:

- Guidance on cyber resilience for financial market infrastructures, Issued by Committee on Payments and Market Infrastructures and Board of the International Organisation of Securities Commissions;
- Federal Financial Institutions Examination Council Cybersecurity Assessment Tool;
- Framework for Improving Critical Infrastructure Cybersecurity, issued by United State National Institute of Standard and Technology; and
- CBEST by Bank of England.

1.2. Important principles for conducting the assessment

1.2.1. **Scope** -- The scope of the assessment set out in C-RAF covers those systems and infrastructure supporting the AIs' Hong Kong business and operation.

1.2.2. **Qualified personnel -** The assessment set out in C-RAF should be conducted by assessor(s) who are qualified and competent. In this connection, AIs are expected to commission an external consultant or colleague(s) representing an internal function (e.g., their internal audit or technology risk management function or other equivalent unit) with adequate expertise and technical knowledge as well as the required qualification to complete the C-RAF. For qualification requirements, please refer to Chapter 5 of this document.

1.2.3. **Documentary evidence** - AIs should retain the C-RAF assessment and results as well as the documentary evidence that show how the control principles set out in the C-RAF have been met. This includes, but not limited to, relevant policies and procedures as well as the final assessment report, working papers and documentation for the assessment.

1.2.4. The HKMA may validate the assessment results and processes, on a sample basis, through its on-going supervisory activities, having regard to the above-mentioned evidence and other factors. If the process is considered as inadequate, or the result is considered as non-factual, the HKMA will take this into account in its overall supervisory assessment in relation to the AIs concerned.

1.2.5. **Authority to sign off assessment** - The results of the assessment (the completed data entry programme and assessment templates) should be reviewed and signed off[2] by the Chief Executive or the

[2] Please use the print-out of the sign-off form on the first page of the assessment template to

Alternate Chief Executive of AI concerned, as well as the assessor responsible for conducting the assessment, using the sign-off form in the data entry programme of each assessment area. Assessment results and the sign-off form(s) should be kept together with the data entry programme.

1.2.6. AIs are required to draw up an improvement plan and a timetable to close any gap(s) identified in cyber resilience. The plan should be endorsed by the management together with the assessment results (data entry programme, completed and signed risk assessment and maturity assessment).

complete the sign-off.

Chapter 2. Inherent risk assessment

2.1. Inherent risk profile

2.1.1. Generally speaking, "inherent risk" reflects the amount of the threats of cyber attacks an AI may face, due to the types, volumes, values and complexities of their business operations in the cyber space. An inherent risk profile is designed to help the AI determine its cyber risk exposure.

2.2. Definitions of different inherent risk levels

2.2.1. The definition of individual inherent risk levels is set out below.

- **Low inherent risk level** – An AI with a "low" inherent risk level generally has adopted very limited emerging technologies. It has very few internet and mobile channels for delivering products and services and a relatively closed operating environment with very limited external connections. The variety of products and services are limited. The AI has a small geographic footprint and few technology employees.
- **Medium inherent risk** – An AI with a "medium" inherent risk level generally adopts new technologies that are somewhat sophisticated. The AI may outsource mission-critical systems and applications and may support elements internally. There is a greater variety of products and services offered through a diverse range of channels, including both the internet and mobile channels.
- **High inherent risk** – An AI with a "high" inherent risk level uses highly complex technologies to deliver a myriad of products and services. New and emerging technologies are utilised across multiple delivery channels, including the internet and mobile channels and direct connections with other organisations. A majority of mission-critical systems or applications are hosted internally. The AI maintains a large number of connections using different

network/communication protocols to transfer data with customers and third parties.

2.3. Key categories of business activities and operational aspects to be assessed

2.3.1. A typical inherent risk profile comprises the following categories taking into account various business and operational aspects of the AI:

- **Technologies** – Different types of connections and technologies may pose different levels of inherent risk to AIs, depending on the complexity and maturity, and nature of the specific technology products or services. When determining the inherent risk under this category, consideration should also be given to the overall set-up of the information technology (IT) infrastructure, such as the number of internet service providers (ISPs) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, the volume of network devices, the number of end-of-life systems, the extent of cloud services, the use of non-corporate devices, etc.
- **Delivery channels** – Different delivery channels for products and services may pose various levels of inherent risk to AIs. The inherent risk of an AI normally increases as the variety and number of delivery channels increases. Higher inherent risk under this category is expected if, for example, products and services are heavily delivered through online and mobile delivery channels and/or automated teller machine (ATM) operations are connected to the Internet.
- **Products and technology services** – Different products and technology services offered by AIs may pose different levels of inherent risk depending on the nature of the specific product or service offered. This category covers various payment services, especially those services that can transfer money direct to overseas counterparties directly, and also

includes consideration of whether the AI provides technology services to other organisations.

- **Business size and organisational characteristics** – This category considers business size and organisational characteristics such as total number of branches in Hong Kong, total asset valuation, the number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in the IT control environment, the locations of business presence, and the locations of operations and data centres.
- **Tracked records on cyber threats** – The volume and type of attacks (attempted or successful) affect the inherent risk exposure of an AI. This category takes into account the volume and sophistication of any reported attacks targeting the AI.

2.4. Determining inherent risk: The "matrix" as the assessment tool

2.4.1. AIs should assess and select the most appropriate inherent risk level for each assessment criterion in Appendix A. The inherent risk levels range from "low" to "high". The risk levels provide parameters for determining the inherent risk for each assessment criterion. Figure 2 shows an illustrative example on how the risk assessment matrix looks like.

Indicator	Assessment criteria	Inherent Risk Level				Supplementary information
		Low	Medium	High	Conclusion	
Wireless network access	Separate access points for guest wireless and corporate wireless	Physically separated	Logically separated	No separation	[Low/ Medium/ High/ Not applicable]	

Figure 2: inherent risk matrix layout

2.4.2. After rating an assessment criterion for "low", "medium" and "high", assessor should also fill in the exact "sizing", exact "volume", exact "amount" or judgement for selecting the rating (if applicable) for

the criterion in the field "supplementary information" in the inherent risk matrix as shown in Figure 2 above.

2.5. Determining inherent risk: Instructions for assessment

2.5.1. **Step 1: Determine the inherent risk level of individual assessment items** – Read through each of the indicator in Appendix A (a sample can be found in Figure 2). In each indicator, there may be one or more assessment criterion/criteria. For each assessment criterion, select the most appropriate description under "low", "medium" or "high" inherent risk and mark the selection in the conclusion box of each assessment criterion.

2.5.2. **Step 2: Determine the overall inherent risk level** – Count the total number of assessment criteria rated "low", "medium" and "high" respectively, and fill in the table shown in Figure 3 below. As a general rule, the inherent risk level with the most assessment criteria rated will be regarded as the overall inherent risk level of the AI. Nevertheless, the AI may take into account other relevant factors (such as the nature and complexity of its products and services, its size, its business model and its customer base) in determining its overall inherent risk level.

Inherent risk level	**Number of assessment criteria rated with inherent risk level "low", "medium" or "high"**
High	
Medium	
Low	
Overall inherent risk level determined by the AI	**Low / Medium / High**
The AI's rationales in determining its overall inherent risk level	

Figure 3: Overall inherent risk level of Bank A

2.6. Overall inherent risk level vs minimum required maturity level

2.6.1. The overall inherent risk level of an AI identified in this assessment will be mapped to the **minimum required maturity level**, as shown in the table below (see Figure 4). AIs are required to attain the **minimum required maturity level**.

Overall Inherent risk level	Minimum required maturity level
High	Advanced
Medium	Intermediate
Low	Baseline

Figure 4: minimum required maturity level

2.6.2. In order to assess whether the actual maturity level of cyber resilience of an AI has reached the **minimum required maturity level**, the second key element of the C-RAF is a "maturity assessment" process, which is detailed in Chapter 3.

Chapter 3. Maturity assessment

3.1. The general framework: seven key domains

3.1.1. The assessment scope of the maturity level of cyber resilience of an AI covers seven key aspects (or "domains"), as shown in Figure 5 below:

Figure 5: 7 domains of the maturity assessment

3.1.2. These seven domains are categorised in three levels: (1) the governance (the centre); (2) the internal environment (represented in the inner circle); and (3) the external environment (represented in the outer circle). The maturity assessment aims to cover a comprehensive review of the entire operating environment and places a great emphasis on having a sound governance framework.

3.1.3. Each domain comprises a number of "components". Figure 6 shows the relationship between the "domains" and the "components".

	Domain	Component
Governance	Governance	Cyber resilience oversight
		Strategy and policies
		Cyber risk management
		Audit
		Staffing and training
Internal environment	Identification	IT asset identification
		Cyber risk identification and assessment
	Protection	Infrastructure protection controls
		Access control
		Data security
		Secure coding
		Patch management
		Remediation management
	Detection	Vulnerability detection
		Anomalies activity detection
		Cyber incident detection
		Threat monitoring and analysis
	Response and recovery	Response planning
		Incident management
		Escalation and reporting
External environment	Situational awareness	Threat intelligence
		Threat intelligence sharing
	Third party risk management	External connections
		Third party management
		Ongoing monitoring on third party risk

Figure 6: domain and component of maturity assessment

3.2. Determining the maturity level of each component: the maturity "matrix" as the assessment

3.2.1. The objectives of the maturity assessment are to determine the level of maturity attained for each component, and to identify gaps and areas of improvement – down to the component level. The identified areas of improvement at the component level can be treated as a "road map" for an AI to improve its cyber resilience to an appropriate level.

3.2.2. To facilitate a consistent assessment of among AIs, we have designed a maturity assessment matrix in Appendix B. It sets out the required level/extent of implementation of each "control principle" for attaining a particular maturity level of that component. Given the evolving nature of cyber threat, these control principles and the way they are mapped to the different maturity levels will be reviewed periodically.

3.2.3. To accommodate the needs of different AIs, we have adopted a risk based approach on maturity requirement. As mentioned in section 2.6, each AI should attain a minimum required maturity level according to its inherent risk level.

3.2.4. Figure 7 below shows a section of a sample maturity matrix for illustration purpose. The full version can be found in Appendix B. For each component, we have set out a number of "control principles", which are divided into different maturity levels.

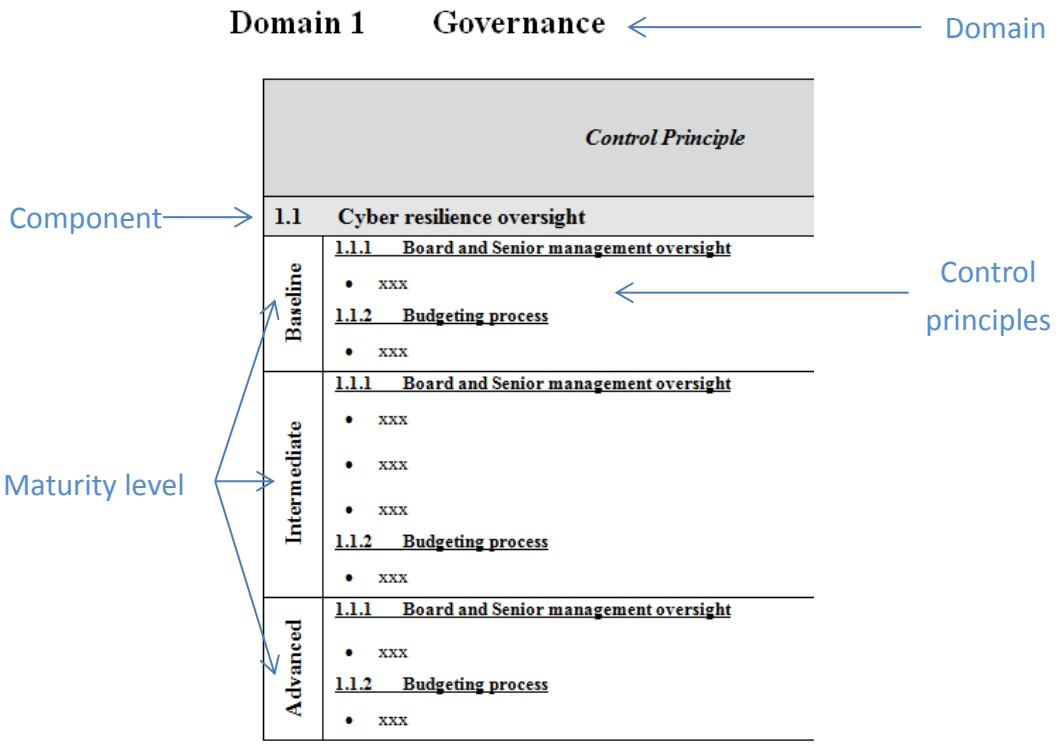

Figure 7: sample maturity matrix

3.3. Determining the maturity level of each component: Instructions for assessment

3.3.1. **Step 1: Perform assessment for applicable control principle – An** AI should assess applicable control principles according to the minimum required maturity level. For example, if an AI is subject to the "baseline" minimum required maturity level, it should assess all control principles at the "baseline" level.

3.3.2. If an AI is subject to the "intermediate" minimum required maturity level, it should assess all control principles at both the "baseline" and the "intermediate" levels.

3.3.3. if an AI is subject to the "advanced" minimum required maturity level, it should assess all control principles at all levels, i.e. "baseline", "intermediate" and "advanced" levels.

3.3.4. **Step 2: Enter assessment result into data entry programme** – Once the maturity assessment is completed, the assessment result of each control principle is needed to be input into the data entry programme.

3.3.5. The assessment result of each control principle is input as shown in Figure 8 below.

Option	Explanation	Description
[Y]	Yes	The control principle is effectively accomplished
[AC]	Alternative Controls	The control principle is considered to be accomplished through the implementation of alternative controls which are also considered to be effective, although the way of accomplishment is not as described in the matrix. Under such circumstances, the assessor should provide details of the alternative controls in the "justification" column.
[RA]	Risk Accepted	The control principle is considered to be accomplished through a risk mitigating measure and the residual risk associated with the control principle is formally accepted by the AIs, based on their risk appetite and risk treatment plan. Under such circumstances, the assessor should provide details of the risk mitigating measure and the residual risk acceptance in the "justification" column.
[N]	No	The control principle is not effectively accomplished.
[NA]	Not Applicable	The control principle is not applicable to the AI, and therefore the control principle is excluded from the determination of the component maturity. Under such circumstance, the assessor should provide the rationale of the control principle exclusion in the "justification" column.

Figure 8: requirements for attaining a particular maturity level for a component

3.3.6. **Step 3: Calculate the percentage of attainment** – For each component, the percentage of attainment of its maturity level should be worked out. The percentage of attainment is the sum of (i) the number of control principle which is accomplished (marked as "Y"), plus (ii) the number of alternative control implemented (marked as "AC"), plus (iii) the number of "risk accepted" (marked as "RA"), and plus (iv) the number of items which are not applicable to the AI (marked as "NA"), divided by total number of control principles in that maturity level, and the result is presented in a percentage term. Figure 9 below is an example illustrated the calculation logic.

Number of control principles						Percentage of attainment
Total	[Y]	[AC]	[RA]	[N]	[NA]	
8	4	1	1	1	1	7/8x100% = 87.5%
10	5	3	1		1	10/10 x 100% = 100%

Figure 9: Examples that illustrate how the percentage of attainment is calculated.

3.3.7. **Step 4: Determine areas of improvement** – For each component, the level of maturity attained is determined based on extent to which applicable control principles at different levels have been accomplished for that component. The required percentage of accomplished control principles (condition) are set out in Figure 10 below.

To attain the following maturity level for a particular component	An AI need to achieve the following conditions for that component		
	Implementation of control principles at the baseline level (%)	Implementation of control principles at the intermediate level (%)	Implementation of control principles at the advanced level (%)
Baseline	100%	n/a	n/a
Medium	100%	100%	n/a
Advanced	100%	100%	100%

Figure 10: requirements for attaining a particular maturity level for a component

3.4. Examples of determining the maturity level

3.4.1. Examples: To illustrate the process of determining the maturity level of AIs, several examples with minimum required maturity level at "advanced" (A), "intermediate" (I) and "baseline" (B), are shown in Figure 11, 12 and 13 respectively.

3.4.2. For Bank A, it is expected to reach the "advanced maturity level". In this case, any of the components which do not reach the advanced maturity level are gaps and, therefore, represent areas of improvement. For example, in the following situation, component (ii) (i.e. "Strategy and policies") would need to be improved, i.e. the various control principles set out in that component should be enhanced so that its maturity level reaches the "advanced" level 3.3.7.

Domain	Component	Maturity level attainment			
		B	I	A	Overall attainment
Governance	(i) Cyber resilience oversight	100%	100%	100%	Advanced
	(ii) Strategy and policies	100%	100%	20%	Intermediate

Figure 11: example maturity level attained for Bank A

3.4.3. For Bank B, it is subject to an "intermediate" minimum required maturity level, then any of the components which do not reach maturity level "intermediate" are areas for improvement. In the following case, only component (ii) (i.e. "Access control") needs to be improved.

Domain	Component	Maturity level attainment			
		B	I	A	Overall attainment
Protection	(i) Infrastructure protection controls	100%	100%	n/a	Intermediate

	(ii) Access control	100%	20%	n/a	Baseline

Figure 12: example maturity level attained for Bank B

3.4.4. For Bank C, it is subject to a "baseline" minimum required maturity level. In this case, any of the components cannot reach maturity level "baseline" are areas for improvement. For example, in the following case, the component (ii) ("Threat intelligence sharing") would have to be improved from "below baseline" to "baseline".

Domain	Component	Maturity level attainment			
		B	I	A	Overall attainment
Situational awareness	(i) Threat intelligence	100%	n/a	n/a	Baseline
	(ii) Threat intelligence sharing	50%	n/a	n/a	Below baseline

Figure 13: example maturity level attained for Bank C

Chapter 4. intelligence-led Cyber Attack Simulation Testing (iCAST)

4.1. Introduction

4.1.1. Traditional penetration tests have provided a detailed and useful assessment of possible technical vulnerabilities, often within a single system or an isolated environment. However, the range of likely scenarios of a targeted attack against an AI (including people and processes as well as technologies) may not be fully covered by traditional penetration tests.

4.1.2. In addition, the scope of penetration tests may not allow an AI to evaluate its capability to identify and respond to a cyber attack, or provide metrics or key performance indicators (KPIs) to measure effectiveness of the cyber resilience programme of an AI. In order to gain an appropriate level of assurance that key financial assets (e.g. data) and systems are protected against technically sophisticated and persistent attacks, testing efforts need to be enhanced and the testers are required to be armed with up-to-date and specific threat intelligence.

4.1.3. In response to these needs and challenges, the HKMA has introduced a new intelligence-led Cyber Attack Simulation Testing (iCAST) framework, which makes reference to the latest internationally recognised testing frameworks.

4.1.4. Under iCAST, the traditional penetration test is augmented by further validation of the knowledge of the penetration tester(s) and threat intelligence to formulate end-to-end testing scenarios (from attack initiation to achieving pre-defined test goal(s). Details about test goal can be found in section 4.5). This will allow the tester(s) to more closely simulate real life attacks from competent adversaries. The AIs should adopt a risk based approach to select the scenarios to be tested under iCAST. In addition, the iCAST

provides KPIs that will help benchmark the ability of the AI to detect and respond to such attacks. There is no specific requirement regarding the tools to be used for conducting iCAST.

4.1.5. AIs which aim to attain the "intermediate" or "advanced" maturity level are required to execute the iCAST during the "maturity assessment" process.

4.1.6. Although the HKMA has introduced the iCAST, traditional penetration tests remain important in many circumstances. AI should perform those tests based on the requirements set out in other Supervisory Policy Manuals, if applicable, and section 4.1 of the maturity assessment matrix in Appendix B.

4.2. Comparing iCAST with traditional penetration testing: what's new?

4.2.1. As set out above, traditional penetration testing usually has a limited scope and focuses on the technical assessment of a single system or an isolated environment. However, latest cyber attacks are often stealthy, targeting at the weakest link of a protection measure (e.g. through phishing emails targeting at AIs' staff), which usually involve people and processes of an AI.

4.2.2. iCAST is specially designed to, and preferred to be, run in the production environment[3] to simulate a real life attack, which also include the assessment of the readiness of human and process elements of an AI.

4.2.3. For example, the assessment of the phishing email "click through" rate could be an indicator on general awareness of the AI;

[3] It is preferred to run the test in the production environment. The control group could decide to run the test in a production like (UAT or pre-production) environment if, for example, the control group has concerns that the test could be intrusive and may cause outage or impact to the production operations. Details on control group can be found in paragraph 4.3.1 of this document.

successful detection of the simulated incident may indicate that the detection mechanism is effective; and a timely and proper damage containment could demonstrate that the response plans are well designed and implemented.

4.2.4. Figure 14 below illustrates the special attentions iCAST can bring on top of traditional penetration testing.

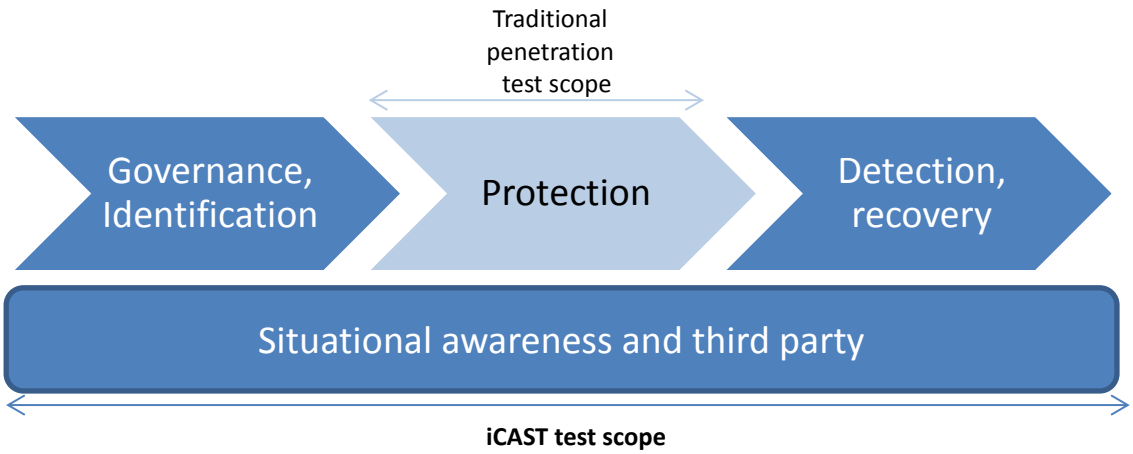

Figure 14: scope differences between traditional penetration test and simulation test (in terms of cybersecurity maturity domains)

4.3. Oversight committee for performing iCAST

4.3.1. Before executing the iCAST, AIs should form a control group to oversee the planning and the execution of the testing process. The group should include senior individuals, usually one for each system being tested under the defined scope, who understands the critical assets and systems, and the economic functions that those assets and systems enable. The representatives will need to be senior enough to understand the risks associated with the activities and they can have access to the security incident escalation chain to control the impact of the simulation within the company. They are made aware of the iCAST, the option of keeping the test in a silent mode, the process of the iCAST and should an iCAST simulated incident be detected.

4.3.2. In case an AI detected an incident, which could be an iCAST

simulated incident, the control group should confirm with the testing team if this is a simulated incident or a real attack from attackers by matching the activities records provided by the tester with the actual detected activities. If it is confirmed to be a simulated incident, the control group should allow incident response team to continue to carry out the incident response plan, such as damage containment. However, the control group should monitor the execution of escalation procedures to avoid placing a false alarm to external parties.

4.3.3. The group will agree the test objectives in terms of systems, processes, partners to be included and the objectives in terms of confidentially, integrity and availability.

4.4. The Five Phases of iCAST

4.4.1. There are five phases in executing the iCAST as set out below.

- Scoping
- Developing threat intelligence analysis
- Developing testing scenarios
- Test
- Reporting

4.4.2. Figure 15 below shows the parties involved and their related task(s) in each phase.

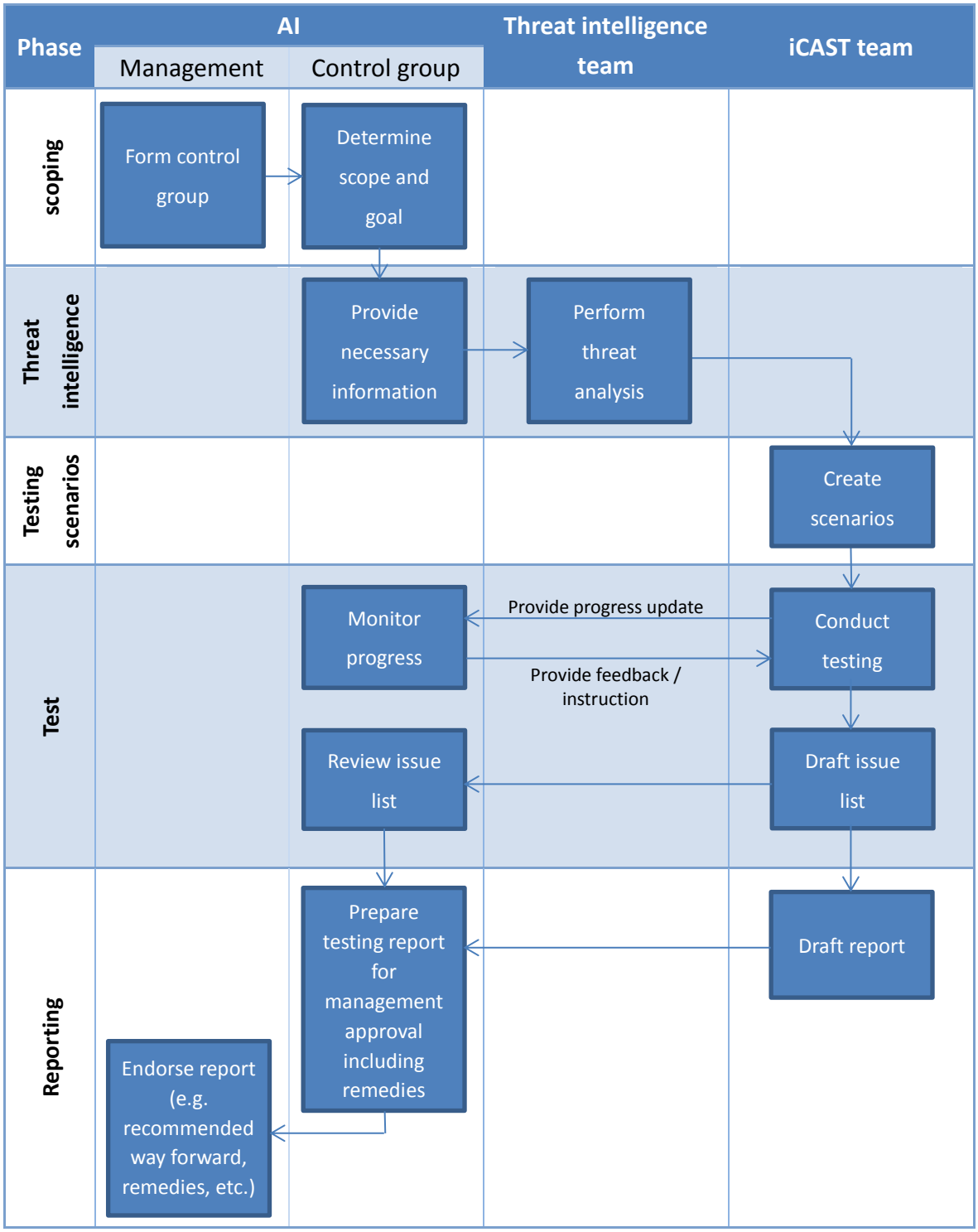

Figure 15: process flow of iCAST

4.5. Phase 1 – Scoping

4.5.1. **Identifying key functions** – AIs should set out all key business and support functions which are under the scope coverage. Key functions are those the failure of which would likely:

- create material operational and reputation risks;
- lead to possible significant financial loss.; or
- cause detrimental impact on the financial stability of Hong Kong.

4.5.2. **Identifying critical services or systems** – Based on the key business and support functions identified, AIs should set out the critical services or systems under each key function. The purpose of each critical service or system should be clearly stated.

4.5.3. **Determining the compromise actions for the testing purpose** – For each critical service and system identified, the tester(s) should determine the threat category (Confidentiality, Integrity and Availability) and test goal (testing activity aims to demonstrate the type(s) of compromise, such as Exfiltration, Insertion, and Privilege Escalation). All of the information should be input to the scoping table as illustrated in Figure 16.

Key function	Key system	Threat Category	Test goal (or compromise action)
Clearing and Settlement	System A	Integrity	Insertion
		Availability	Privilege escalation

Figure 16: an example of scoping table

4.6. Phase 2 – Analysing threat intelligence analysis

4.6.1. **What is threat intelligence –** Threat intelligence is information which may provide details of the motivations, intent, game plan and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. The primary purpose of gathering threat intelligence is to inform business to make decisions and ensure preparedness regarding the risks, implications and defence mechanisms associated with threats.

4.6.2. **Usage of threat intelligence** – By leveraging threat intelligence, an AI can transform itself from a reactive approach to a proactive approach on preventing, defending and detecting possible cyber attacks. The threat intelligence can make the iCAST more tailored to and abreast of the latest threats of AIs.

4.6.3. **Purposes of performing threat intelligence analysis** – Cyber threat intelligence analysis involves the gathering of threat intelligence from a wide range of sources. The analysis needs to validate the intelligence and ensure its currency and accuracy. Such intelligence can be tailored into testing scenarios for the penetration tester(s) to conduct.

4.6.4. Threat intelligence can help create realistic threat scenarios describing attacks against an AI, which can be used by a simulation attack team to guide its simulation test. Scenarios are based on available real world threat actors combined with open source intelligence on the AI as well as some knowledge of the key functions that form the scope and target of the test.

4.6.5. **Threat intelligence report** – The threat intelligence report presents a summary of the key threats, detailed profiles of the highest-scored threats and potential scenarios in which a high scoring threat actor might target the AI. Threat scenarios in this

report are based on real-life examples of cyber attacks including the motivations of the attackers, their objectives and the methods they employ to meet them. Scenarios will be further developed into realistic and effective simulation test plan for next phase.

4.6.6. Besides, threat actor goals should be included in the threat intelligence report, which provide a set of milestones and goals (for details, please refer to paragraph 4.7.2 of this document) that the simulation testing team aims to achieve.

4.6.7. **Generic report** – With respect to AIs with a "medium" inherent risk level, they need to accomplish the "intermediate" maturity level at a minimum accordingly, and a simplified version of threat intelligence report is adequate for this case. The simplified version is a generic threat intelligence report which basically covers threat intelligence of the Hong Kong banking industry, in which the report should be prepared within three months before the test is carried out, and is not necessary to be tailored for a specific AI.

4.6.8. **Tailored report** – If an AI's inherent risk level is "high", a tailored threat intelligence report is required. Such report is needed for performing the simulation testing in order to accomplish the advanced maturity level of cyber resilience to match its inherent risk profile. Threat actors in this tailored report should be generated based on targeted threat intelligence analysis for the AI.

4.6.9. Regardless of whether an AI is going to use generic or tailored threat intelligence report, the report should be generated by a qualified person/team. For details about qualification requirement, please refer to Chapter 5.

4.7. Phase 3 – Testing scenarios

4.7.1. Based on a risk-based approach, tester(s) should develop several testing scenarios ("test cases"), which simulate real-life, high-risk attacks. Testing scenarios should be generated based on the threat intelligence report prepared in Phase 2.

4.7.2. Each scenario is a "story line" of the test, which should include,

- **Test goal(s)** – one or more pre-agreed end goal(s) of each testing scenario, which can be evidence showing that the tester(s) can take adverse actions against the AI which may compromise confidentiality, integrity and/or availability of the AI, such as: (i) get access to, delete or alter a specific piece of information; (ii) control of certain access rights of a critical system or service; iii) bring down a critical system, system component and/or service of the AIs, iv) encrypting important files for ransom, v) initiating funds movements to other AIs, etc. The tester(s) are only required to demonstrate the capabilities with evidence supporting the conclusion, and is/are NOT required to carry out the compromising actions.
- **Initiation of test** – determine channels and techniques to be used for launching the attack.
- **Chain of tasks** – after the initiation of test, what are the target steps to be followed to achieve the pre-agreed goal(s).
- **Milestones** – interim test goals, such as to gain access or control to internal systems, service, computing resources, and stay persistence.
- **Timeline** – the targeted and agreed time to complete each task. If a task cannot be accomplished within the timeline, the participating AI is considered to have successfully protected itself against the test (attack), or detected the test (attack). The test results, despite their positive or negative in nature, would be included as one of the KPIs in the final report.
- **Condition(s) for continuing or stopping the test** – identify pre-agreed condition(s) to which tester(s) should stop the test, (e.g. making impact to the participating AIs' system performance) or gain supports (such as necessary information required to carry the next action in story line) from the participating AIs (when any of the pre-set tasks failed to perform within the pre-set timeline as mentioned above) to continue the test.

4.8. Phase 4 – Testing

4.8.1. In the testing phase, the tester(s) should carry out the testing based on the scenarios determined in phase 3 mentioned above.

4.8.2. The testing team should communicate with the control group closely, at least on a weekly basis, to share the progress of testing, obstacles encountered, and determine if the test should be continued.

4.9. Phase 5 – Reporting

4.9.1. After the testing process, the following reports should be produced:

i) iCAST simulation test summary;
ii) Threat intelligence report (see paragraph 4.6.53); and
iii) Simulation testing report (see paragraph 4.9.4).

(1) Report to be endorsed by AI's management

4.9.2. AIs, with the support of tester, should prepare the iCAST simulation test summary. Management of the AI should review and endorse the testing result accordingly.

(2) Report to be submitted

4.9.3. **Threat intelligence report** – As mentioned in paragraph 4.6.5, a threat intelligence report should have been prepared in testing. The threat intelligence report should be attached together with the summary.

4.9.4. **Simulation testing report** – Simulation testing report includes details of the approach taken to the testing, the results and observations from the test, and where necessary, areas for improvement in terms of governance, policies and procedures, technical controls, education and awareness. In case the test was conducted by AI's internal resources, the report should be reviewed and endorsed by management of the AI.

Chapter 5. Qualification requirements

5.1. General requirements

5.1.1. For carrying out the inherent risk assessment, maturity assessment and the iCAST, AIs should engage assessor(s) and tester(s) which are competent and qualified. The assessor(s) and tester(s) should have sufficient qualification and experience to conduct the above mentioned assessments or tests.

5.1.2. The HKMA has been working with Hong Kong Institute of Bankers (HKIB) and the Hong Kong Applied Science and Technology Research Institute (ASTRI), to launch a Professional Development Programme in cybersecurity, essentially a training and certification programme. With the support from CREST International, a UK based cybersecurity certification body, the programme in Hong Kong is designed and benchmarked against the latest international standards in this field. Cybersecurity professionals who have obtained the relevant certificates under this new training programme will generally be considered as having the required expertise to perform the assessments and testing under C-RAF.

5.1.3. Cybersecurity professionals who have obtained other qualifications in related fields may also be regarded as having the required expertise to perform the assessments and testing under C-RAF. It is our policy to put in place suitable arrangements to ensure that relevant or equivalent experience and expertise in the cybersecurity field will be appropriately recognised for this purpose. In this connection, the HKMA is prepared to set up a proper mechanism for determining the equivalent qualifications, taking into account the local circumstances and comments from the industry.

5.2. Roles involved in the assessment and testing process, and their required level of expertise

5.2.1. Under C-RAF, there are two types of cybersecurity professionals involved, namely the "assessors" and the "testers".

5.2.2. The "assessors" are responsible for conducting the inherent risk and maturity assessments. With respect to the assessors' qualification requirement, please refer to section 5.3.1.

5.2.3. The "testers" are responsible for performing the iCAST tasks.

- An "**iCAST manager**" manages the attack simulation testing from a project management perspective. An iCAST manager should have a wide breadth of knowledge in all areas of simulation testing and proven experience in managing incidents, penetration tests and attack simulation exercises.

- An "**iCAST specialist**" performs threat intelligence collection and analysis and compiles threat intelligence report ; designs test scenarios based on threat intelligence report; initiates test through various channels (such as phishing email, social engineering, etc.) and concludes final test goals. An iCAST specialist should be the core person who conducts the testing, and may be assisted by other iCAST tester(s), if necessary. An iCAST specialist should have proven experience in penetration tests and attack simulation testing exercises.

- An "**iCAST tester**" should have adequate knowledge to support iCAST specialists to conduct attack simulation testing, such as analysis of data collected and preparation of the findings/issues and/or the assessment report.

- There is no specific requirement on the size and structure of the iCAST team. It should be flexible to fit with the different levels of complexity of the testing. For example, an iCAST team member can also join the threat intelligence team set out in figure 15.

5.3. Mapping of roles and qualification requirements

5.3.1. Figure 17 below summarises the key roles participating C-RAF with qualification requirements are imposed. Relevant certificates are listed here for reference.

Role	Relevant certificates
Assessor	• Certified Information Systems Auditor (CISA), • Certified Information Systems Security Professional (CISSP) or other equivalent qualification.
iCAST manager	• CCASP[4] – Certified Simulated Attack Manager or other equivalent qualification.
iCAST specialist	• CCASP – Certified Simulated Attack Specialist or other equivalent qualification.
iCAST tester	• CCASP – Certified Infrastructure Tester • CCASP – Certified Web Application Tester or other equivalent qualification.

Figure 17: A mapping of roles and qualification requirements

[4] Certified Cyber Attack Simulation Professional (CCASP) is the new certification programme of Hong Kong Institute of Bankers (HKIB), which is supported by CREST International.

Appendix A – Inherent risk matrix

Category 1 – Technologies

- When determining the inherent risk of this category, consideration is also given to the overall set-up of the IT infrastructure. Certain types of technologies and connections may pose a higher inherent risk to AIs depending on the complexity and maturity, and nature of the specific technology products or services.

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Total number of Internet service provider (ISP) connections (including branch connections) which are connected to the corporate network	Number of connections	Less than 6	Between 6 – 12	More than 12	[Low/ Medium/ High/ Not applicable]	
Unsecured external connections, number of connections not users (e.g., file transfer protocol, Telnet, rlogin)	Number of unsecured connections	Less than 2	Between 2 – 6	More than 6	[Low/ Medium/ High/ Not applicable]	
Wireless network access	Separate access points for guest and corporate wireless	Physically separated	Logically separated	No separation	[Low/ Medium/ High/ Not applicable]	
Non-corporate devices (physical devices not	Number of staff who can get access	Less than 10	between 10 - 100	More than 100	[Low/ Medium/ High/ Not applicable]	

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
owned by AIs) allowed to connect to the corporate network	corporate resources using non-corporate device					
	Application	Not allowed	E-mail access only	E-mail access or more	[Low/ Medium/ High]	
Third parties, including number of organisations and number of individuals from vendors and subcontractors, with access to internal systems	Number of third parties or third parties individuals	Less than 5 third parties or less than 20 individuals	6 to 10 third parties or 21 to 50 individuals	More than 10 third parties or more than 50 individuals	[Low/ Medium/ High/ Not applicable]	
	How they access systems	On-site	Virtual private network over leased line	Virtual private network over the Internet	[Low/ Medium/ High/ Not applicable]	
Wholesale customers with dedicated connections	Number of dedicated connections	Less than 5	Between 5 – 10	More than 10	[Low/ Medium/ High/ Not applicable]	
Internally hosted and in-house developed applications supporting critical activities	Number of applications	Less than 5	Between 5 - 20	More than 20	[Low/ Medium/ High/ Not applicable]	
Internally hosted, vendor-developed applications supporting critical activities	Number of applications	Less than 10	Between 10 - 50	More than 50	[Low/ Medium/ High/ Not applicable]	

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
User-developed technologies (UDT) and end-user computing that support critical activities	Number of UDTs -- (includes Microsoft office end-user developed tools)	Less than 20	Between 20 – 50	More than 50	[Low/ Medium/ High/ Not applicable]	
End-of-life (EOL) systems of critical operations	Number of systems that have reached EOL and have no further support/patch from vendor	Less than 2	Between 2 - 5	More than 5	[Low/ Medium/ High/ Not applicable]	
Open Source Software (OSS) with no commercial support	Number of OSS supporting critical operations	Less than 2	Between 2 - 10	More than 10	[Low/ Medium/ High/ Not applicable]	
Network devices (e.g., routers, and firewalls; include physical and virtual)	Number of network devices	Less than 50	Between 50 - 200	More than 200	[Low/ Medium/ High/ Not applicable]	
Individuals and/or third-party service providers that support critical activities[5], which have direct or indirect implications to cyber risk	Number of individuals from third-party or third party service providers support critical activities	Less than 5 third party service providers or Less than 10 individual	Between 5 to 10 third party service providers or 10 to 50 individual	More than 10 third party service providers or more than 50 individual	[Low/ Medium/ High/ Not applicable]	

[5] Third-party service providers -- do not have access to internal systems, but the AI relies on their services.

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Cloud computing services hosted externally to support critical activities	Use of cloud computing	None	Private cloud only	Public, hybrid, private and/or international cloud	[Low/ Medium/ High]	
	Number of cloud computing services	Less than 2	Between 2 – 5	More than 5	[Low/ Medium/ High/ Not applicable]	

Category 2 – Delivery Channels

- Different delivery channels for products and services may pose various risks to AIs.
- The inherent risk of an AI normally heightens as the variety and number of delivery channels increases.
- A higher inherent risk is resulted in this category, for example, if products and services are delivered through online and mobile delivery channels and automated teller machine (ATM) operations are connected to the Internet.

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Internet presence (customer)	Type of Internet web-facing services	None	The channel is used for informational only	Provide banking services	[Low/ Medium/ High]	
Mobile presence	Type of services provided	None	The channel is used for informational or notification purpose	Provide banking services	[Low/ Medium/ High]	
Social media presence	Type of services provided	None	The channel is used for informational or communicate to customers	Provide banking services (e.g. Retail account origination, partnership with social media companies)	[Low/ Medium/ High]	
Automated Teller Machines (ATM) (Operation)	Network of the ATM machines	Self-managed or managed by a third party in a closed network. (e.g. cash reload services outsourced)	Managed by a third party and with connections to other FIs (e.g. joint ATM network)	Self-managed or managed by a third party and with connection to the Internet	[Low/ Medium/ High/ Not applicable]	

Category 3 – Products and technology services

- Different products and technology services offered by AIs may pose a higher inherent risk depending on the nature of the specific product or service offered. This category covers various payment services and also includes consideration of whether the AI provides technology services to other organisations.

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Issue debit or credit cards	Number of valid cards issued	Less than 10,000	Between 10,000 to 100,000	More than 100,000	[Low/ Medium/ High/ Not applicable]	
Prepaid cards	Number of valid cards issued	Less than 5,000	Between 5,000 to 10,000	More than 10,000	[Low/ Medium/ High/ Not applicable]	
Person-to-person payments (P2P)	Number of customers	Less than 10,000	Between 10,000 - 50,000	More than 50,000	[Low/ Medium/ High/ Not applicable]	
	Monthly transaction volume	Less than 100,000	Between 100,000 - 500,000	More than 500,000	[Low/ Medium/ High/ Not applicable]	
Wire transfers	Request channel(s)	In person	In person, phone, and fax	Online, text, e-mail, mobile or others	[Low/ Medium/ High/ Not applicable]	
	Type of wire transfer	None	SWIFT	Others	[Low/ Medium/ High]	
Global remittances	Gross daily transaction volume (% of total assets)	Less than 3%	Between 3% to 25%	More than 25%	[Low/ Medium/ High/ Not applicable]	
Treasury services and	Services offered	Limited services offered	Services offered -- lockbox, CHATS	services offered -- currency services,	[Low/ Medium/ High/ Not	

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
clients			origination, remote deposit capture	online investing, investment sweep	applicable]	
	Number of clients	Less than 1,000	Between 1,000 to 10,000	More than 10,000	[Low/ Medium/ High/ Not applicable]	
Trust services	Assets under management total	Less than HK$1 billion	Between HK$1 billion to HK$50 billion	Over HK$50 billion	[Low/ Medium/ High/ Not applicable]	
Act as a correspondent bank (Interbank transfers)	Number of bank served act as a correspondent bank	Less than 50 institutions	Between 50 to 200	More than 200	[Low/ Medium/ High/ Not applicable]	
Merchant acquirer (sponsor merchants or card processor activity into the payment system)	Operational model	Act as a merchant acquirer	Act as a merchant acquirer; outsource card payment	Act as a merchant acquirer and card payment processor	[Low/ Medium/ High/ Not applicable]	
	Number of merchants	Less than 1,000	Between 1,000 – 10,000	More than 10,000	[Low/ Medium/ High/ Not applicable]	
Securities trading	Daily aggregate transaction total	Less than HK$100 million	Between HK$100 million to HK$1 billion	Over HK$1 billion	[Low/ Medium/ High/ Not applicable]	

Category 4 – Business size and organisational characteristics

- This category considers business size and organisational characteristics, such as number of branches in Hong Kong, asset valuation (based on audited financial statement), number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in the IT control environment, locations of business presence, and locations of operations and data centres.

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Total number of branches	Number of branches in Hong Kong	Less than 20	Between 20 to 50	More than 50	[Low/ Medium/ High/ Not applicable]	
Total revenue of HK business	Total revenue value in HK Dollar	Less than 0.1 billion	Between 0.1 billion to 10 billion	More than 10 billion	[Low/ Medium/ High/ Not applicable]	
Total asset value of HK business	Total global asset value in HK Dollar	Less than 1 billion	Between 1 billion to 100 billion	More than 100 billion	[Low/ Medium/ High/ Not applicable]	
Host IT services for other organisations (either through joint systems or administrative support)	Number of unaffiliated organisations being supported	Less than 2	Between 2 – 5	More than 5	[Low/ Medium/ High/ Not applicable]	

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Direct employees of the whole AI supporting Hong Kong Business (including information technology and cybersecurity contractors)	Number of employees	Less than 500	Between 500 to 1,000	More than 1,000	[Low/ Medium/ High/ Not applicable]	
Changes in IT and cybersecurity staffing	Turnover of key and senior personnel[6] within the last 12 months	Less than 10	Between 10 to 20	More than 20	[Low/ Medium/ High/ Not applicable]	
Privileged access (administrators–network, database, applications, systems, etc.)	Administration staff are maintained in-house or out-sourced	All in-house	less than 50% are out-sourced	more than 50% are out-sourced	[Low/ Medium/ High/ Not applicable]	
	Turnover rate (per annum)	Less than 10%	Between 10% to 30%	Over30%	[Low/ Medium/ High/ Not applicable]	
Number of Cybersecurity staff supporting Hong Kong business (including staff who take care of cybersecurity in all 3 lines of defence)	No. of staff	More than 30	Between 10 and 30	Less than 10	[Low/ Medium/ High/ Not applicable]	

[6] Please refer to the Glossary for the definition of the "Key and Senior personnel"

Category 5 – Tracked records on cyber threats

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
Reported cyber attacks impacting the AI for Hong Kong business (last 12 months)	Number of attempted cyber attacks (e.g. SQL injection, social engineering, etc.)	No attempted attacks or reconnaissance	10 or less	More than 10	[Low/ Medium/ High]	
	Number of successful but contained attacks without any direct or indirect loss	No successful but contained attacks	5 or less	More than 5	[Low/ Medium/ High]	
	Number of breaches (bypassed all layers of defence architecture prepared by the AI) and caused direct or indirect loss	No breach record	2 or less	More than 2	[Low/ Medium/ High]	
	Types of attacks - Phishing	No phishing attack	Employees and customers received *generic* phishing campaigns.	Employees and customers received targeted phishing campaigns.	[Low/ Medium/ High]	
	Types of attacks - (Distributed) Denial of Service (DoS/ (DDoS)	No DoS incident	Experienced randomly attempted DoS attack.	Experienced focus and repeatedly attempted DoS attack.	[Low/ Medium/ High]	
	Types of attacks	No reported social engineering incident	Targeting high net worth customers and	Targeting specifically to attack senior	[Low/ Medium/	

Indicators	Assessment criteria	Inherent Risk Level				Supplementary information (sizing, volume and judgement info)
		Low	Medium	High	Conclusion	
	- Social engineering		employees at the AI, or its third parties service providers.	management, administrators, and highly privileged application users.	High]	
	Types of attacks - Malware	No malware were detected or malware were detected at the network firewall, mail gateway or web proxy.	Malware were detected at the endpoints' anti-virus / anti-malware tool.	Malware were detected at the mission-critical application servers or infrastructure.	[Low/ Medium/ High]	

Inherent risk level profile

- Count the total number of assessment criteria rated "low", "medium" and "high" respectively, and fill in the table below. As a general rule, the inherent risk level with the most assessment criteria rated will be regarded as the overall inherent risk level of the AI. Nevertheless, the AI is also suggested to take into account other relevant factors (such as the nature and complexity of its products and services, its size, its business model and its customer base) in determining its overall inherent risk level.

Inherent risk level	Number of assessment criteria rated with inherent risk level "low", "medium" or "high"
High	
Medium	
Low	
Overall inherent risk level determined by the AI	High / Medium / Low
The AI's rationales in determining its overall inherent risk level	

Appendix B – Maturity assessment matrix

Please fill in the assessment template to show the extent to which each of the detailed requirements under each component has been implemented. Please do so by selecting the appropriate option, i.e. "Y", "AC", "RA", "N" and "NA".

Option	Explanation	Description
[Y]	Yes	The control principle is effectively accomplished
[AC]	Alternative Controls	The control principle is considered to be accomplished through the implementation of alternative controls which are also considered to be effective, although the way of accomplishment is not as described in the matrix. Under such circumstances, the assessor should provide details of the alternative controls in the "justification" column.
[RA]	Risk Accepted	The control principle is considered to be accomplished through a risk mitigating measure and the residual risk associated with the control principle is formally accepted by the AIs, based on their risk appetite and risk treatment plan. Under such circumstances, the assessor should provide details of the risk mitigating measure and the residual risk acceptance in the "justification" column.
[N]	No	The control principle is not effectively accomplished.
[NA]	Not Applicable	The control principle is not applicable to the AI, and therefore the control principle is excluded from the determination of the component maturity. Under such circumstance, the assessor should provide the rationale of the exclusion of the control principle in the "justification" column.

Domain 1 – Governance

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
1.1	**Cyber resilience oversight**		
Baseline	**1.1.1 Board and Senior management oversight**		
	• Designated members of management or an appropriate board committee should be held accountable to the board for implementing and managing cybersecurity and business continuity programmes.	**[ ]**	
	• Cybersecurity risks are included in the agenda items in management meetings when prompted by highly visible cyber events or regulatory alerts. These updates can be presented by a senior representative with Technology Risk Management, or Cybersecurity or Information Security function.	**[ ]**	
	1.1.2 Budgeting process		
	• Cybersecurity resources, tools and staff are budgeted items and are reviewed through periodic budgeting processes.	**[ ]**	
	• There is a process to formally discuss and estimate potential expenses of Cybersecurity measures and loss associated with cyber incidents as part of the budgeting process.	**[ ]**	
	1.1.3 Regular reporting		
	• Management provides a written report on the overall status of the cybersecurity and business continuity programmes to the board or an appropriate board committee at least annually.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**1.1.1 Board and Senior management oversight**		
	• A cyber risk appetite statement is in place and approved by the board or an appropriate board committee.	**[ ]**	
	• At least annually, the board or an appropriate board committee reviews and approves the cybersecurity programme.	**[ ]**	
	• Management or a dedicated committee is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.	**[ ]**	
	• There is a process to ensure that cyber risks that exceed the risk appetite are escalated to management or a dedicated committee.	**[ ]**	
	1.1.2 Budgeting process		
	• The board or an appropriate board committee reviews and approves management's prioritisation and resource allocation decisions based on the results of the cyber risk assessments.	**[ ]**	
	1.1.3 Regular reporting		
	• Management provides a written report on the overall status of the cybersecurity and business continuity programmes to the board or an appropriate board committee at least quarterly.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Y/RA/N/NA***
Advanced	**1.1.1 Board and Senior management oversight**		
	• The board or an appropriate board committee has cybersecurity expertise or engages experts to provide assistance in oversight responsibilities.	**[ ]**	
	• The board or an appropriate board committee has a process to ensure that management takes appropriate actions to address the changing cyber risks or any significant cyber issues.	**[ ]**	
	• Management has a formal process to continuously improve cybersecurity oversight.	**[ ]**	
	• Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.	**[ ]**	
	1.1.2 Budgeting process		
	• The budgeting process for requesting additional cybersecurity staff and tools is integrated into business units' budgeting processes.	**[ ]**	
	• The budgeting process for requesting additional cybersecurity resources, staff and tools is in line with the current resources and tools to the cybersecurity strategy.	**[ ]**	
	1.1.3 Regular reporting		
	• The standard board meeting package includes reports and metrics that go beyond events and incidents, and able to address the cyber threat trends and the AI's cybersecurity posture.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
1.2	**Strategy and policies**		
Baseline	**1.2.1 Strategy and programme** • A cybersecurity strategy is in place and integrates technology, policies, procedures, and training to mitigate the cyber risk. • There is enterprise-wide coordination in all elements of the cybersecurity programme. **1.2.2 Policies** • Policies commensurate with its cyber risk and complexity are in place to address the concept of cyber threat intelligence sharing. • Board-approved policies commensurate with its cyber risk and complexity that address cybersecurity are in place. • Policies commensurate with its cyber risk and complexity are in place to address the concepts of incident response and resilience.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	
Intermediate	**1.2.1 Strategy and programme** • A cybersecurity strategy is in place to augment its cyber resilience. • A formal cybersecurity programme is in place and is based on technology and security industry standards or benchmarks. **1.2.2 Policies** • A formal process is in place to update policies as the inherent cyber risk profile changes.	**[ ]** **[ ]** **[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
Advanced	**1.2.1 Strategy and programme** • Management periodically review the cybersecurity strategy to address evolving cyber threats and changes to the inherent cyber risk profile.	**[ ]**	
	• The cybersecurity strategy is incorporated into, or conceptually fits within, the enterprise-wide risk management strategy.	**[ ]**	
	• Management link the strategic cybersecurity objectives to tactical goals.	**[ ]**	
	• The cybersecurity strategy outlines the future state of cybersecurity with short-term and long-term perspectives.	**[ ]**	
	1.2.2 Policies • A comprehensive set of policies commensurate with its risk and complexity is in place to address the concepts of threat intelligence.	**[ ]**	
	• A formal process is in place to cross-reference and update all policies related to cyber risks across business lines in a timely manner.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
1.3	**Cyber risk management**		
Baseline	**<u>1.3.1 Cyber risk management function</u>** • A cybersecurity and business continuity risk management function(s) is in place. **<u>1.3.2 Risk management programme</u>** • The risk management programme incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting. • Management review and use the results of audits to improve the existing cybersecurity policies, procedures, and controls. • Management monitor moderate and high residual risk issues from the cybersecurity risk assessment until items are adequately addressed. • A social media policy is in place to provide guidance to staff for not posting work related sensitive information to social media.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	
Intermediate	**<u>1.3.1 Cyber risk management function</u>** • The dedicated or non-dedicated cybersecurity function has a clear reporting line that does not present a conflict of interest concern. • A formal cybersecurity programme is in place and based on technology and security industry standards or benchmarks.	**[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
	1.3.2 Risk management programme • The risk management programme specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance). • Benchmarks or target performance metrics are established for showing improvements or regressions of the security posture over time. • Management use the results of audits and review to improve cyber resilience.	**[ ]** **[ ]** **[ ]**	
Advanced	**1.3.1 Cyber risk management function** • Risk management staff reports to management and the board or an appropriate board committee about any significant discrepancies from business unit's assessments of cyber-related risk. **1.3.2 Risk management programme** • Cybersecurity metrics are used to facilitate strategic decision-making and funding in areas of need. • Cyber risk management monitors cyber-related risk limits for business units. • The cyber risk data aggregation and real-time reporting capabilities support the ongoing reporting needs, particularly during cyber incidents. • A cyber insurance programme is being evaluated to reduce the institutional risk exposure.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
1.4	**Audit**		
Baseline	**<u>1.4.1 Audit scope</u>** • Audit or review evaluates policies, procedures, and controls for significant cyber risks and control issues based on a risk-based approach, associated with operations, including cyber risks in new products, emerging technologies, and information systems. • The audit function validates controls related to the storage or transmission of confidential data. • The audit function validates that the cyber risk management function is commensurate with the cyber risk and complexity. • The audit function validates that the cyber threat intelligence collection and collaboration are commensurate with the cyber risk and complexity. • The audit function validates that the cybersecurity controls is commensurate with the cyber risk and complexity. **<u>1.4.2 Audit function</u>** • A formal process is in place for the audit function to update its procedures based on changes to the inherent cyber risk profile.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**1.4.1 Audit scope** • The audit function validates that the cyber incident response programme and resilience are commensurate with the cyber risk and complexity. • The audit function regularly reviews management's cyber risk appetite statement. **1.4.2 Audit function** • A formal process is in place for the audit function to update its procedures based on changes to the evolving cyber threat landscape across the sector.	**[ ]** **[ ]** **[ ]**	
Advanced	**1.4.1 Audit scope** • Audit function regularly reviews the cyber risk appetite statement in comparison to assessment results and incorporates a review of gaps identified. • Audits or reviews are used to identify cybersecurity control weaknesses, their root causes, and the potential impact to business units. **1.4.2 Audit function** • A formal process is in place for the audit function to update its procedures based on changes to the evolving cyber threat landscape across other sectors the institution depends upon.	**[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
1.5	**Staffing and training**		
Baseline	**<u>1.5.1 Staffing</u>**		
	• Cybersecurity roles and responsibilities have been clearly identified and defined.	**[ ]**	
	• Formal processes are in place to identify additional cybersecurity expertise, resources and tools needed to improve cybersecurity defences.	**[ ]**	
	• Staff with cybersecurity responsibilities have the requisite qualifications to conduct the necessary tasks of the position.	**[ ]**	
	<u>1.5.2 Training</u>		
	• Annual cybersecurity training includes cyber incident response, current cyber threats (e.g., phishing, spear phishing and social engineering), and emerging issues.	**[ ]**	
	• Staff members receive cyber threat intelligence regularly and when prompted by highly visible cyber events or regulatory alerts.	**[ ]**	
	• A continuing training and skill development programme for cybersecurity staff is in place.	**[ ]**	
	• Management ensure that adequate cybersecurity training is provided to relevant staff, which is appropriate to their job responsibilities.	**[ ]**	
	• Employees with privileged account permissions receive additional cybersecurity training commensurate with the levels of their responsibilities.	**[ ]**	
	• Business units are provided with cybersecurity training relevant to their particular business risks.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
Intermediate	**1.5.1 Staffing** • Management with appropriate cybersecurity knowledge and experience are responsible for leading the cybersecurity efforts. • Staff members with cybersecurity responsibilities periodically renew the requisite qualifications for performing the necessary tasks of their positions. • Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk. • Audits or management reviews are done to identify gaps in existing security capabilities and expertise. **1.5.2 Training** • Management should ensure the effectiveness of cyber resilience for all levels of staff members (e.g., awareness of social engineering or phishing techniques). • Management should ensure that lessons learned from social engineering and phishing exercises are adequately included in cybersecurity awareness programmes. • Retail customers and commercial clients receive cybersecurity awareness information on a regular basis. • Business units receive cybersecurity training relevant to their particular business risks.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
Advanced	**1.5.1 Staffing**		
	• A programme for talent recruitment, retention, and succession planning for the cybersecurity and resilience staff is in place.	**[ ]**	
	• Dedicated cybersecurity staff members develop, or contribute to developing, integrated enterprise-level security and cyber defence strategies.	**[ ]**	
	• Employment candidates are subject to background verification, such as employment history and reference, proportional to the confidentiality of the data accessed, business requirements, and acceptable risk	**[ ]**	
	1.5.2 Training		
	• A training policy is in place to routinely update its training to security staff to adapt to new threats.	**[ ]**	
	• Directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the cyber risk.	**[ ]**	

Domain 2 – Identification

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
2.1	**IT asset identification**		
Baseline	**2.1.1 IT asset management** • An inventory of the IT assets (including hardware, software, data, and systems hosted internally and externally) is maintained.	**[ ]**	
	• The IT assets (including hardware, software, data, and systems) are prioritised for cybersecurity protection based on the data classification and business value.	**[ ]**	
	• Management assign accountability for maintaining an inventory of the IT assets.	**[ ]**	
	• The IT asset inventory, including identification of critical IT assets, is reviewed at least annually to address new, relocated, re-purposed, and sunset IT assets.	**[ ]**	
	• A documented asset life-cycle process is in place to assess whether assets to be acquired are subject to appropriate cybersecurity safeguards. • A change management process is in place to request and approve changes to IT system configurations, hardware, software, applications, and security tools.	**[ ]**	

Control principle		*Implemented?*	
		Y/RA//N/NA	***Justification***
Intermediate	**2.1.1 IT asset management** • A process is in place to proactively manage systems when they approach their end-of-life (e.g., replacement) to limit cybersecurity risks. • Changes are formally approved by an authorised individual or committee with appropriate knowledge, authority and with separation of duties. • There is a formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes. **2.1.2 IT configuration management** • A formal change request, documented approval, and an assessment of security implications are required for any changes to the baseline IT configurations.	**[ ]** **[ ]** **[ ]** **[ ]**	
Advanced	**2.1.1 IT asset management** • The supply chain risk is reviewed before the acquisition of mission-critical information systems including system components. • Tools and/or processes are in place to enable tracking, updating, asset prioritising, and custom reporting of the IT asset inventory. • Tools and/or processes are in place to detect and block unauthorised changes to software and hardware. • The change management system has pre-defined thresholds for determining whether and when a cyber risk assessment of the impact of the change is required. **2.1.2 IT configuration management** • Tools are implemented to detect and block any unauthorised changes to software and hardware.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
2.2	**Cyber risk identification and assessment**		
Baseline	**2.2.1 Cyber risk identification** • The cyber risk assessment is able to identify critical systems and high-risk transactions that warrant additional cybersecurity controls. **2.2.2 Assessment scope** • A cyber risk assessment focused on safeguarding customer information is able to identify reasonable and foreseeable cyber threats, the likelihood and potential damage of cyber threats, and the sufficiency of policies, procedures, and customer information systems. • The cyber risk assessment is updated regularly to address the deployment risk of new technologies, products, services, and connections.	**[ ]** **[ ]** **[ ]**	
Intermediate	**2.2.1 Cyber risk identification** • Cyber risk assessments are done to identify the cybersecurity risks stemming from new products, services, or relationships. **2.2.2 Assessment scope** • The focus of the risk assessment has expanded beyond customer information to address all information assets (such as the internal information). • The risk assessment considers the risk of using end-of-life (EOL) software and hardware components.	**[ ]** **[ ]** **[ ]**	
Advanced	**2.2.1 Cyber risk identification** • An enterprise-wide risk management function is established to incorporate cyber threat analysis and specific risk exposure as part of the enterprise risk assessment. **2.2.2 Assessment scope** • The risk assessment is able to adjust to cater for widely known and emerging risks or risk management practices.	**[ ]** **[ ]**	

Domain 3 – Protection

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
3.1	**Infrastructure protection controls**		
Baseline	**3.1.1 Network protection**		
	• Network perimeter defence tools (e.g., border router and firewall) are used.	**[ ]**	
	• Based on risk-based approach, all network ports of high risks are monitored on an on-going basis.	**[ ]**	
	• Strong encryption is required for authentication and data transmission over wireless network. (*N/A if there are no wireless networks.)	**[ ]**	
	• There is a firewall at each Internet connection and between any Demilitarised Zone (DMZ) and internal network(s).	**[ ]**	
	• Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.	**[ ]**	
	• Changes to firewall rules should be reviewed before becoming effective.	**[ ]**	
	• The complete firewall rules should be regularly audited or verified at least annually.	**[ ]**	
	• Intrusion detection/prevention systems (IDS/IPS) detect and/or block actual and attempted attacks or intrusions.	**[ ]**	
	• Technical controls are in place to prevent unauthorised devices, including rogue wireless access devices, from connecting to the internal network(s).	**[ ]**	
	• Control measures are in place to prevent unauthorised addition of new external connections and removal of existing external connections.	**[ ]**	
	• Tools are installed to block attempted access by unregistered devices to internal networks.	**[ ]**	
	• Domain Name System Security Extensions (DNSSEC) is deployed across the enterprise.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
	3.1.2 System configuration		
	• Implementation of systems configurations (for servers, desktops, routers, etc.) is in accordance with the industry standards, which are properly enforced on an on-going basis.	**[ ]**	
	• Ports, functions, protocols and services are prohibited if they are no longer needed for business purposes.	**[ ]**	
	• Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	**[ ]**	
	• Programmes that can override system, object, network, virtual machine, and application controls are restricted, and proper authorisation is needed when used.	**[ ]**	
	• Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorised software.	**[ ]**	
	• Documented hardening standards should be in place for operating systems and network devices used in the organisation, and a process should be in place to ensure all devices (in data and voice networks) are hardened as per these standards.	**[ ]**	
	• Public-facing servers are routinely checked for integrity to limit the window of time a system is exposed to potential threats.	**[ ]**	
	3.1.3 Device protection		
	• System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Y/RA/N/NA***
Intermediate	**3.1.1 Network protection**		
	• A risk-based solution is in place for the Internet hosting provider, such as smart web content delivery process, to mitigate the risk of any disruptive cyberattacks (e.g., DDoS attacks).	**[ ]**	
	• Guest wireless networks are fully segregated physically from the internal network(s). (*N/A if there are no wireless networks.)	**[ ]**	
	• The enterprise network is segmented in multiple, separate trust or security zones with defence-in-depth strategies (e.g. logical network segmentation, hard backups, air-gapping, etc.) to mitigate the risk of cyberattacks.	**[ ]**	
	• Security controls are implemented for remote access to all administrative consoles, including restricted virtual systems.	**[ ]**	
	• Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorised traffic. (*N/A if there are no wireless networks.)	**[ ]**	
	• Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.)	**[ ]**	
	• Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network.	**[ ]**	
	3.1.2 System configuration		
	• Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defence layers.	**[ ]**	
	• Controls for unsupported systems are implemented and tested.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	***Y/RA/N/NA***
Advanced	**3.1.1 Network protection**		
	• Tools are installed and/or processes are in place to block attempted access from unpatched employee-owned devices and third-party devices	**[ ]**	
	• Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted zones.	**[ ]**	
	3.1.2 System configuration		
	• Technical measures are in place to prevent the execution of unauthorised code on the owned or managed devices, and systems components.	**[ ]**	
	• The institution proactively seeks to identify control gaps that may be used as part of a zero-day attack.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
3.2	**Access control**		
Baseline	**3.2.1 User account management**		
	• Identification and authentication are required to manage the access to systems, applications, and hardware.	**[ ]**	
	• Access controls are in place, including password complexity and limits to password attempts and reuse.	**[ ]**	
	• All physical and logical access is removed immediately upon notification of involuntary termination or voluntary departure of an employee.	**[ ]**	
	• Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.		
	• User access reviews are performed periodically for all systems and applications based on the risk exposure to the application or system.	**[ ]**	
	• All default passwords and unnecessary default accounts are changed before system implementation and on a regular basis.	**[ ]**	
	• All passwords are encrypted in storage and in transit.	**[ ]**	
	• The user accounts of the production and non-production environments are segregated to prevent unauthorised access or changes to information assets.	**[ ]**	
	3.2.2 User account provisioning		
	• Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	**[ ]**	
	• Employee access to systems and confidential data provides for separation of duties.	**[ ]**	

Control principle	*Implemented?*	
	Y/N/AC/RA/NA	*Justification*
3.2.3 Privileged user account management		
• Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).	**[ ]**	
• Administrators should either have two accounts: one for administrative use and one for general purpose, non-administrative tasks or their administrative privileges are enabled and then disabled based on the demand.	**[ ]**	
3.2.4 Customer access management		
• Customer access to internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk.	**[ ]**	
• Customer service (e.g., the call centre) utilises formal procedures to authenticate customers commensurate with the risk of the transaction or request.	**[ ]**	
3.2.5 Physical access management		
• Physical security controls are used to prevent unauthorised access to IT hardware and telecommunication systems.	**[ ]**	
• Physical access to high-risk or confidential systems is restricted, logged, and unauthorised access is blocked.	**[ ]**	
3.2.6 Remote access management		
• Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.	**[ ]**	
3.2.7 Cryptographic keys access management		
• Controls are in place to prevent unauthorised access to cryptographic keys.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**3.2.1 User account management** • Based on the risk-based approach, changes to user access permissions trigger automated notices (e.g. e-mails; Short Message Service (SMS); system alerts to the monitoring systems) to appropriate personnel.	**[ ]**	
	3.2.3 Privileged user account management • Access controls are in place for database administrators to prevent unauthorised downloading or transmission of confidential data.	**[ ]**	
	• Multifactor authentication (e.g., tokens, digital certificates) is used for employee access to high-risk systems as identified in the cyber risk assessment(s). (*N/A if no high risk systems.)	**[ ]**	
	3.2.3 3rd party access management • Strong authentication is used to secure all third-party access to the institution's network and/or systems and applications.	**[ ]**	
Advanced	**3.2.1 User account management** • Based on the risk-based approach, user access controls are in place to prevent unauthorised access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.)	**[ ]**	
	3.2.4 Customer access management • Controls are in place to prevent malware and man-in-the-middle attacks for customer authentication in high-risk transactions.	**[ ]**	
	• Tokenisation should be considered to substitute unique values for confidential information (e.g., virtual credit card).	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
3.3	**Data security**		
Baseline	**3.3.1 End point data security**		
	• Controls are in place to restrict the use of removable media to authorised personnel only.	**[ ]**	
	• Controls are in place to prevent unauthorised individuals from copying confidential data to removable media.	**[ ]**	
	• Antivirus and anti-malware tools are deployed on end-point devices that do not support sandboxing architecture (e.g., workstations, laptops, and mobile devices).	**[ ]**	
	• Mobile devices with access to the institution's data are centrally managed for antivirus and patch deployment. (*N/A if mobile devices are not used.)		
	• Institution data on a mobile device is wiped remotely when that device is missing or stolen. (*N/A if mobile devices are not used.)	**[ ]**	
	• A control process is in place to destroy or wipe data on hardware and portable/mobile media when a device is no longer needed.	**[ ]**	
	3.3.2 Data protection		
	• Confidential data are encrypted when transmitted across public or untrusted networks (e.g., the Internet).	**[ ]**	
	• Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used.)	**[ ]**	
	• Use of customer data in non-production environments (e.g. testing environment) complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements.	**[ ]**	
	3.3.3 Data disposal		
	• Polices and processes are in place to dispose or destroy data and within expected time frames.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**3.3.1 End point data security** • Data loss prevention controls or devices are implemented for outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers). • Mobile device management controls are in place, including the integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.) • If mobile devices are allowed to connect to the corporate network for storing and accessing company information, capability for remote software version/patch validation should be in place. (*N/A if mobile devices are not used.) **3.3.2 Data protection** • Tools are adopted to prevent unauthorised access to or exfiltration of confidential data.	**[ ]** **[ ]** **[ ]** **[ ]**	
Advanced	**3.3.1 End point data security** • Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container. **3.3.2 Data protection** • Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the trusted zones. • The data classification and risk assessment policies should include the criteria for encryption of select data at rest.	**[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
3.4	**Secure coding**		
Baseline	**3.4.1 Secure development** • Developers working for the institution should follow secure programme coding practices, that meet industry standards. • Based on risk-based approach, security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.) • Based on risk-based approach, security controls of internally developed software code are reviewed before migrating the code to production. (*N/A if there is no software development.) • Control process should be in place to review and assess the need to hold the intellectual property and production code in escrow. (*N/A if there is no production code to hold in escrow.) • Based on risk-based approach, security testing should occur at the unit testing, system integration testing and user acceptance testing for applications, including mobile applications. (*N/A if there is no software development.)	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	
Intermediate	**3.4.1 Secure development** • Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications. • The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.	**[ ]** **[ ]**	

Control principle		*Implemented?*	
		Y/RA/N/NA	***Y/RA/N/NA***
Advanced	**3.4.1 Secure development** • A risk-based, information assurance function is in place to evaluate the security of internal applications. • Based on risk-based approach and focusing on high-risk applications, vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production. • All interdependencies between applications and services have been identified and reviewed for adequacy. • Based on risk-based approach and focusing on high-risk applications, code reviews are completed on internally developed or vendor-provided custom applications to ensure that there are no security gaps.	**[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
3.5	**Patch management**		
Baseline	**3.5.1 Patch management programme**		
	• A patch management programme is implemented to ensure that software and firmware patches are applied in a timely manner.	**[ ]**	
	• Systems are configured to retrieve patches from the official sources.	**[ ]**	
	• Patch management reports are reviewed and reflect missing security patches and a proper follow-up process is in place.	**[ ]**	
	3.5.2 Patch assessment and testing		
	• Patches are tested before being applied to systems and/or software.	**[ ]**	
	• A formal process is in place to acquire, test, and deploy software patches based on criticality.	**[ ]**	
Intermediate	**3.5.1 Patch management programme**		
	• Tools and/or processes are in place to identify missing security patches as well as the number of days since each patch became available.	**[ ]**	
	• Missing patches across all environments are prioritised and tracked.	**[ ]**	
	3.5.2 Patch assessment and testing		
	• Operational impact is evaluated before deploying security patches.	**[ ]**	
	• Patches for high-risk vulnerabilities are tested and applied when released or the risk is accepted and accountability assigned.	**[ ]**	
Advanced	**3.5.1 Patch management programme**		
	• Patch monitoring software is installed on all servers to identify any missing patches for the operating system software, middleware, database, and other key software.	**[ ]**	
	• Patch management reports are reviewed to ensure that security patches are tested and implemented within aggressive time frames (e.g., 0-30 days).	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
3.6	**Remediation management**		
Baseline	**3.6.1 Issues management** • Issues identified in cyber risk assessments are prioritised and resolved based on criticality and within the time frames established in the response to the assessment report. • Formal processes are in place to resolve weaknesses identified during the penetration/simulation testing. **3.6.2 Testing after remediation** • Remediation efforts are confirmed by conducting a follow-up vulnerability scan.	**[ ]** **[ ]** **[ ]**	
Intermediate	**3.6.1 Issues management** • The simulation testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved. **3.6.3 Incident forensic** • Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties. • Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.	**[ ]** **[ ]** **[ ]**	
Advanced	**3.6.1 Issues management** • The maintenance and repair of organisational assets are performed by authorised individuals with approved and controlled tools only. • The maintenance and repair of organisational assets are logged and reviewed in a timely manner. • All high risk issues identified in the penetration/simulation testing, vulnerability scanning, and other testing are escalated to the board or an appropriate board committee for risk acceptance with adequate mitigating measures if not resolved in a timely manner.	**[ ]** **[ ]** **[ ]**	

Domain 4 – Detection

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
4.1	**Vulnerability detection**		
Baseline	**4.1.1 Antivirus and anti-malware** • Antivirus and anti-malware tools, used to detect attack and protect devices, are updated automatically. • E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links). **4.1.2 Penetration/Simulation testing** • Penetration testing and vulnerability scanning are conducted and analysed routinely according to the risk assessment for business systems and internal network. • Penetration testing is performed on web-based systems or devices before they are launched or undergo significant change.	[ ] [ ] [ ] [ ]	
Intermediate	**4.1.1 Antivirus and anti-malware** • E-mails and attachments are automatically scanned to detect malware and are blocked when malware is present. **4.1.2 Penetration/Simulation testing** • Audit or risk management resources review the simulation testing scope and results to help determine the need for rotating companies based on the quality of the work. • Threat Intelligence is leveraged to design testing scenarios for performing intelligence-led Cyber Attack Simulation Testing (iCAST).	[ ] [ ] [ ]	
Advanced	**4.1.2 Penetration/Simulation testing** • Vulnerability scanning is rotated to scan all high-risk systems in production environment throughout the year. • Intelligence-led Cyber Attack Simulation Testing (iCAST) is conducted to detect control gaps in employee behaviour, security defences, policies, and resources. Threat Intelligence Report is used as input for the Simulation Testing.	[ ] [ ]	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
4.2	**Anomalies activity detection**		
Baseline	**4.2.1 Log monitoring and analysis**		
	• Logs of physical and/or logical access are reviewed following events.	**[ ]**	
	• Access to critical systems by third parties is monitored.	**[ ]**	
	• Activities performed by privileged IDs are monitored.	**[ ]**	
	• Time synchronisation with a centralised and secure time source (such as a NTP server) should be in place for the production environment.	**[ ]**	
	• Systems or devices are in place to detect anomalous behaviour during the authentication process by the customer, employee, and third-party.	**[ ]**	
	• Based on the risk-based approach, audit log records and other security event logs are reviewed regularly and retained in a secure manner.	**[ ]**	
	• Logs provide traceability for all system access by individual users.	**[ ]**	
	• Logging practice and thresholds for security logging are reviewed periodically to ensure that appropriate log management is in place.	**[ ]**	
	4.2.2 Security information and event management		
	• A process is in place to detect anomalous activities through monitoring across the environment.	**[ ]**	
	• Thresholds have been established to determine activity within logs that would warrant management response.	**[ ]**	
	4.2.3 Customer transaction monitoring		
	• Customer transactions generating anomalous activity alerts are monitored and reviewed.	**[ ]**	
	• Online customer transactions are actively monitored for anomalous behaviour.	[ ]	

Intermediate	**4.2.1 Log monitoring and analysis** • Audit logs are backed up to a centralised log server or media to prevent unauthorised changes to the logs. **4.2.2 Security information and event management** • Tools to detect unauthorised data mining are installed. • Tools actively monitor security logs for anomalous behaviour and alert within established parameters. • Processes are in place to monitor potential and unusual insider activities that could lead to data theft or destruction. **4.2.3 Customer transaction monitoring** • An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	
Advanced	**4.2.2 Security information and event management** • Anomalous activities and other network and system alerts are correlated across business units to detect and prevent multi-faceted attacks (e.g., simultaneous account takeover and DDoS attack). • A system is in place to monitor and analyse employee behaviour (e.g. network use patterns, work hours, and known devices) to alert on anomalous activities. • Measures for monitoring sensitive data or files are implemented to prevent loss of sensitive data. • Technical measures apply defence-in-depth techniques for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks. **4.2.3 Customer transaction monitoring** • External transfers from customer accounts generate alerts and require review and authorisation if anomalous behaviour is detected.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
4.3	**Cyber incident detection**		
Baseline	**4.3.1 Event monitoring**		
	• Processes are in place to monitor for the presence of unauthorised users, devices, connections, and software.	**[ ]**	
	• Responsibilities for monitoring and reporting suspicious systems activities have been assigned.	**[ ]**	
	• The physical environment is monitored to detect potential unauthorised access.	**[ ]**	
	• A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	**[ ]**	
	4.3.2 Detection and alert		
	• Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert the security monitoring function and management to potential attacks.	**[ ]**	
	• Alert parameters are set for detecting cyber incidents that prompt mitigating actions.	**[ ]**	
	• System performance reports contain information that can be used as a risk indicator to detect cyber incidents.	**[ ]**	
	• Tools and processes are in place to detect, alert, and trigger the incident response programme whenever anomalous behaviors of insider activities, attack patterns or signatures are detected".	**[ ]**	

Intermediate	**4.3.1 Event monitoring** • A normal network activity baseline is established. • Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorised or unintentional transmissions of confidential data. • Security monitoring is in place for critical assets. **4.3.2 Detection and alert** • A process is in place to discover infiltration, before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems. • Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond immediately such as the security monitoring function. • Network and system alerts are correlated across business units to better detect and prevent multifaceted attacks.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	
Advanced	**4.3.2 Detection and alert** • Automated tools are installed to detect unauthorised changes to critical system files, firewalls, IPS, IDS, or other security devices. • Real-time network monitoring and detection tools are implemented. • Real-time alerts are sent to the responsible team/function or centralised security operation centre (e.g. the security monitoring or incident response function) for action. • Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters. • Incident detection processes are in place and with the capability of correlating events across the enterprise. • Sophisticated and adaptive technologies are deployed that can detect and alert the incident response team of specific tasks when threat indicators across the enterprise indicate potential external and internal threats.	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
4.4	**Threat monitoring and analysis**		
Baseline	**4.4.1 Threat analysis** • Processes are in place to monitor threat intelligence to discover emerging threats.	**[ ]**	
Intermediate	**4.4.1 Threat analysis** • The threat intelligence and analysis process is assigned to a specific group or individual. • Security processes and technology are centralised and coordinated in a Security Operations Centre (SOC) or equivalent. • Monitoring systems operate continuously with adequate support for efficient incident handling.	**[ ]** **[ ]** **[ ]**	
Advanced	**4.4.1 Threat analysis** • Threat intelligence sources that address all components of the threat profile are prioritised and monitored. • Threat intelligence is analysed to develop threat summary reports including cyber risk details and specific actions. • Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritise mitigating actions in anticipation of threats. • Threat intelligence is used to update IT security architecture and IT configuration standards. • The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends	**[ ]** **[ ]** **[ ]** **[ ]** **[ ]**	

Domain 5 – Response and recovery

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
5.1	**Response planning**		
Baseline	**5.1.1 Incident response plans**		
	• A policy and process is in place to set out the procedures on how to react and respond to cyber incidents and controls for digital forensic.	**[ ]**	
	• The incident response plan is designed to prioritise cyber incidents, enabling a rapid response and data recovery.	**[ ]**	
	• Business impact analysis, business continuity, disaster recovery, crisis management plans, and data backup programmes are in place to recover operations following a cyber incident.	**[ ]**	
	• Alternative processes have been established to continue critical activity within a reasonable time period.	**[ ]**	
	5.1.2 Incident response testing		
	• Widely reported events and different scenarios, including (i) losses of both production and backup systems and sites; (ii) massive destruction or alteration of data; or (iii) data corruption of both current and backup copies, are used to improve incident detection and response.	**[ ]**	
	• Regular testing of system and data integrity and recoverability from multiple copies of data backups is conducted to verify these data are accessible and usable.	**[ ]**	
	• Business continuity and data recovery testing is conducted at least annually and involves collaboration with critical third parties.	**[ ]**	
	5.1.3 Incident Response team		
	• The incident response team includes individuals with relevant expertise and have clearly defined role and responsibilities.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**5.1.1 Incident response plans**		
	• Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called upon to assist the institution during or following an incident.	**[ ]**	
	• Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful cyberattack.	**[ ]**	
	• A direct cooperative or contractual agreement(s) is in place with an incident response organisation(s) or provider(s) to assist rapidly with mitigation efforts.	**[ ]**	
	• Lessons learned from real-life cyber incidents and attacks are used to improve the risk mitigation capabilities and the incident response plan.	**[ ]**	
	• Any changes to the processes, systems/applications or the access of the entitlements necessary for cyber incident management are reviewed by management for formal approval before implementation.	**[ ]**	
	5.1.2 Incident Response Testing		
	• Cyberattack scenarios are analysed to determine potential impact to critical business processes.	**[ ]**	
	• Resilience testing includes scenarios based on analysis and identification of realistic and highly likely new and emerging cyber threats.	**[ ]**	
	• The critical online systems and processes are tested to withstand stresses for extended periods	**[ ]**	
	• The results of cyber event exercises are used to improve the incident response plan and automated triggers.	**[ ]**	
	5.1.3 Incident Response team		
	• The incident response team coordinates and communicates with internal and external stakeholders during or following a cyberattack.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
Advanced	**5.1.1 Incident response planning**		
	• Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.	**[ ]**	
	• Multiple systems, programmes, or processes are implemented into a comprehensive cyber resilience programme to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents.	**[ ]**	
	• A process is in place to continuously improve the incident response plan which is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cyber incident.	**[ ]**	
	5.1.2 Incident response testing		
	• Resilience testing is comprehensive and coordinated across all critical business functions.	**[ ]**	
	• The institution validates that it is able to recover from cyber events similar to known sophisticated attacks at other organisations.	**[ ]**	
	• Incident response testing evaluates, from an attacker's perspective, on how its assets at critical third parties may be targeted.	**[ ]**	
	• A process is in place to correct root causes for problems discovered during cybersecurity resilience testing.	**[ ]**	
	• Cyber incident scenarios involving significant financial loss are used to stress test the cyber risk management.	**[ ]**	
	• Testing needs to be done to ensure the ability to shift business processes or functions between different processing centres or technology systems for cyber incidents without interruption to business or loss of productivity or data.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
5.2	**Incident management**		
Baseline	**5.2.1 Incident containment** • A process is in place to help contain and control cyber incidents to prevent further unauthorised access to customer information and restore operations with minimal service disruption. • Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware). **5.2.2 Mitigation, analysis and investigation** • Appropriate third parties are identified to be called upon, as needed, to provide mitigation services. • Processes are in place to ensure IT assets damaged by a cyber incident are quarantined, removed, disposed of, and/or replaced. • Processes are in place to trigger the incident response programme when an incident occurs at a third party.	**[ ]** **[ ]** **[ ]** **[ ]**	
Intermediate	**5.2.2 Mitigation, analysis and investigation** • Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident. • Processes are in place to ensure that restored IT assets are appropriately reconfigured and thoroughly tested before re-use in the operation.	**[ ]** **[ ]**	
Advanced	**5.2.3 Collaboration between incident management and threat intelligence** • If available, digital forensic records are used to support incident investigation analysis and mitigation and improve the cybersecurity measures and policies. • The incident management function collaborates effectively with the cyber threat intelligence function during an incident. • Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents.	**[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
5.3	**Escalation and reporting**		
Baseline	**5.3.1 Escalation and communication**		
	• Communication and escalation channels exist to provide employees a means for reporting cyber events in a timely manner.	**[ ]**	
	• Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorised access to or use of sensitive customer information.	**[ ]**	
	• Criteria have been established for escalating cyber incidents or vulnerabilities to the senior management based on the potential impact and criticality of the risk.	**[ ]**	
	• Regulators, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorised access to systems or a cyber incident occurs that could result in degradation of services.	**[ ]**	
	5.3.2 Incident reporting		
	• Cyber incidents are classified, logged, and tracked.	**[ ]**	
	• A process exists to contact personnel who are responsible for analysing and responding to an incident.	**[ ]**	
	• An annual report of cyber incidents or violations is prepared for the board or an appropriate board committee to review.	**[ ]**	
	• A process exists to notify potentially impacted third parties.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
Intermediate	**5.3.1 Escalation and communication** • Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their roles in incident escalation. • A communication plan is used to notify other organisations, including third parties, of incidents that may affect them or their customers. • An external communication plan is used for notifying media regarding incidents when applicable. **5.3.2 Incident reporting** • Tracked cyber incidents are correlated for trend analysis and reporting.	**[ ]** **[ ]** **[ ]** **[ ]**	
Advanced	**5.3.2 Incident reporting** • The institution has established quantitative and qualitative metrics for the cyber incident response process. • Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.	**[ ]** **[ ]**	

Domain 6 – Situational awareness

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
6.1	**Threat intelligence**		
Baseline	**6.1.1 Cyber threat collection** • The institution belongs or subscribes to a threat intelligence sharing source(s) , (for example, the HKAB's Cyber Intelligence Sharing Platform) that provides information on cyber threats, analysis of tactics, patterns, and risk mitigation recommendations. • The institution uses threat intelligence to monitor relevant cyber threats and enhance cyber risk management and control.	**[ ]** **[ ]**	
Intermediate	**6.1.1 Cyber Threat collection** • A formal cyber threat intelligence programme is implemented and includes subscription to threat feeds from external providers and internal sources. • Protocols are implemented for collecting information from industry peers and government. • A read-only, central repository of cyber threat intelligence is maintained.	**[ ]** **[ ]** **[ ]**	
Advanced	**6.1.1 Cyber Threat collection** • A cyber intelligence framework is used for gathering cyber threat intelligence. • Threat intelligence is automatically received from multiple sources in real time. • The threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels. • A threat analysis system is implemented that correlates threat data and then takes risk-based actions while alerting management.	**[ ]** **[ ]** **[ ]** **[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
6.2	**Threat intelligence sharing**		
Baseline	**<u>6.2.1 Internal sharing</u>** • A formal protocol is in place for sharing cyber threat intelligence and incident information to employees based on their specific job function. **<u>6.2.2 External collaboration</u>** • Contact information for law enforcement and the regulator(s) is maintained and updated regularly. • Intelligence about cyber threats is shared with law enforcement and regulators when required or prompted.	**[ ]** **[ ]**	
Intermediate	**<u>6.2.1 Internal sharing</u>** • Management communicate threat intelligence with business risk context and specific risk management recommendations to the business units. **<u>6.2.2 External collaboration</u>** • A formal and secure process is in place to share threat and vulnerability information with other entities. • A representative from the institution participates in law enforcement or cyber threat intelligence-sharing meetings.	**[ ]** **[ ]** **[ ]**	
Advanced	**<u>6.2.2 External collaboration</u>** • Information-sharing agreements are used as needed or required to facilitate sharing threat intelligence with other financial sector organisations or third parties. • Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums. • A process is in place to communicate and collaborate with the external parties, including communication with the public regarding cyber threats as applicable.	**[ ]** **[ ]** **[ ]**	

Domain 7 – Third party risk management (please refer to the Glossary for the definition of "third party")

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
7.1	**External connections**		
Baseline	• Policies with sufficient coverage are in place to address the external connections and network-connected third-parties, excluding government and public utilities.	**[ ]**	
	• Critical business processes that are dependent on external connections or network-connected third-parties have been identified.	**[ ]**	
	• Network and systems' data flow diagrams of external connections and network-connected third-parties are identified, documented and authorised.	**[ ]**	
	• Network and systems' data flow diagrams of external connections and network-connected third-parties are updated after change and reviewed annually.	**[ ]**	
	• Information of external connections and network-connected third-parties are treated as confidential, and manage with strict access control.	**[ ]**	
Intermediate	• The audit function assesses the management of external connections and network-connected third-parties, excluding government and public utilities, to ensure that adequate monitoring, escalation and resolution procedures are established and operating effectively.	**[ ]**	
	• Controls for primary and backup of external or third-party connections are monitored and tested on a regular basis.	**[ ]**	
	• A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow and network infrastructure of the external and third-party connections.	**[ ]**	
	• Security controls are designed and verified to detect and prevent intrusions from external or third-party connections.	**[ ]**	
Advanced	• The security implication of all the changes in external or third-party network connections is validated and documented before implementation.	**[ ]**	
	• The AI works closely with service providers to maintain and improve the security of external and third-party connections, such as end-to-end encryption for the network traffic and the use of the lease lines.	**[ ]**	

	Control principle	*Implemented?*	
		Y/N/AC/RA/NA	*Justification*
7.2	**Third party management (please refer to the Glossary for the definition of "third party")**		
Baseline	**7.2.1 Contract management**		
	• Formal contracts that address relevant security and privacy requirements are in place for third parties that are network-connected and process, store, or transmit AI's sensitive or critical data.	**[ ]**	
	• Contracts acknowledge that the third party is responsible for the security and privacy of the AI's sensitive or critical data that it stores, processes, or transmits over secure connections.	**[ ]**	
	• Contracts identify the recourse available to the institution should the third party that is network-connected and processes, stores or transmits AI's sensitive or critical data, fail to meet defined security requirements.	**[ ]**	
	• Contracts establish responsibilities for responding to security incidents.	**[ ]**	
	• Contracts specify the security requirements for the return or destruction of AI's sensitive or critical data upon contract termination.	**[ ]**	
	7.2.2 Due diligence		
	• Before contracts are signed, risk-based due diligence on cybersecurity control is performed on prospective third parties that will be network-connected and will process, store and transmit AI's sensitive or critical data.	**[ ]**	
	• A list of third-parties, that are network-connected, and process, store or transmit AI's sensitive or critical data, is maintained.	**[ ]**	

Control principle		*Implemented?*	
		Y/N/AC/RA/NA	***Justification***
Intermediate	**7.2.1 Contract management** • Responsibility for notification of cybersecurity incidents and vulnerabilities by the third parties that are network-connected, and process, store or transmit AI's sensitive or critical data is documented in contracts or service-level agreements.	**[ ]**	
Advanced	**7.2.1 Contract management** • A termination/exit strategy has been established for the third parties that are network-connected, and process, store or transmit AI's sensitive or critical data.	**[ ]**	

	Control principle	*Maturity level attained*	
		Y/RA/N/NA	***Justification***
7.3	**Ongoing monitoring on third party risk (please refer to the Glossary for the definition of "third party")**		
Baseline	• The cybersecurity assessments of third parties that are network-connected and process, store or transmit AI's sensitive or critical data are updated and reviewed regularly. • Ongoing monitoring practices include reviewing cyber resilience plans of the third parties that are network-connected and process, store or transmit AI's sensitive or critical data. • A formal programme assigns responsibility for ongoing oversight of the access of third parties that are network-connected and process, store or transmit AI's sensitive or critical data.	**[ ]** **[ ]** **[ ]**	
Intermediate	• Monitoring of third parties that are network-connected and process, store or transmit AI's sensitive or critical data, is scaled, in terms of depth and frequency, according to the risk of the third parties. • Controls are in place to identify when required third-party information needs to be obtained or analysed.	**[ ]** **[ ]**	
Advanced	• Periodic on-site assessments or review of auditor report (e.g. SSAE 16 Type II SOC 2) of third parties that are network-connected and process, store or transmit AI's sensitive or critical data, are conducted to ensure appropriate cybersecurity controls are in place on a risk based approach. • Third party employee access to AI's sensitive or critical data on both AI-hosted and third party hosted systems are tracked actively based on the principles of least privilege.	**[ ]** **[ ]**	

Maturity level attainment summary

- Please fill in the required maturity level and actual maturity attainment of each component in the below table.

Required maturity level based on inherit risk assessment	[advanced(A) / intermediate(I) / baseline(B)]

Domain/ component	Actual maturity level [A/I/B]	Required maturity attained? [Y/N]
Domain 1 – Governance		
Cyber resilience oversight		
Strategy and policies		
Cyber risk management		
Audit		
Staffing and training		
Domain 2 – Identification		
IT asset identification		
Cyber risk identification and assessment		
Domain 3 – Protection		
Infrastructure protection controls		
Access control		
Data security		
Secure coding		
Patch management		
Remediation management		

Domain/ component	Actual maturity level [A/I/B]	Required maturity attained? [Y/N]
Domain 4 – Detection		
Vulnerability detection		
Anomalies activity detection		
Cyber incident detection		
Threat monitoring and analysis		
Domain 5 – Response and recovery		
Response planning		
Incident management		
Escalation and reporting		
Domain 6 – Situational awareness		
Threat intelligence		
Threat intelligence sharing		
Domain 7 – Third party risk management		
External connections		
Third party management		
Ongoing monitoring on third party risk		

Glossary

Keywords	Keywords Origin	Definition
Corporate wireless access	Appendix A "Category 1"	A non-contact access point to provide network connectivity to the corporate network
Critical activity	Appendix A "Category 1"	An activity that its failure will cause significant disruption to the AI's operations or seriously impact the AI's services to its customers
Global remittance	Appendix A "Category 3"	A cross-border money transfer service
Key and senior personnel	Appendix A "Category 4"	Key and senior personnel refers to persons who are important in business operation or cyber security operation of the firm such as team heads supporting IT critical systems or cybersecurity infrastructure and IT administrator
Open source software(OSS)	Appendix A "Category 1"	A non-commercial software that its source code is publicly available for anyone to inspect, modify, and enhance
Person-to-person payment (P2P)	Appendix A "Category 3"	An payment approach that allows customers to transfer funds from their bank accounts or credit cards to another individual's account through the Internet or any mobile devices
Resilience testing	Appendix B5.1.2 (Intermediate) & (Advanced)	A testing of an organisational business continuity and disaster recovery plans to ensure the system to recover from expected or unexpected events with planned recovery point objective and recovery time objective
Organisational asset	Appendix B3.6.1 (Advanced)	The tangible or intangible item owned and controlled by the organisation to generate positive economic value
Physical environment	Appendix B4.3.1 (Baseline)	The business environment with access to AIs-owned electronic devices that can connect to the internal corporate network

Strong encryption	Appendix B3.1.1 (Baseline) & (Intermediate)	An encryption method with algorithms which are of well-established international standards and subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, or government agencies to increase the difficulty of illegitimate attack
Supply chain risk	Appendix B2.1.1 (Advanced)	The risk that arises from the attempt of any parties to penetrate the supply chain to gain unauthorised access to read data, alter data, or interrupt communications
Termination/exit strategy	Appendix B7.2.1 (Advanced)	An approach to maintain data ownership, confidentiality and portability after terminating the business relationship with any third party service providers
Third party	Appendix B7	Third-party that are network-connected, and process, store, or transmit AI's sensitive or critical data, excluding government and public utilities.
Total assets	Appendix A "Category 3"	The total assets value that is stated on the audited financial statement
Treasury service	Appendix A "Category 3"	The transaction or investment service that helps organisations to optimise the cash flow, maintain the liquidity and manage the risk
Trust service	Appendix A "Category 3"	The services refer to MPF, retail funds, unit trusts, exchange traded funds, real estate's investment funds, private trusts and charitable trusts
Unsupported system	Appendix B3.1.2 (Intermediate)	A system that the developer no longer issues any software patches or security updates
User-developed technologies(UDT) and end-user computing	Appendix A "Category 1"	Business application tools and software which allow business users to develop simple applications to automate their operations, perform data analysis and generate reports
Wire transfer	Appendix A "Category 3"	A transfer method of completing an electronic transfer from one party to another locally or globally