GL20

GUIDELINE ON CYBERSECURITY

Insurance Authority

Contents **Page**

1. Introduction

1.1 This Guideline is issued by the Insurance Authority ("IA") pursuant to section 133 of the Insurance Ordinance (Cap. 41) ("the Ordinance") and its principal function to regulate and supervise the insurance industry for the protection of existing and potential policy holders. It sets the minimum standard for cybersecurity that authorized insurers are expected to have in place and the general guiding principles which the IA uses in assessing the effectiveness of an insurer's cybersecurity framework.

1.2 Cyber risk is one of the most significant operational risks that insurers face, particularly with regard to the business operations they conduct digitally and on-line. Cybersecurity incidents can result in financial loss, business disruption, damage to reputation and other adverse consequences to an insurer. Accordingly, this Guideline requires authorized insurers to put in place resilient cybersecurity measures to protect their business data and the personal data of their existing or potential policyholders, and to ensure continuity of their business operations.

1.3 To evaluate whether the cybersecurity measures put in place by authorized insurers are adequate and effective, the Cyber Resilience Assessment Framework ("CRAF") enclosed at the Appendix to this Guideline, which forms part of this Guideline, provides a structured assessment framework which aims to assist insurers to assess their inherent risks and maturity level of their cybersecurity measures against a set of prescribed control principles.

2. Interpretation

2.1 In this Guideline, unless the context otherwise specifies:

(a) "captive insurers" has the meaning assigned to it under section 2(7) of the Ordinance;

(b) "critical system" in relation to an authorized insurer, means a system, the failure of which will cause significant disruption to the operations of the insurer or materially impact the insurer's service to its existing or potential policy holders;

(c) “cyber risk” refers to any risks that emanate from the transmission, storage, use or processing of data transmitted, stored and retrieved in electronic means, including technology tools and platform such as computer systems, mobile applications, the internet and telecommunications networks. It encompasses data breach and leakage, loss of data, physical damage to such data caused by cybersecurity incidents, fraud committed by misuse of and unauthorized access to data, any liability arising from data storage and transmission, and the availability, integrity, and confidentiality of such data;

(d) “cybersecurity” refers to strategies, policies, standards, practices, technology, and innovations regarding the security of an authorized insurer’s systems and operations. It may encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities;

(e) “cybersecurity incident” refers to an event that threatens the security of the system of an authorized insurer which includes leakage of data in electronic form, denial of service attack, compromise of protected information systems or data assets, malicious destruction or modification of data, abuse of information systems, massive malware infection, website defacement, and malicious scripts affecting networked systems;

(f) “marine mutual insurer” means an authorized insurer which only carries on insurance business by means of its members (being owners, charterers or operators of ships or other persons related to the shipping business) mutually insuring each other against marine related risks;

(g) “relevant incident” means a system malfunction or cybersecurity incident, which has a severe and widespread impact on an authorized insurer’s operations or materially impacts the insurer’s service to its existing or potential policy holders;

(h) “system” means any data, hardware, software, network, or other information technology (“IT”) component which is part of an IT infrastructure;

(i) "system malfunction" means a failure of any of an authorized insurer's critical systems caused by cyber risk.

2.2 Unless otherwise specified, words and expressions used in this Guideline shall have the same meanings as given to them in the Ordinance.

3. Status of this Guideline and its application

3.1 Unless otherwise directed by the IA, this Guideline (excluding CRAF in the Appendix) applies to all authorized insurers, except:

(a) captive insurers; and

(b) marine mutual insurers.

3.2 The requirements in CRAF apply to all authorized insurers in relation to the insurance business they carry on in or from Hong Kong, except:

(a) captive insurers;

(b) marine mutual insurers;

(c) Lloyd's;

(d) special purpose insurers; and

(e) insurers which have ceased insurance underwriting or accepting new insurance business in Hong Kong and are in the course of running off their insurance liabilities.

(section 1.2.1 in the CRAF).

3.3 This Guideline should be read in conjunction with the relevant provisions of the Ordinance, other relevant Ordinances, and any other rules, regulations, codes, circulars and guidelines made or issued under the Ordinance and other relevant Ordinances.

3.4 This Guideline does not have the force of law and should not be interpreted in a way that would override the provision of any law. A non-compliance with the provisions in this Guideline would not by itself render an authorized insurer liable to judicial or other proceedings. A non-compliance may, however, reflect on the IA's view of the continued fitness and properness of the directors or controllers of authorized insurers to which this Guideline applies. The IA may also take guidance from this Guideline in considering whether there has been an act or omission likely to be prejudicial to the interests of policy holders or potential policy holders (albeit the IA will always take account of the full context, facts and impact of any matter before it in this respect).

3.5 Whilst this Guideline seeks to assist authorized insurers to identify and mitigate cyber risks, it is not intended to be an exhaustive list of requirements and does not constitute professional advice. Insurers are expected to implement adequate and effective cybersecurity measures which are appropriate and commensurate with the size, nature and complexity of their business. Insurers should seek professional advice if they have any questions relating to cybersecurity and any matters arising from this Guideline.

4. Overview of CRAF

4.1 CRAF are prescriptive guidelines on risk assessment and control principles to assist authorized insurers in implementing their cybersecurity framework effectively. It is a structured assessment framework for authorized insurers to evaluate their inherent risk and maturity level of their cybersecurity measures against a set of prescribed control principles. By adopting CRAF, insurers can better understand, assess, strengthen, and continuously improve their cyber resilience.

4.2 CRAF comprises the following main elements:

(i) Inherent risk assessment: authorized insurers to which CRAF applies, assess the inherent cyber risk exposure of their organizations using a set of risk indicators to determine the overall inherent risk rating of their respective organizations;

(ii) Cybersecurity maturity assessment: authorized insurers to which CRAF applies, assess according to the cybersecurity maturity level they are expected to achieve based on their overall inherent risk rating, and compare the cybersecurity maturity level expected of them against their actual cybersecurity maturity based on a set of prescribed control principles; and

(iii) protocol on submission to the IA of assessment results and improvement/remedial plan where authorized insurers' actual cybersecurity maturity level falls short of the level expected of them.

Please refer to the details of CRAF at the Appendix.

5. Cybersecurity strategy and framework

5.1 Authorized insurers should establish and maintain a cybersecurity strategy and framework tailored to mitigate relevant cyber risks that are commensurate with the nature, size and complexity of their business. The cybersecurity strategy and framework should be endorsed by the Board of the insurer.

5.2 Insurers, when establishing the cybersecurity strategy and framework, may make reference to or benchmark with the technology as well as the best available and practicable quality assurance standards, taking into account of their business nature, size, complexity and risk profile. Examples of such standards may include ISO/IEC 27001, ISACA (COBIT), Cyber Security Self-Assessment Guidance issued by the Office of the Superintendent of Financial Institutions, and Framework for Improving Critical Infrastructure Cybersecurity issued by National Institute of Standards and Technology of the U.S.

5.3 The cybersecurity framework should clearly define the insurer's cybersecurity objectives, as well as the requirements for competency of relevant personnel or system users. It should include well-defined processes and technology necessary for managing cyber risks and timely communication of the strategy with all users.

5.4 Insurers should review and update regularly their cybersecurity strategy to ensure that the strategy remains relevant when there is significant change in their mode of business operation or in the external business environment (including external cyber risk landscape). For example, a review should be undertaken at least on an annual basis, upon the occurrence of cyber incidents to the insurer or major external cyber events which potentially could impact the insurer, or upon the deployment of new systems or major systems changes.

6. Governance

6.1 The board of directors of an authorized insurer (the "Board") should hold the overall responsibility for cybersecurity controls and ensure accountability within the insurer by articulating clear responsibilities and lines of reporting and escalation for cybersecurity controls. It should cultivate a strong level of awareness of and commitment to cybersecurity.

6.2 The Board should establish a defined risk appetite and tolerance limit on cyber risks for the insurer and oversee the design, implementation and effectiveness of related cybersecurity programs. It may establish a designated management team to oversee and implement cybersecurity measures and controls. The designated management team should consist of members with the appropriate skills and knowledge to understand and manage cyber risks. Where the Board establishes a designated management team, the Board and the designated management team are responsible for overseeing the design, implementation and assessment of the effectiveness the insurer's cybersecurity strategy and framework and for ensuring these are continuously kept up to date.

7. Risk identification, assessment and control

7.1 Insurers should identify cyber risks and conduct assessment on the effectiveness of the mitigating measures to protect against and manage cyber risks within the risk appetite and tolerance limit set by the Board or its designated management team. A self-assessment tool for the overall cyber risk management program should be put in place, as part of an enterprise risk management program, which should encompass:

(i) identifying business functions, activities, products and services and maintaining a current inventory or mapping of its information assets and system configurations, including interconnections and dependencies with other internal and external systems; and prioritizing their relative importance;

(ii) evaluating inherent cyber risks presented by users, process and technology and underlying data that support each identified function, activity, product and service;

(iii) conducting business impact analysis for cyber risk, i.e. a determination of risks and prioritization of risk responses through identification of threats, vulnerabilities, likelihood and impacts.

7.2 Insurers should regularly review and assess if changes to cyber risk mitigation processes are necessary when significant changes to organizational and operational structure and systems take place. For example, the review should be on an annual basis or upon major deployment of systems.

8. Continuous monitoring

8.1 Insurers should establish systematic monitoring processes for early detection of cybersecurity incidents; regularly evaluate the effectiveness of internal control procedures; and update the risk appetite and tolerance limit as appropriate.

8.2 There should be effective monitoring measures including, among others, network monitoring, testing, internal audit and external audit.

8.3 As part of the monitoring process, insurers should manage the identities and credentials for physical and remote access to information assets. They should recognize signs of a potential cyber risk, or monitor if an actual breach has taken place in their systems.

8.4 Insurers should test all elements of their cybersecurity framework to determine their overall effectiveness at least on an annual basis. Insurers can use one or a combination of the latest available methodologies and practices, for example vulnerability assessment, scenario-based testing and penetration test.

9. Response and recovery

9.1 Insurers should develop a cybersecurity incident response plan, which covers scenarios of cybersecurity incidents and corresponding contingency strategies to maintain and restore critical functions and essential activities in such scenarios. This should also include criteria for the escalation of the response and recovery activities to the Board or its designated management team.

9.2 In case of a cybersecurity incident, insurers should assess the nature, scope and impact of the incident and take all immediate practicable steps to contain the incident and mitigate its impact.

9.3 Insurers should notify internal stakeholders, and where applicable, external stakeholders and consider joint incident response actions, if necessary. In this regard, insurers should perform incident response drill at least on a yearly basis.

9.4 Upon the detection of a relevant incident, the insurer should report the incident with the related information to the IA as soon as practicable, and in any event no later than 72 hours from detection.

9.5 Once stable operations are resumed, insurers should identify and mitigate all vulnerabilities that were exploited, and remediate the identified vulnerabilities to prevent similar incidents as part of their recovery process from the relevant incident.

10. Information sharing and training

10.1 Insurers should establish a process to gather and analyse relevant cyber risk information and participate in information sharing groups, e.g. information sharing intelligence platform, for timely information sharing to allow spontaneous and appropriate precautionary measures to be taken in combating cyber-attacks and other forms of cyber risks, both locally and internationally.

10.2 Cyber risks and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. Insurers should arrange adequate training for all system users on the subject of cybersecurity awareness and the latest developments in cybersecurity, taking into account the type and level of cyber risks they may face. Insurers are encouraged to promote the professional competence and capacity of their staff, especially those responsible for cybersecurity and systems.

11. Implementation

11.1 This Guideline shall take effect from 1 January 2025.

December 2024

Appendix

Cyber Resilience Assessment Framework

Contents **Page**

Chapter 1: Overview

1.1. Introduction

1.1.1 This Cyber Resilience Assessment Framework ("CRAF") forms part of the Guideline on Cybersecurity (GL20) ("GL20"). CRAF is a structured assessment framework under which authorized insurers can evaluate their inherent risks and maturity levels of their cyber resilience using a set of risk indicators, control principles and calculation methodologies.

1.1.2 CRAF consists of four parts. The first part sets out its applicability to insurers and the assessment approach under CRAF. The second and third parts explain how the assessments on an insurer's overall inherent risks and cybersecurity maturity level are conducted. The fourth part sets out the protocol on submission to the Insurance Authority ("IA") of assessment results and improvement/remedial plan where insurers' actual cybersecurity maturity level falls short of the level expected of them.

1.1.3 Unless otherwise specified, words and expressions used in this Appendix to GL20 shall have the same meaning given to them in GL20 and the Glossary of Key Terms and Abbreviations in this Appendix.

1.2. Assessment Approach

1.2.1 Application

CRAF applies to all authorized insurers in relation to the insurance business they carry on in or from Hong Kong, with the exception of Lloyd's, captive insurers, special purpose insurers, marine mutual insurers (as defined in GL20), and insurers which have ceased insurance underwriting or accepting new insurance business in Hong Kong and are in the course of running off their insurance liabilities.

1.2.2 Scope of CRAF

CRAF should cover all systems, infrastructure (both on-premises and cloud infrastructure), processes, and individuals supporting an authorized insurer's Hong Kong insurance business.

Under CRAF, an insurer's overall inherent risk assessment and cybersecurity maturity assessment should be conducted in accordance with the qualitative or quantitative assessment criteria set out in Annex A to this Appendix and the list of control principles set out in Annex B to this Appendix respectively.

1.2.3 Frequency

Both the inherent risk assessment and cybersecurity maturity assessment should be conducted at least every three years. Authorized insurers may conduct the assessments more frequently (e.g. annually) or upon any major changes to their business nature or technologies.

An insurer should also, upon the IA's request, conduct assessment on an ad hoc basis when the IA considers it appropriate.

1.2.4 Assessor and Validator Qualifications

Authorized insurers should engage competent persons who have the appropriate qualifications and experience to objectively conduct the assessments in accordance with CRAF and to evaluate the robustness of the insurers' controls and their effectiveness in minimising cyber risk.

Both the inherent risk assessment and cybersecurity maturity assessment may be conducted by internal staff of the insurer or external consultant appointed by an insurer ("Assessor"). Should the insurer decide to engage its internal staff to conduct the assessment as the Assessor, such internal staff may be member of the insurer's information technology / cybersecurity teams, risk management team, internal audit team or other relevant internal party ("Internal Staff"). Unless otherwise specified below, the Assessor does not have to possess any of the prescribed qualifications in Annex C. Depending on the circumstances as described below, validation may be required to confirm the result of the assessments by an external consultant appointed by the insurer ("Validator") who must possess at least one of the prescribed qualifications listed in Annex C. For the purpose of performing the independent validation for the assessment, the Validator must not be an employee of the insurer or a body corporate that belongs to the same group of companies of the insurer.

Inherent risk assessment

The inherent risk assessment should be conducted in accordance with the Inherent Risk Assessment Matrix in Annex A.

If the inherent risk rating is determined to be low, then the insurer may proceed to conduct the cybersecurity maturity assessment.

If the inherent risk rating is determined to be medium or high and the assessment is conducted by an Assessor who does not possess any of the prescribed qualifications in Annex C, then the inherent risk assessment should be re-performed by another Assessor who must possess at least one of the prescribed qualifications listed in Annex C. If the inherent risk assessment is performed or re-performed by an Internal Staff as an Assessor, then the result of the inherent risk assessment must also be independently validated by a Validator.

Cybersecurity maturity assessment

Once its inherent risk rating is determined (and validated, if necessary), the insurer should proceed to conduct the cybersecurity maturity assessment in accordance with the Cybersecurity Maturity Assessment Matrix in Annex B.

For an insurer with a low inherent risk rating, cybersecurity maturity assessment may be conducted by an Assessor who can either be the insurer's Internal Staff or an external consultant appointed by the insurer.

For an insurer with a medium or high inherent risk rating, the cybersecurity maturity assessment must be conducted by an Assessor who possess at least one of the prescribed qualifications listed in Annex C. If the assessment is performed by an Internal Staff as the Assessor, the results of cybersecurity maturity assessment must also be independently validated by a Validator.

An insurer should, upon the IA's request, engage an external consultant to re-perform or validate independently all aspects or any part of the performance or results of its inherent risk assessment and/or the cybersecurity maturity assessment.

1.2.5 Sampling

Assessors are required to perform both design effectiveness review and operating effectiveness testing of an authorized insurer's cybersecurity controls. Taking into consideration of the time needed for insurers to implement cybersecurity controls, sample-based testing of controls should cover samples taken from at least the preceding 6 months if the cyber resilience assessment is to be conducted for the first time, and samples from at least the preceding 12 months for any subsequent assessments.

The samples to be reviewed, sampling size and sampling approach used for the cyber resilience assessment should be determined by the Assessor with respect to the assessment. It is recommended that a risk-based approach be taken. The samples should be reasonably representative and prudent to reflect the control implementation status of relevant systems and infrastructure (e.g. different types and layers of technologies used by the insurer) being assessed and commensurate to the nature, scale and complexity of the insurer and the risk it faces. In general, risk-based sampling approach should take into consideration of the control frequency or instances occurred when determining the sample size, and critical applications should be prioritised for sampling.

1.2.6 Submission Protocol

Authorized insurers should submit to the IA the results of the assessments containing the information stated in paragraphs (i) to (iv) below within 12 months (for insurers with a high inherent risk rating) and 18 months (for insurers with a low or medium inherent risk rating) from the effective date of this CRAF. Following the first submission, insurers should submit the results of the assessments every three years thereafter.

(i) inherent risk assessment results, including the insurer's overall inherent risk rating and the risk ratings for each individual indicator in the form of a template prescribed by the IA, together with relevant documents and information in support of the ratings;

(ii) cybersecurity maturity assessment results, including the insurer's overall cybersecurity maturity level and the cybersecurity maturity levels for each individual control principle applicable to the insurer in the form of a template prescribed by the IA, together with relevant documents and information in support of the results. Insurers should also state all the gaps in control principles identified with an improvement/remedial plan containing clear action points and target completion date for each action point. Unless otherwise justified, all improvement/remediation action points should be completed in a timely manner and no later than the next cybersecurity maturity assessment (typically performed every three years);

(iii) for insurers with medium or high inherent risk rating, the identified gaps of control principles, if any, from the Threat Intelligence Based Attack Simulation ("TIBAS") exercise with descriptions of findings and finding risk ratings. Please refer to section 5.5 of Domain 5 in Annex B for the details of TIBAS requirements; and

(iv) any other information in relation to the assessments reasonably requested by the IA.

The results of the assessments including completed assessment templates prescribed by the IA should be reviewed and signed off by the Chief Executive or Senior Executive of the insurer, such as key persons in control function of the insurer (e.g. internal audit, compliance or risk management), as well as the Assessor(s) and/or Validator(s) responsible for conducting the inherent risk assessment and cybersecurity maturity assessment.

Chapter 2: Inherent Risk Rating Assessment

2.1. Inherent Risk Profile

The Inherent Risk Assessment Matrix in Annex A is used to evaluate an authorized insurer's inherent risk profile which represents the insurer's cyber risk exposure based on its nature of business, company size, transaction volumes, and cyber attack history.

An insurer's inherent risk represents the level of cyber risk it is exposed to in the absence of any cybersecurity controls, while residual risk is the level of cyber risk that remains after appropriate cybersecurity controls have been put in place.

2.2. Inherent Risk Rating

Under CRAF, a three-tier approach is adopted to assess an authorized insurer's inherent risk rating for each indicator, i.e. High, Medium, Low, or Not Applicable (if an indicator does not apply), based on the qualitative or quantitative assessment criteria set out in the Inherent Risk Assessment Matrix.

The insurer's inherent risk rating is determined based on the totality of its ratings for all the indicators. Under the three-tier approach, an insurer's overall inherent risk rating is classified into three levels:

(i) High risk - An insurer with a "High" inherent risk rating adopts technologies extensively to offer a vast variety of products and services. It takes advantage of technologies over multiple delivery channels, such as websites, mobile applications, social media and direct connections with third parties. The insurer may engage external vendors to host some or the majority of its critical systems or applications. The insurer uses multiple connections consisting of multiple networks or communication protocols to exchange data with its stakeholders, such as customers and service providers. The insurer is typically a large corporation employing a large number of staff and/or intermediaries, leading to a large attack surface with numerous cyber attack attempts being reported throughout the year.

(ii) Medium risk - An insurer with a "Medium" inherent risk rating generally adopts some new technologies that are fairly complex. Most of the critical systems and applications are hosted internally, although outsourcing arrangements of selected systems and applications may still be in place. A wide range of products and services are offered through multiple delivery channels, such as websites, mobile applications, and social media. The insurer is typically a medium size corporation that has a moderate business presence with some cyber attack attempts being reported throughout the year.

(iii) Low risk - An insurer with a "Low" inherent risk rating only adopts a few emerging technologies and has limited Internet and mobile channels to deliver its products and services. It has a closed operating environment with few external connections, and its portfolio consists of only a few products and services. The systems and applications used would be for basic functions only and complex customer experiences would not be offered online. The insurer is typically a company with a small team size which has a limited attack surface with a few or no cyber attack attempts being reported.

2.2.1 Categories of Risk Indicators

Under CRAF, the inherent risk profile comprises of the following 5 categories of risk indicators which are sufficiently broad taking into account various business and operational aspects of the authorized insurers. The 5 categories of risk indicators are:

(i) Technologies and connection types – Different types of connections and technologies can present various levels of inherent risk to insurers, depending on the complexity, maturity, and characteristics of the information technology ("IT") infrastructure and underlying systems. There are multiple factors to be considered under this category, including network exposure, confidential data exposure and high risk components.

Key indicators for this category include the number of Internet service providers ("ISPs") and third-party connections; the use of wireless networks; the number of network and Bring-Your-Own-Device ("BYOD") devices; third parties system access; the number of systems with sensitive information; the number of end-of-life ("EOL") systems and the extent of cloud computing being used.

(ii) Delivery channels – The use of various delivery channels, most commonly websites, mobile applications and social media, affect the inherent risk level of an insurer. The number of customers onboarded through these delivery channels, and the types of services provided through them also determine the insurer's cyber risk exposure. In addition, adoption of other innovative channels such as the metaverse, kiosk, and Internet of Things devices will also increase the insurer inherent risk level.

(iii) Products and technology services – The types of products and technology services offered by an insurer may pose different levels of inherent risk, depending on the nature of the products and services, as well as the transaction volume. This category of risk indicators aims to quantify the risk of online business processing, as well as the use of new technologies, such as blockchain, artificial intelligence, smart contract, machine learning, robotic process automation, etc. by the insurer.

(iv) Organizational characteristics – This category considers the characteristics and size of an insurer, such as the number of insurance policies and their respective value; the total amount of premium received; the number of employees, individual agents and intermediaries of the insurer. Their insurer's three lines of defence and third-party support are also considered under this category.

(v) External threats – Past track records of cyber attacks (attempted or successful) can also indicate the risk level of an insurer. This category takes into account the number of attempted cyber attacks and breaches, various types of attacks (e.g., phishing, social engineering, Denial of Service ("DoS"/"DDoS"), malware, structured query language ("SQL") injection, Cross Site Scripting ("XSS"), and Cross Site Request Forgery ("CSRF")) reported.

2.3. Inherent Risk Rating Scoring

An authorized insurer should apply the assessment criteria and descriptions of risk levels stated in the Inherent Risk Assessment Matrix at Annex A to determine its inherent risk rating (i.e. High, Medium and Low) for each of the indicators of all the 5 categories. For example:

Indicator	Assessment criteria	Description of Risk Level		
		Low	Medium	High
Cyber attacks impacting the insurer's Hong Kong insurance business for the last 12 months	Types of attacks - Phishing - Social engineering	No phishing attack	Phishing emails targeting employees or customers at the insurer or third parties supporting critical activities were received	Spear phishing emails targeting specific (e.g. high net worth) customers, specific employees at the insurer or specific third parties supporting critical activities were received

In a case where more than one description of risk level applies to the insurer, the highest risk level should be selected. Taking the above as an example. If an insurer has received both phishing emails (i.e. medium risk) and spear phishing emails targeting specific employees (i.e. high risk), the insurer's risk rating for this aspect of the indicator should be "High".

If an indicator has more than one assessment criteria, risk rating should be determined for each assessment criteria. For example, there are a total of 6 assessment criteria under the indicator (cyber attacks impacting on the insurer's Hong Kong insurance business for the last 12 months). Risk rating should be determined for each of the 6 assessment criteria.

The insurer's overall inherent risk rating will be determined according to the largest number of risk levels of all the indicators subject to the following principles:

Principle 1 – applicable if the largest number of risk indicators is "Low" only

If the largest number of risk indicators is "Low" upon performing the assessment, the number of "Low" risk indicators should be compared with the aggregate of the "Medium" and "High" risk indicators with the following rules apply:

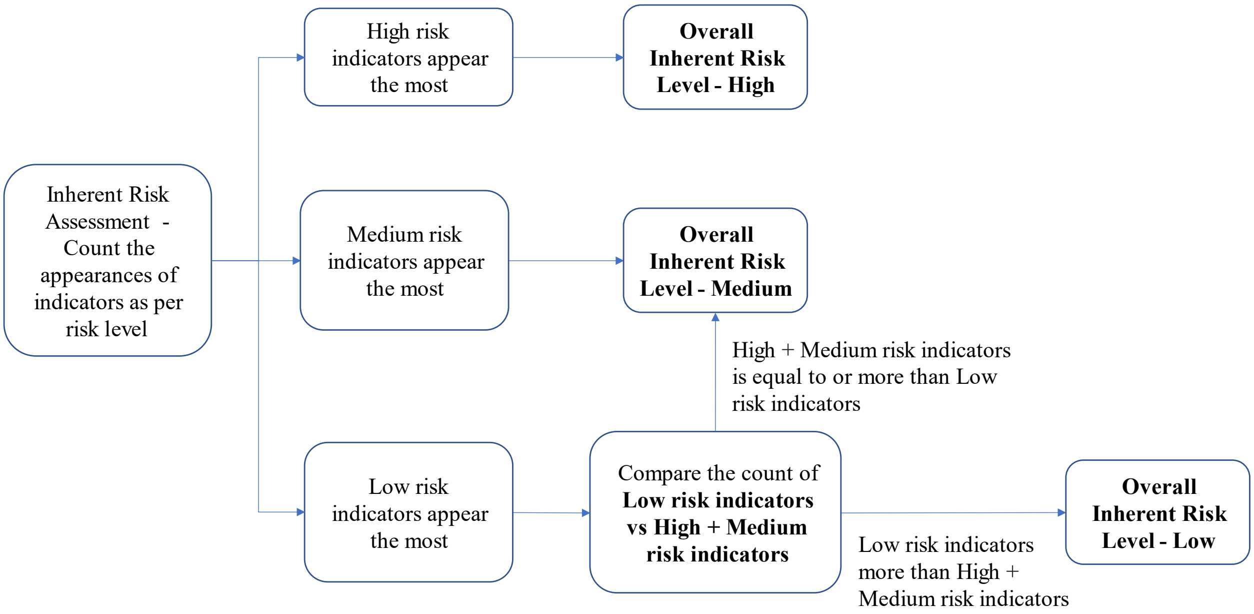
(a) If the number of "Low" risk indicators is equal to or less than the aggregate of "Medium" and "High" risk indicators, the insurer's overall inherent risk rating should be "Medium"; and

(b) If the number of "Low" risk indicators is more than the aggregate of "Medium" and "High" risk indicators, the insurer's overall inherent risk rating should be "Low".

Flowcharts A, 1 and 2 and Examples 1 and 2 below illustrate the above method of calculation.

Flowchart A

Flowchart A illustrates how an insurer's overall inherent risk level is determined under different scenarios.



Inherent Risk Assessment - Count the appearances of indicators as per risk level
High risk indicators appear the most
Overall Inherent Risk Level - High
Medium risk indicators appear the most
Overall Inherent Risk Level - Medium
High + Medium risk indicators is equal to or more than Low risk indicators
Low risk indicators appear the most
Compare the count of Low risk indicators vs High + Medium risk indicators
Low risk indicators more than High + Medium risk indicators
Overall Inherent Risk Level - Low

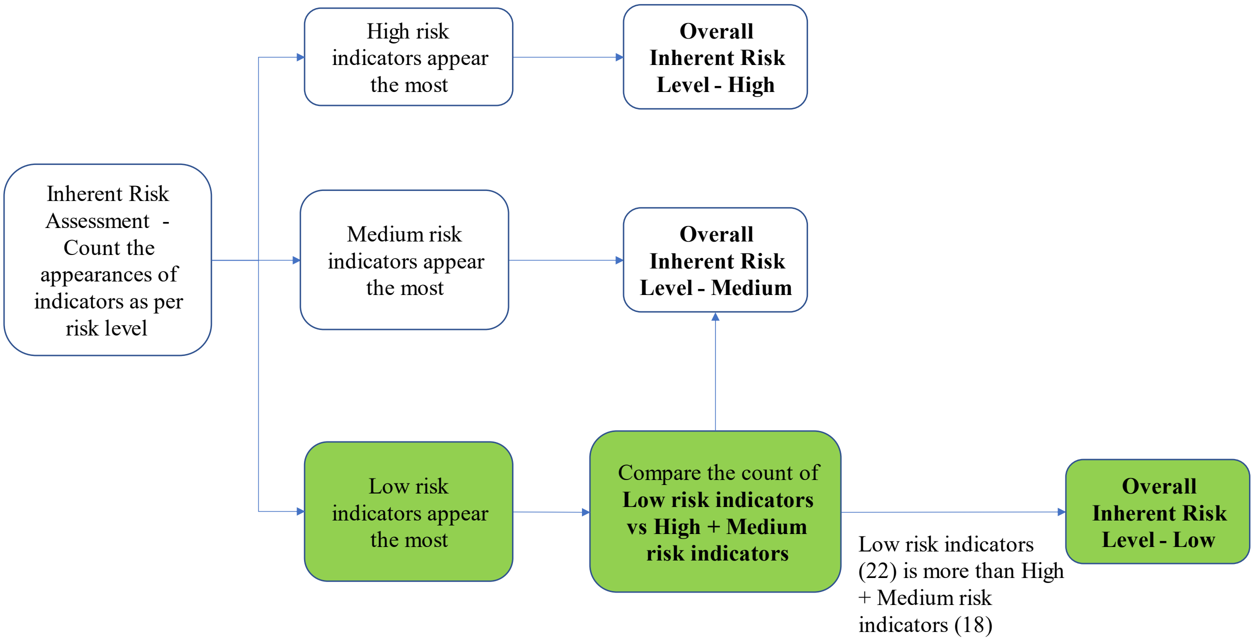
Example 1

An insurer has the following indicator risk ratings distribution:

Low	Medium	High
22 indicators	9 indicators	9 indicators

As the total number of "Low" risk indicators (22) are more than aggregate of "Medium" and "High" risk indicators (18), the insurer's overall inherent risk is "Low". This is illustrated in Flowchart 1 below.

Flowchart 1


Inherent Risk Assessment - Count the appearances of indicators as per risk level
High risk indicators appear the most
Overall Inherent Risk Level - High
Medium risk indicators appear the most
Overall Inherent Risk Level - Medium
Low risk indicators appear the most
Compare the count of Low risk indicators vs High + Medium risk indicators
Low risk indicators (22) is more than High + Medium risk indicators (18)
Overall Inherent Risk Level - Low

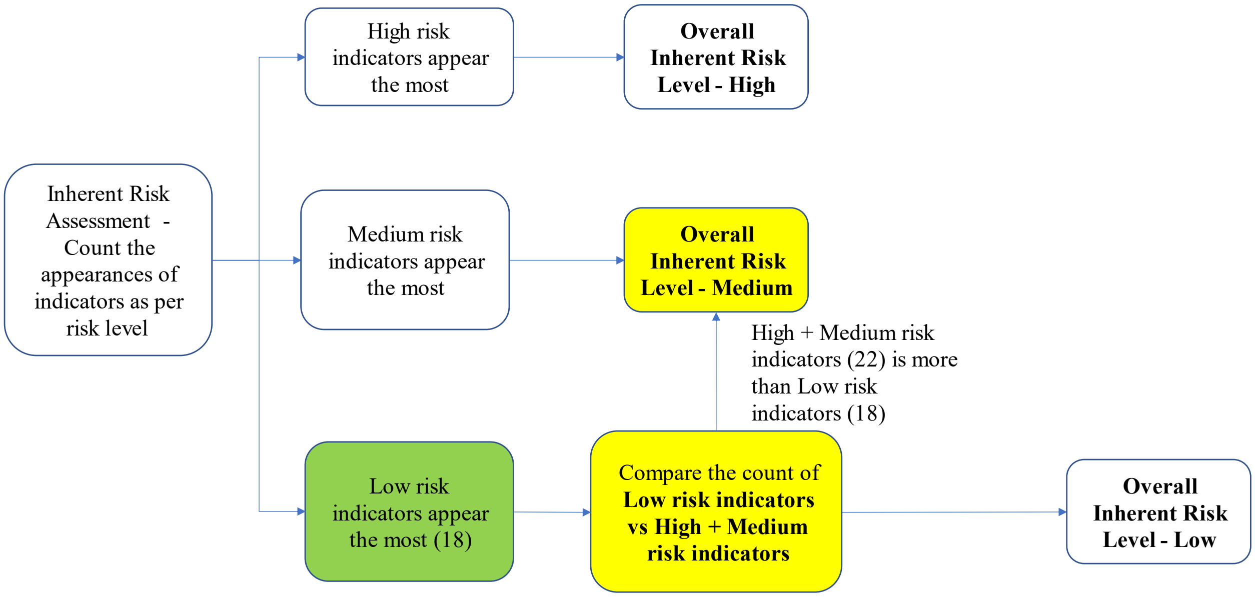
Example 2

An insurer has the following indicator risk ratings distribution:

Low	Medium	High
18 indicators	11 indicators	11 indicators

As the total number of "Low" risk indicators (18) are less than the aggregate of "Medium" and "High" risk indicators (22), the insurer's overall inherent risk rating is "Medium". This is illustrated in Flowchart 2 below.

Flowchart 2



Inherent Risk Assessment - Count the appearances of indicators as per risk level
High risk indicators appear the most
Overall Inherent Risk Level - High
Medium risk indicators appear the most
Overall Inherent Risk Level - Medium
High + Medium risk indicators (22) is more than Low risk indicators (18)
Low risk indicators appear the most (18)
Compare the count of Low risk indicators vs High + Medium risk indicators
Overall Inherent Risk Level - Low

Principle 2 – applicable if more than one risk rating having the highest number

Where the numbers of indicators of different risk levels are equal to the other, the following rules should apply:

(a) Subject to (b) and (c) below, where the numbers are equal, the higher risk indicator should be selected:

(i) If the number of "Medium" risk indicators is same as the number of "High" risk indicators, the overall inherent risk rating should be "High" (please refer to Example 3 and Flowchart 3 below);

(ii) If the number of "Low" risk indicators is the same as the number of "Medium" risk indicators, the overall inherent risk level should be "Medium";

(b) If the number of "Low" risk indicators is same as the number of "High" risk indicators, the overall inherent risk rating should be "Medium" (please refer to Example 4 and Flowchart 4 below); and

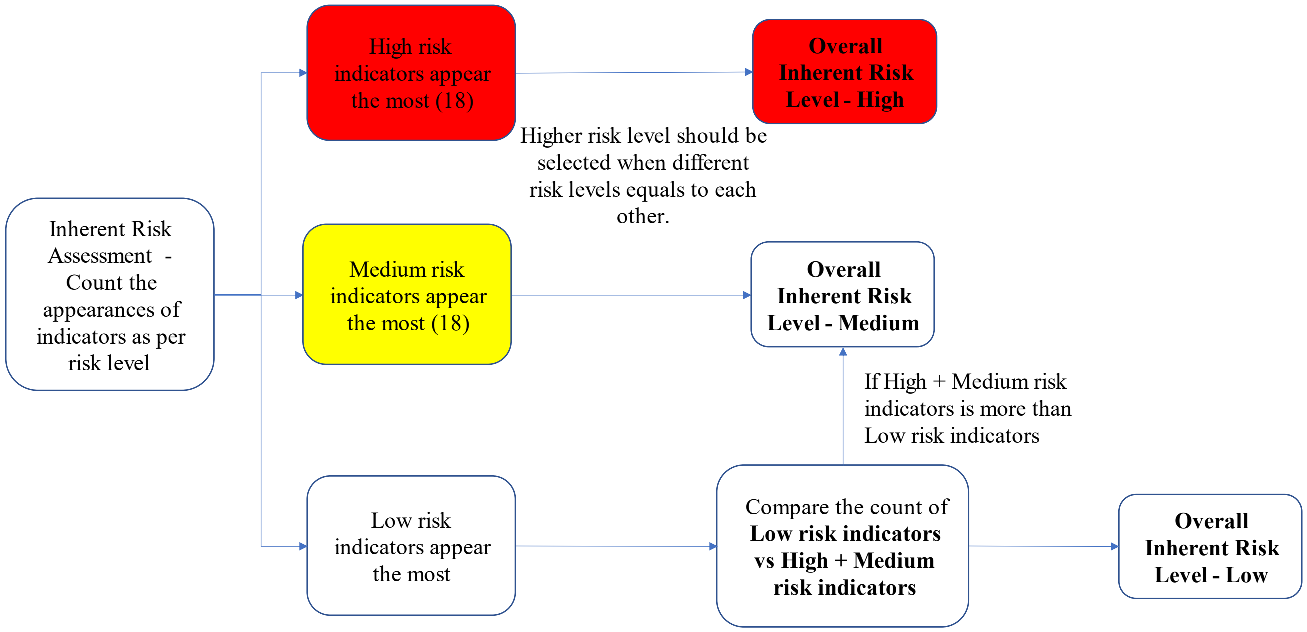
(c) If the number of "Low" risk, "Medium" risk and "High" risk indicators are the same, the overall inherent risk rating should be "Medium".

Example 3

An insurer has the following indicator risk ratings distribution:

Low	Medium	High
4 indicators	18 indicators	18 indicators

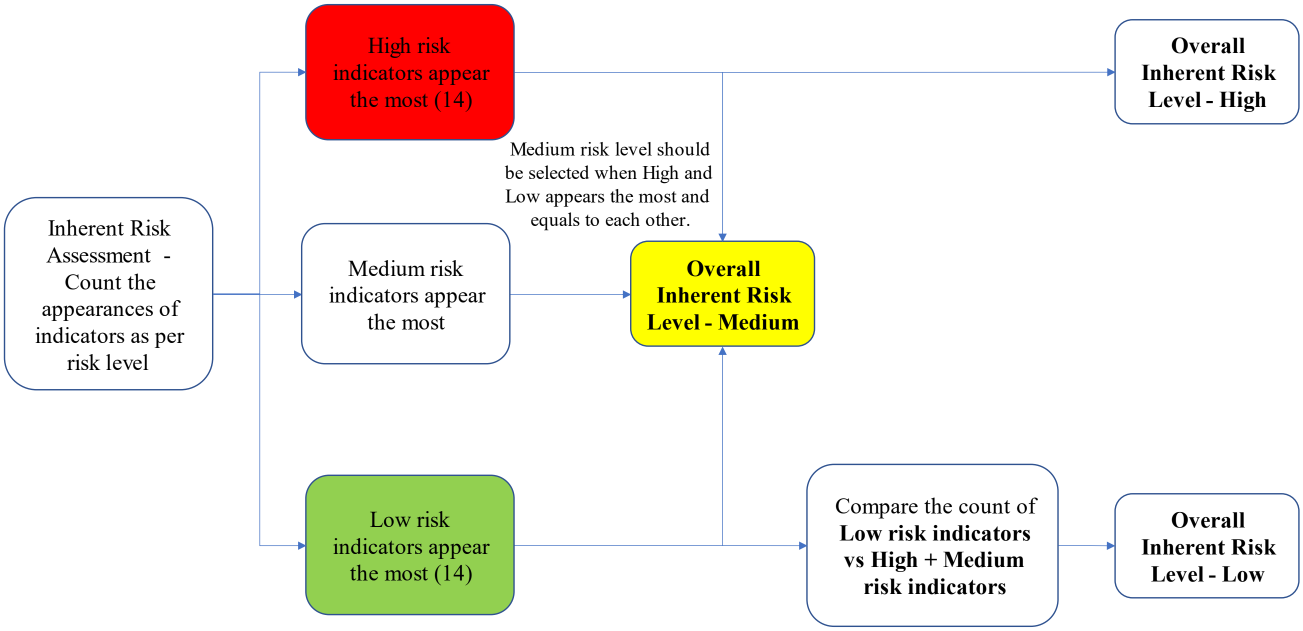
Flowchart 3


Inherent Risk Assessment - Count the appearances of indicators as per risk level
High risk indicators appear the most (18)
Medium risk indicators appear the most (18)
Low risk indicators appear the most
Overall Inherent Risk Level - High
Higher risk level should be selected when different risk levels equals to each other.
Overall Inherent Risk Level - Medium
If High + Medium risk indicators is more than Low risk indicators
Compare the count of Low risk indicators vs High + Medium risk indicators
Overall Inherent Risk Level - Low

Example 4

Low	Medium	High
14 indicators	12 indicators	14 indicators

Flowchart 4


Inherent Risk Assessment - Count the appearances of indicators as per risk level
High risk indicators appear the most (14)
Medium risk indicators appear the most
Low risk indicators appear the most (14)
Medium risk level should be selected when High and Low appears the most and equals to each other.
Overall Inherent Risk Level - Medium
Overall Inherent Risk Level - High
Compare the count of Low risk indicators vs High + Medium risk indicators
Overall Inherent Risk Level - Low

For the avoidance of doubt, any indicators which are considered not applicable to the insurer should be excluded from the calculation and should not be regarded as "Low" indicators. Assigning the risk rating of "Low" to a "Not Applicable" indicator will underestimate the insurer's overall inherent risk rating.

An insurer may opt for a higher overall inherent risk rating than that which would otherwise apply to it based on an assessment conducted using the Inherent Risk Assessment Matrix at Annex A, and deploy more advanced cybersecurity control measures. Insurers which opt for an overall "High" inherent risk level are exempted from conducting the inherent risk rating assessment provided that it maintains the use of the same "High" inherent risk rating for the purpose of conducting the cybersecurity maturity assessment.

An insurer should not apply a lower overall inherent risk rating than that which would otherwise apply to it based on an assessment conducted using the Inherent Risk Assessment Matrix.

An insurer should, upon the IA's request, engage independent Assessor(s) and / or Validator(s) to conduct or validate (as the case may be) an overall inherent risk rating assessment.

Chapter 3: Cybersecurity Maturity Assessment

3.1. Cybersecurity Maturity Assessment Domains, Components and Control Principles

Authorized insurers should apply the prescribed set of control principles stated in the Cybersecurity maturity Assessment Matrix in Annex B to evaluate their actual cybersecurity controls maturity level against the prescribed control principles applicable to them.

In the said matrix, the control principles are spread across 7 domains (i.e. Governance, Identification, Protection, Detection, Response and Recovery, Situational Awareness and Third Party Risk Management). Each domain has several components and each component has a prescribed set of control principles. The control principles are what an insurer is expected to have in place. The insurer's overall inherent risk rating will determine the level of control principles (i.e. Baseline grade, Intermediate grade and Advanced grade) that it is expected to have in place. The insurer should assess its actual cybersecurity controls maturity level against the control principles applicable to it. Chapter 3.2 below explains how the assessment should be carried out.

3.2. Cybersecurity Maturity Rating

To determine an authorized insurer's cybersecurity maturity level, the following steps should be taken:

(i) Ascertain insurer's expected cybersecurity maturity level: An insurer's inherent risk rating will determine the control principles of the components that the insurer is expected to achieve. An insurer is expected to achieve 100% of the control principles applicable to it. For example, if the insurer's overall inherent risk rating is "Low", it is expected to achieve 100% of the control principles of all the components at the Baseline grade only. If an insurer's overall inherent risk rating is "High", it is expected to achieve 100% of the control principles of all the components at the Baseline, Intermediate and Advanced grades[1]. Please refer to the Tables 1 and 2 which set out the matrix

[1] Not all components have control principles across all grades. Control principles for certain components are categorized in one or two grades only. For example, no control principles of Advanced grade are applicable to components 1.3 (Cyber risk management), 2.1 (IT asset management), 4.3 (Cyber incident detection) and 7.3 (Ongoing monitoring of third-party risk), no control principles of Intermediate grade are applicable to component 7.2 (Third-party management), no control principles of

between the insurer's overall inherent risk ratings and the control principles it is expected to achieve. The control principles for each component falling into the Baseline grade, Intermediate grade and Advanced grade are set out in the Cybersecurity Maturity Assessment Matrix in Annex B.

Table 1

Insurer's Overall Inherent Risk Rating	**Control Principles of each component under different grades expected to be achieved by insurer**		
	Baseline grade	**Intermediate grade**	**Advanced grade**
Low risk	100%	N/A	N/A
Medium risk	100%	100%	N/A
High risk	100%	100%	100%

Table 2

Insurer's Overall Inherent Risk Rating	**Grade**	**Minimum Controls Principles expected to be achieved by insurer**
Low risk	Baseline grade	Baseline control principles
Medium risk	Intermediate grade	Baseline control principles and Intermediate control principles
High risk	Advanced grade	Baseline control principles, Intermediate control principles and Advanced control principles

(ii) Ascertain insurer's actual cybersecurity maturity level: The insurer should evaluate its actual cybersecurity maturity level against the cybersecurity

Baseline grade are applicable to component 3.6 (Remediation management) and no control principles of Advanced and Baseline grades are applicable to component 5.5 (TIBAS). Please refer to Annex B for details.

maturity level that is expected of it. To do this, the insurer should take the following steps:

(a) Assess the status of the insurers' actual fulfilment of the control principles applicable to it by applying the criteria table below. For example, with respect to the component of access control (see section 3.1 of Domain 3 (Protection) in Annex B), an insurer which has an overall high inherent risk rating is expected to fulfil all the 15 control principles listed in the Baseline, Intermediate and Advanced grades of the control principles. The insurer should assess each of the 15 control principles by applying the criteria in Table 3 below.

Table 3

Status of fulfilment of each control principle applicable to insurer	**Denotation**	**Criteria**
Implemented	Y	The Control Principle has been fulfilled.
Alternative Control	AC	The Control Principle has not been fulfilled but alternative measures have been effectively implemented to addresses the risk. In this case, the Assessor should provide details of the alternative controls.
Risk Accepted	RA	The Control Principle has not been fulfilled. However, after considering relevant mitigating measures and the insurer's risk appetite, the residual risk is sufficiently low and formally accepted by the management of the insurer. In this case, the Assessor should provide details of the risk-mitigating measures and the reason for accepting the residual risk which has been deemed to be sufficiently low.

Not Implemented	N	The Control Principle has not been fulfilled. In this case, the Assessor should provide details of the remediation plan and timeline.
Not Applicable	NA	The Control Principle is not applicable to the insurer and therefore cannot be evaluated. In this case, the Assessor should provide the rationale of Control Principles exclusion. Insurer should select “Not Applicable” if the assessment criteria do not apply to its situation. For example, “Not Applicable” should be selected for the question on “How third parties access systems” if the number of third parties which can access the insurer’s internal systems is deemed to be nil.

(b) Calculate the percentage of control principles for each component fulfilled by the insurer using the following formula:

$$\text{Percentage of control principles} = (Nf + Ni + Nr) / Ncp * 100\%$$

Nf: number of control principles fulfilled/implemented
Ni: number of control principles implemented by alternative control
Nr: number of control principles which the risk is accepted by the insurer
Ncp: number of control principles applicable to an insurer (for the avoidance of doubt, control principle which is “Not Applicable” is excluded from this calculation)

Table 4 below shows the method of calculation using “Access Control” at the baseline grade as an example of component applicable to an insurer.

Table 4

		Status of fulfilment of Control Principles of Access Control					Percentage of Control Principles of the component (Access Control) fulfilled by insurer under the Baseline grade Green / (Green + Yellow) x 100%
	Total number of control principles (Access Control) under the Baseline grade (see Annex B)	**Y**	**AC**	**RA**	**N**	**NA (excluded from the calculation)**	
Example 1	15	10	2	1	1	1	93% (13/14 x100%)
Example 2	15	9	1	2	3	0	80% (12/15 x 100%)
Example 3	15	10	3	1	0	1	100% (14/14 x 100%)

(c) Determine the insurer's overall cybersecurity maturity level. There are 4 different levels: Advanced, Intermediate, Baseline and Below Baseline. As stated in Table 1 above, an insurer is expected to achieve 100% of the control principles of all the components of the 7 domains applicable to the insurer. Its overall cybersecurity maturity will depend on its actual achievement of the control principles. For example:

- An insurer which has an overall "Low" inherent risk rating is expected to fulfil 100% of the control principles of the components of all the 7 domains in the Baseline grade. If it does so, its overall cybersecurity maturity level would be "Baseline level". If it does not, its overall cybersecurity maturity level would be "Below Baseline level".

- An insurer which has an overall “Medium” inherent risk rating is expected to fulfil 100% of the control principles of the components of all the 7 domains in both the Baseline and Intermediate grades. If it does so, its overall cybersecurity maturity level would be “Intermediate level”. If it can only achieve 100% of the control principles of the components of the 7 domains in the Baseline grade but less than 100% of the control principles of the components of all the 7 domains in the Intermediate grade, its overall cybersecurity maturity level would still be “Baseline level”. If it can achieve 100% of the control principles of the components of all the 7 domains in the Intermediate grade but less than 100% of the control principles of the components of all the 7 domains in the Baseline grade, its overall cybersecurity maturity level would be “Below Baseline level”. If it can neither achieve 100% of the control principles of the components of the 7 domains in the Baseline grade nor the Intermediate grade, its overall cybersecurity maturity level would be “Below Baseline level”. A summary is shown in Table 5 below.

Table 5

Fulfilment of Control Principles of the components of the 7 domains			**Overall Cybersecurity Maturity Level of insurer**
Baseline grade	**Intermediate grade**	**Advanced grade**	
100%	100%	Not applicable	Intermediate
100%	Below 100%	Not applicable	Baseline
Below 100%	100%	Not applicable	Below Baseline
Below 100%	Below 100%	Not applicable	Below Baseline

- An insurer with an overall “High” inherent risk rating is expected to fulfil 100% of the control principles of the components of all the 7 domains in the Baseline, Intermediate and Advanced grades. Table 6 below illustrates how such insurer’s overall cybersecurity maturity level should be determined.

Table 6

Fulfilment of Control Principles of the components of the 7 domains			**Overall Cybersecurity Maturity Level of insurer**
Baseline grade	**Intermediate grade**	**Advanced grade**	
100%	100%	100%	Advanced
100%	100%	Below 100%	Intermediate
100%	Below 100%	100%	Baseline
100%	Below 100%	Below 100%	Baseline
Below 100%	100%	100%	Below Baseline
Below 100%	Below 100%	100%	Below Baseline
Below 100%	100%	Below 100%	Below Baseline
Below 100%	Below 100%	Below 100%	Below Baseline

3.3. Other Cybersecurity Assessment Frameworks

Authorized insurers may wish to adopt cybersecurity assessment frameworks other than CRAF. For example, some insurers may wish to adopt the same cybersecurity assessment frameworks adopted by their headquarters or regional hubs located outside Hong Kong or those assessment frameworks they have previously adopted (for example, group-wide assessment performed based on the National Institute of Standards and Technology ("NIST") Cybersecurity Framework).

Should an insurer decide to adopt any cybersecurity assessment framework other than CRAF, the insurer should demonstrate to the IA's satisfaction that the control principles to be used in the proposed alternative framework(s) are comparable to those for assessing cybersecurity maturity level under CRAF and that all the following conditions must be met:

- Scope – The proposed cybersecurity assessment frameworks should cover the systems, infrastructure, processes, and individuals supporting the insurer's Hong Kong insurance business;

- Mapping of assessment scope – A mapping exercise should be conducted by the insurer proposing to adopt alternative cybersecurity assessment frameworks to demonstrate that the assessment scope of the proposed assessment frameworks is comparable to that of the control principles as set out in the Cybersecurity Maturity Assessment Matrix under CRAF in Annex B;

- Closing any gap – If the proposed assessment framework(s) does/do not cover certain aspects of the Cybersecurity Maturity Assessment under CRAF, or the sample size taken for Hong Kong insurance business is deemed insufficient, insurer should undertake additional assessment(s) such as increasing sample size to bridge any gaps as identified;

- Qualification – The proposed assessment frameworks must be conducted by qualified independent Assessor(s) who is/are not the insurer's Internal Staff and such Assessor(s) must possess at least one of the qualifications as listed in Annex C;

- Submission – Insurer should still present its assessment results to the IA in the format prescribed by the IA even if it adopts assessment framework(s) other than CRAF; and

- Assessment period – Assessment result(s) of any assessment framework(s) proposed to be adopted should have been completed within one year immediately preceding the date of submission to the IA. In general, the fieldwork completion date for the recent assessment(s) being proposed to be adopted can be used to determine whether the assessment falls within this one-year timeframe.

Annex A – Inherent Risk Assessment Matrix

Category 1 – Technologies and Connection Types

Indicators	Assessment criteria	Inherent Risk Level			
		Low	**Medium**	**High**	**Conclusion**
Total number of Internet service provider (“ISP”) connections connected to the corporate network	Number of connections	0 to 2	3	4 or above	[Low/ Medium/ High]
Number of unsecured external connections (i.e. connections without encryption, e.g. file transfer protocol, Telnet, rlogin) with third parties	Number of connections	0	1 to 2	3 or above	[Low/ Medium/ High]
Wireless network access	Segmentation approach	Separate wireless access networks for guest and corporate; or wireless network is not implemented	Guest and corporate wireless access networks are logically separated	Guest and corporate wireless networks are not separated	[Low/ Medium/ High]
Personal BYOD devices allowed to connect to the insurer network	Number of corporate staff who have access to corporate resources (e.g. internal network and systems,	1 to 24	25 to 75	76 or above	[Low/ Medium/ High/ Not applicable]

	including email) using non-corporate device.				
	Number of agents who have access to corporate resources (e.g. internal network and systems, including email) using non-corporate device.	1 to 99	100 to 2,500	2,501 or above	[Low/ Medium/ High/ Not applicable]
	Application type	Not allowed	E-mail access only	E-mail access and / or other application	[Low/ Medium/ High]
Integrated systems with external organisations, including Application Programming Interface (“API”) gateways	Number of external organisations whose systems are integrated with the systems of your company (including but not limited to intermediaries/ hospitals/clinics). API gateways should be included and counted as one external organisation per gateway.	0	1 to 2	3 or above	[Low/ Medium/ High]
Third parties, including the number of organisations (external or intragroup) and the number of individuals from vendors and subcontractors, with access to internal systems and/or sensitive	Number of third parties or individuals from third parties	0	1 to 10	11 or above	[Low/ Medium/ High]
	How third parties access systems	On-site, with no virtual private network used	Virtual private network over a leased line	Virtual private network over the Internet	[Low/ Medium/ High/ Not applicable]

information (e.g. customer data)					
Systems with personal information	Number of systems with personal information stored	0 to 1	2 to 7	8 or above	[Low/ Medium/ High]
Systems with personal medical information and/or statutory information related to insurance	Number of systems with personal medical information and/or statutory information related to underwritten policies (e.g. employee compensation, motor insurance etc.) stored	0 to 1	2	3 or above	[Low/ Medium/ High]
End-of-life ("EOL") systems used for critical operations	Number of EOL systems that are receiving no further support or patches from the vendor	0	1 to 3	4 or above	[Low/ Medium/ High]
Network devices (e.g. routers and firewalls; includes physical and virtual)	Number of network devices	0 to 19	20 to 150	151 or above	[Low/ Medium/ High]
Cloud computing services hosted externally to support critical activities	Use of cloud computing	None	Private cloud only	Public or hybrid (i.e. use of other type of cloud computing on top of private cloud)	[Low/ Medium/ High]

Category 2 – Delivery Channels

Indicators	Assessment criteria	Inherent Risk Level			
		Low	Medium	High	Conclusion
Internet presence	Type of Internet web-facing services	No website	Website for informational purposes only (e.g. announcements)	Website for supporting transactions (e.g. insurance policy issuance, insurance claims) or payments	[Low/ Medium/ High]
	Number of registered Internet/ web portal customers	1 to 1999	2,000 to 16,000	16,001 or above	[Low/ Medium/ High/ Not applicable]
	Number of registered Internet/ web portal insurance intermediaries	1 to 29	30 to 350	351 or above	[Low/ Medium/ High/ Not applicable]
Mobile presence	Type of services provided	No mobile application	Mobile application for informational purposes only (e.g. announcements)	Mobile application for supporting transactions (e.g. policy issuance, insurance claims) or	[Low/ Medium/ High]

				payments	
	Number of registered mobile application customers	1 to 6,999	7,000 to 40,000	40,001 or above	[Low/ Medium/ High/ Not applicable]
	Number of registered mobile application insurance intermediaries	1 to 1,499	1,500 to 5,000	5,001 or above	[Low/ Medium/ High/ Not applicable]
Social media presence	Type of services provided	No social media channel is used	Social media for informational purposes only (e.g. announcements)	Social media for supporting transactions (e.g. policy issuance, insurance claims) or payments	[Low/ Medium/ High]
Other channels used for customer service and engagement	Types of channels used for customer service and engagement other than Internet, mobile applications and social media (e.g. metaverse, kiosk, IoT devices etc.)	No other channel used	Other channels for informational purposes only (e.g. announcements)	Other channels for supporting transactions (e.g. policy issuance, insurance claims) or payments	[Low/ Medium/ High]

Category 3 – Products and Technology Services

Indicators	Assessment criteria	Inherent Risk Level			
		Low	Medium	High	Conclusion
Online business processing	Percentage of online traded policies (online traded policies vs total traded policies over 12 months)	0%	1% to 20%	21% or above	[Low/ Medium/ High]
	Percentage of online claims (online claims vs total claims over 12 months)	0%	1% to 25%	26% or above	[Low/ Medium/ High]
	Percentage of online policy amendments (online policy amendments vs total policy amendments over 12 months). Such amendments include updating contact information of the insured person.	0%	1% to 10%	11% or above	[Low/ Medium/ High]
New technology implementation	Number of new technologies used in the first time within 12 months (e.g., blockchain, artificial intelligence, smart contract, machine learning, robotic process automation etc.)	0	1	2 or above	[Low/ Medium/ High]

Category 4 – Organizational Characteristics

Indicators	Assessment criteria	Inherent Risk Level			
		Low	Medium	High	Conclusion
Number of insurance policies	Total number of in-force policies (N/A for reinsurers)	0 to 8,299	8,300 to 35,000	35,001 or above	[Low/ Medium/ High/ N/A for reinsurers]
Amount of policy value (sum insured/ insurance liability)	Total amount of sum insured/ insurance liability (for annuity) (in HKD) (N/A for general insurers)	0 to 29,999,999,999	30,000,000,000 to 140,000,000,000	140,000,000,001 or above	[Low/ Medium/ High/ N/A for general insurers]
Amount of gross premium	Total gross premium (in HKD) over the past 12 months as per the insurance return submitted to IA	0 to 399,999,999	400,000,000 to 700,000,000	700,000,001 or above	[Low/ Medium/ High]
Number of direct employees of the entire insurer supporting Hong Kong insurance business (for this purpose, the number of employees of the contractors engaged for information technology and cybersecurity are included)	Number of employees	0 to 14	15 to 50	51 or above	[Low/ Medium/ High]

Number of individual agents of the entire insurer supporting Hong Kong insurance business	Number of individual agents	0	1 to 30	31 or above	[Low/ Medium/ High]
Number of non-individual intermediary supporting Hong Kong insurance business	Number of non-individual intermediary (including broker companies and agencies)	0 to 39	40 to 150	151 or above	[Low/ Medium/ High]
Privileged access (administrators–network, database, applications, systems, etc.)	Administration staff are maintained in-house or outsourced (including those sited at headquarters)	All in-house and with limited administrators at headquarters	Some reliance on external administrators (e.g. contractors, vendors or third parties including group or headquarters)	Many or most administrators are external	[Low/ Medium/ High]
Number of cybersecurity personnel supporting the insurer's Hong Kong insurance business (including staff responsible for cybersecurity in all 3 lines of defence, including offshore or offsite via headquarters or outsourcing)	Number of staff personnel supporting cybersecurity operations, risk management, and audit	11 or above	3 to 10	2 or below	[Low/ Medium/ High]

Category 5 – External Threats

Indicators	Assessment criteria	Inherent Risk Level			
		Low	Medium	High	Conclusion
Cyber attacks impacting the insurer for its Hong Kong insurance business for the last 12 months	Number of attempted cyber attacks (including reconnaissance)	0	1 to 25	26 or above	[Low/ Medium/ High]
	Number of breaches (i.e. which bypassed all layers of defences prepared by the insurer) and caused direct or indirect loss	No breach record	1	2 or above	[Low/ Medium/ High]
	Types of attacks - Phishing - Social engineering	No phishing attack	Phishing emails targeting employees or customers at the insurer or third parties supporting critical activities were received	Spear phishing emails targeting specific (e.g. high net worth) customers, specific employees at the insurer or specific third parties supporting critical activities were received	[Low/ Medium/ High]
	Types of attacks - (Distributed) Denial of Service ("DoS"/ "DDoS")	No DoS incident	Experienced an attempted DDoS attack within the last 12 months	Experienced multiple attempted DDoS attack within the last 12 months	[Low/ Medium/ High]

	Types of attacks - Malware	No malware was detected, or malware was detected at the network firewall, mail gateway or web proxy.	Malware was detected at endpoints by an anti-virus / anti-malware tool	Malware was detected in the mission-critical application servers or infrastructure	[Low/ Medium/ High]
	Types of attacks - SQL Injection, XSS, CSRF	No SQL Injection, XSS or CSRF	SQL Injection, XSS or CSRF was attempted at non-mission-critical applications	SQL Injection, XSS or CSRF was attempted at mission-critical applications	[Low/ Medium/ High]

Annex B – Cybersecurity Maturity Assessment Matrix

Domain 1 – Governance

1.1 Cyber resilience oversight

Maturity	Control Principles
Baseline	**1.1.1 Board and Senior Management Oversight** • Designated members of management or an appropriate Board Committee are held accountable to the Board for implementing and managing cybersecurity and business continuity programmes. • Cybersecurity risks are included as agenda items in management meetings when prompted by highly visible cyber events or regulatory alerts. These updates may be presented by a senior representative with Technology Risk Management ("TRM"), Cybersecurity or Information Security function.
	1.1.2 Regular Reporting • Management provides a written report on the overall status of the cybersecurity (including cyber incidents) and business continuity programmes to the Board or an appropriate Board Committee at least annually.
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. • The Board or an appropriate Board Committee has cybersecurity expertise or engages experts to provide assistance in oversight responsibilities. • A process is in place to ensure that cyber risks that exceed the insurer's risk appetite are escalated to management or a dedicated committee. • The Board or appropriate Board Committee reviews and approves management's prioritisation and resource allocation decisions based on the results of the cyber risk assessments.
Advanced	**1.1.1 Board and Senior Management Oversight** • Management or a dedicated committee is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.

	• The Board or an appropriate Board Committee has a process to ensure that management takes appropriate actions to address changing cyber risks or any significant cyber issues.
	1.1.2 Regular Reporting • The standard Board meeting package includes reports and metrics that go beyond events and incidents and are able to address the cyber threat trends and insurer's cybersecurity posture.

1.2 Strategies and policies

Maturity	Control Principles
Baseline	**1.2.1 Strategy and programme** • A cybersecurity strategy is in place to mitigate cyber risk by integrating technology, policies, procedures, and training.
	1.2.2 Policies • Board or dedicated committee-approved policies that address cybersecurity commensurate with the insurer's cyber risk and complexity are in place. • Policies commensurate with the insurer's cyber risk and complexity are in place to address the concepts of incident response and resilience.
Intermediate	**1.2.2 Policies** • A formal process is in place to update policies regarding cybersecurity and cyber resilience practices as the insurer's inherent cyber risk profile changes.
Advanced	**1.2.1 Strategy and programme** • Management periodically reviews the cybersecurity strategy to address evolving cyber threats in light of gathered threat intelligence and changes to the inherent cyber risk profile (e.g. arising from new technologies, additional third-party risk, or new business lines).
	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.

1.3 Cyber risk management

Maturity[2]	Control Principles
Baseline	**1.3.1 Cyber risk management function** • A cybersecurity and business continuity risk management function(s) is in place. • A responsible officer is appointed to ensure the insurer's compliance with applicable data protection regulations.
	1.3.2 Risk management programme • A social media policy is in place to provide guidance to staff and prohibit posting sensitive work-related information on social media platforms.
Intermediate	**1.3.1 Cyber risk management function** • Three lines of defence are independent from each other. First line of defence (e.g. Chief Information Security Officer or other equivalent roles) and second line of defence (e.g. Head of TRM or other equivalent roles) are defined and segregated. • The cybersecurity function has a clear reporting line that does not present a conflict of interest concern.
	1.3.2 Risk management programme • Benchmarks or target performance metrics are established that show improvements or regressions in the security posture over time.

1.4 Audit

Maturity	Control Principles
Baseline	• The audit function evaluates policies, procedures, and controls for significant cyber risks and control issues using a risk-based approach associated with operations and threat intelligence collection, including cyber risks of new products, emerging technologies, and information systems.

[2] No control principles of Advanced grade are applicable to this component. As such, an insurer which has an overall "High" inherent risk rating is expected to fulfill 100% of the control principles of both Baseline and Intermediate grades of this component only.

	• An audit is performed regularly to provide the Board of Directors and Senior Management with an independent and objective opinion of the adequacy and effectiveness of the insurer’s cyber risk management, governance, and controls relative to its existing and emerging cyber risks and threats.
Intermediate	• The frequency of audits is commensurate with the criticality of and risk posed by the insurer’s assets, functions, systems, and processes.
Advanced	• A formal process is in place to update the audit function’s planning (including scoping and testing program) in response to changes in the insurer’s inherent cyber risk profile. • The audit function regularly reviews management’s cyber risk appetite statement.

1.5 Staffing and training

Maturity	Control Principles
Baseline	**1.5.1 Staffing** • Cybersecurity roles and responsibilities have been identified and defined. • Staff with cybersecurity responsibilities have the requisite qualifications to conduct the necessary tasks associated with the position.
	1.5.2 Training • Regular (at least annual) cybersecurity training and skills development is provided to cover the latest cyber trends, cyber threats, emerging issues, and cyber incident response.
Intermediate	**1.5.2 Training** • A continuing training and skill development programme for cybersecurity staff is in place. • Management ensures that adequate cybersecurity training is provided to relevant staff at a level appropriate to their job responsibilities.
Advanced	**1.5.1 Staffing** • Audits or management reviews are done to identify gaps in existing security capabilities and expertise.
	1.5.2 Training • Management ensures that role-based security training is provided to users for a defined period, such as when there are changes to privileged access rights or critical business information systems.

	• The Board and Senior Management are provided with appropriate levels of cybersecurity training by subject matter experts that addresses issues of how complex products, services, and lines of business may affect the insurer’s cyber risk. • Regular (at least annual) cybersecurity training and skill development programmes include practical exercises (e.g. social engineering, table-top, or cyber range exercises) to reinforce training objectives.

Domain 2 – Identification

2.1 IT asset management

Maturity[3]	Control Principles
Baseline	• An inventory of the insurer's IT assets, including hardware, software, data, and systems hosted internally and externally, is maintained to facilitate assessment of whether appropriate cybersecurity safeguards are in place. • Management assign accountability for maintaining an inventory of the IT assets. • The IT asset inventory and the identification of critical IT assets is reviewed at least annually to address new, relocated, re-purposed, and sunset IT assets.
Intermediate	• IT assets are prioritised for cybersecurity protection based on their data classification and business value and are at the level of granularity deemed necessary by the insurer's own assessment for tracking and reporting critical assets, regardless of whether they are new, relocated, re-purposed, or sunset IT assets. • A process is in place to proactively manage systems when they approach their end-of-life phase (e.g. replacement) to limit cybersecurity risks.

2.2 Cyber risk identification, assessment, treatment, and monitoring

Maturity	Control Principles
Baseline	**2.2.1 Identification** • A risk owner is accountable for ensuring that proper risk treatment measures are implemented and enforced. • Insurer should establish an IT asset management process, covering but not limited to IT asset deployment, monitoring and end-of-life management.
	2.2.2 Assessment • The cyber risk assessment is updated regularly to address the deployment risk of new technologies, products, services, and connections.

[3] No control principles of Advanced grade are applicable to this component. As such, an insurer which has an overall "High" inherent risk rating is expected to fulfill 100% of the control principles of both Baseline and Intermediate grades of this component only.

Intermediate	**2.2.3 Treatment** • For each type of risk identified, there are risk mitigation and control strategies consistent with the value of the information assets and the insurer's level of acceptable risk tolerance.
	2.2.4 Monitoring, Review, and Reporting • A risk register is maintained to facilitate monitoring and reporting of identified risks and regularly reviewed to evaluate the effectiveness of the controls implemented to minimise risk exposure.
Advanced	**2.2.2 Assessment** • The focus of the risk assessment has expanded beyond customer information to address all information assets (such as internal information). • The risk assessment includes consideration of the risk of using end-of-life ("EOL") software and hardware components.
	2.2.3 Treatment • A methodological approach has been adopted to evaluate, prioritise, and implement appropriate risk-reduction controls. • The criteria for acceptance are clearly defined and commensurate with the insurer's risk tolerance, with the risk acceptance formally endorsed by Senior Management. • A formal evaluation of the need for cyber or other insurance programmes to transfer institutional risk exposure has been completed.
	2.2.4 Monitoring, Review, and Reporting • Risk metrics have been developed to highlight assets with the highest risk exposure and evaluate the effectiveness of mitigating controls.

Domain 3 – Protection

3.1 Access Control

Maturity	Control Principles
Baseline	**3.1.1 User account management** • Identification and authentication are required to manage the access to systems, applications, and devices. • Access controls are in place, including minimum password length, password complexity, and limits to password attempts and reuse. • All physical and logical access is removed timely upon notification of the involuntary 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 the appropriate personnel. • User access reviews are performed periodically for all systems and applications based on the risk exposure to the application or system. • All passwords should be protected with cryptographic functions in storage and in transit. • Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. • Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. • The principle of separation of duties is in place to restrict employee access to systems and confidential data. • Customer access to internet-based products or services requires authentication controls (e.g. multi-factor authentication) that are commensurate with the risk.
	3.1.3 Physical access management • Physical security controls are used to prevent unauthorized access to IT hardware and telecommunication systems.
	3.1.4 Remote access management • Remote access by employees, contractors, and third parties uses encrypted connections and multi-factor authentication.

	3.1.5 Wireless access management • Authorization of wireless access to the information system is required before allowing a connection to access the network.
	3.1.6 Mobile access management • Authorization of the connection of mobile devices to organisational information systems is required.
	3.1.7 Cryptographic keys management • Controls are in place to prevent unauthorized access to cryptographic keys.
Intermediate	**3.1.2 Privileged user account management** • Elevated privileges (e.g. administrator privileges) are limited and tightly controlled (e.g. least privileged basis, and requiring stronger password controls). • Mechanism should be in place to audit and review the execution of privileged functions. • Multi-factor authentication (e.g. tokens, digital certificates) is used for employee access to high-risk systems as identified in the cyber risk assessment(s).
	3.1.3 Physical access management • There is ongoing monitoring of physical access alarms and surveillance equipment.
	3.1.5 Wireless access management • The information system protects wireless access to the system using authentication of users and devices, as well as encryption. • Usage restrictions, configuration/connection requirements, and implementation guidance have been established.
	3.1.6 Mobile access management • Usage restrictions, configuration requirements, connection requirements, and implementation guidance have been established.
	3.1.7 Cryptographic keys management • A cryptographic key management policy and procedures covering key generation, distribution, installation, renewal, revocation, and expiry should be established.
Advanced	**3.1.2 Privileged user account management** • Multi-factor authentication has been implemented for privileged accounts with local and / or network access.

3.2 Infrastructure protection control

Maturity	Control Principles
Baseline	**3.2.1 Network protection** • Network perimeter defense tools (e.g. border router and firewall) are used. • Based on a 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 the 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 networks. • Intrusion detection/prevention systems ("IDS"/ "IPS") are in place to detect and/or block actual and attempted attacks or intrusions. • Technical controls are in place to prevent unauthorized devices, including rogue wireless access devices, from connecting to internal networks.
	3.2.2 System configuration • Systems configurations (for servers, desktops, routers, etc.) are implemented according to industry standards and are properly enforced on an on-going basis. • System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met.
	3.2.3 Environmental controls • The insurer should implement environmental controls covering power, cooling, fire detection and suppression to protect the devices within the data centre.
Intermediate	**3.2.1 Network protection** • The firewall rules are regularly audited or verified on a risk-based approach at least annually. • A risk-based solution is in place for the Internet hosting provider, such as a smart web content delivery process, to mitigate the risk of any cyber attacks (e.g. DDoS attacks). • Guest wireless networks are fully segregated from the internal network(s) either physically or logically. (*N/A if there are no wireless networks.) • Security controls have been implemented for remote access to all administrative consoles, including restricted virtual systems.

	3.2.2 System configuration • Documented hardening standards are in place for operating systems and network devices used in the organisation, and a process to ensure all devices (in data and voice networks) are hardened in line with these standards.
Advanced	**3.2.1 Network protection** • The enterprise network is segmented in multiple, separate trust or security zones with defence-in-depth strategies (e.g. logical network segmentation, air-gapping, etc.) to mitigate the risk of cyber attacks. • Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorized 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.).

3.3 Data protection

Maturity	Control Principles
Baseline	**3.3.1 End point data security** • Controls are in place to restrict the use of removable media to authorized personnel only. • Antivirus and anti-malware tools are deployed on end-point devices that do not support sandboxing architecture (e.g. workstations, laptops, and mobile devices). • Insurer data on a mobile device can be wiped remotely when that device is reported 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 no longer needed.
	3.3.2 Data protection • Confidential data is encrypted when transmitted across public or untrusted networks (e.g. the Internet).
Intermediate	**3.3.1 End point data security** • Controls are in place to prevent unauthorized individuals from copying confidential data to removable media. • Data loss prevention controls or devices have been implemented for outbound communications.

	• Mobile device management controls are in place, including 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 insurer information, capabilities for remote software version/patch validation are in place. (*N/A if mobile devices are not used.).
	3.3.2 Data protection • Data classification and risk assessment policies include statements of the criteria for encryption of selected data at-rest and data in-transit. • Use of customer data in non-production environments (e.g. testing environment) complies with legal, regulatory, and internal policy requirements for concealing or removing sensitive data elements.
Advanced	**3.3.1 End point data security** • Data governance is in place to identify the encryption requirements and oversee the effective implementation of cryptographic functions across data at-rest and data in-transit.
	3.3.2 Data protection • Confidential data is encrypted in transit across private connections (e.g. dedicated leased lines) and within the trusted zones.

3.4 Secure development

Maturity	Control Principles
Baseline	• A framework has been established to manage the system development life cycle ("SDLC").
Intermediate	• The SDLC framework covers the processes, procedures, and controls required across several phases or activities, including planning, requirement gathering, design, implementation, and testing. • Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications. • The security of applications, including those connected to the Internet and have application programming interfaces (APIs), are tested based on a risk-based approach against known types of cyber attacks (e.g. from Open Worldwide Application Security Project ("OWASP") Top 10) before implementation, or following significant changes.

Advanced	• Based on a risk-based approach and focusing on high-risk applications, vulnerabilities identified through code reviews and/or static code analyses are conducted on internally developed or vendor-provided custom applications to ensure that there are no security gaps before deploying into production. • Strict change control and release management processes are in place that require security criteria to be met before each phase or activity of the SDLC is completed, extending to both internal systems and externally procured systems for critical functions. • Policies are in place to ensure secure coding, source code review, and application security testing standards are applied during Agile software development.

3.5 Patch and change management

Maturity	Control Principles
Baseline	**3.5.1 Patch management programme** • A patch management programme has been implemented to ensure that software and firmware patches are applied promptly.
	3.5.2 Patch assessment and testing • Patches are tested before being applied to systems and/or software.
	3.5.3 Change management process • A change management process is in place to request and approve changes to IT system configurations, hardware, software, applications, and security tools.
Intermediate	**3.5.1 Patch management programme** • Patch management reports are reviewed and reflect missing security patches across all environments. • A proper follow-up process is in place to classify actions based on priority and track actions to timely closure.
	3.5.2 Patch assessment and testing • A formal process is in place to acquire, test, and deploy software patches based on criticality.
	3.5.3 Change management process • Formal change requests, documented approvals and assessment of security implications are required for any changes to the baseline IT configurations.

	• An authorized individual or committee with appropriate knowledge, authority, and separation of duties formally approves changes.
Advanced	**3.5.3 Change management process** • Tools have been implemented to detect and block any unauthorized changes to software and hardware.

3.6 Remediation management

Maturity[4]	**Control Principles**
Intermediate	• Issues identified in cyber risk assessments are prioritised and resolved based on criticality, and within the time frames established in response to the assessment report. • Remediation efforts are confirmed by conducting a follow-up vulnerability scan, where applicable.
Advanced	• Formal processes are in place to resolve weaknesses identified during penetration/simulation testing.

[4] No control principles of Baseline grade are applicable to this component. As such, an insurer which has an overall "Low" inherent risk rating is not expected to fulfill any control principles stated herein for this component.

Domain 4 – Detection

4.1 Vulnerability detection

Maturity	Control Principles
Baseline	**4.1.1 Antivirus and anti-malware** • Antivirus and anti-malware tools used to detect attacks 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 the internal network.
Intermediate	**4.1.2 Penetration / Simulation Testing** • A combination of penetration testing and vulnerability scanning is conducted routinely on a risk-based approach to determine security gaps before deployment into production.
Advanced	**4.1.1 Antivirus and anti-malware** • Behavioural analysis is automatically conducted through implemented processes and tools for e-mails and attachments to detect for and block against malware when present.
	4.1.2 Penetration / Simulation Testing • Vulnerability scanning is rotated to scan all high-risk systems in production environment throughout the year.

4.2 Anomalies activity detection

Maturity	Control Principles
Baseline	**4.2.1 Log monitoring and analysis** • Based on a risk-based approach, audit log records and other security event logs are reviewed regularly and retained securely. • Logs are available that provide traceability for all system access by individual users.
	4.2.2 Security information and event management

	• A process is in place to detect anomalous activities through monitoring across the environment.
	4.2.3 Customer transaction monitoring • Customer transactions generating anomalous activity alerts are monitored and reviewed.
Intermediate	**4.2.1 Log monitoring and analysis** • Time synchronisation with a centralised and secure time source (such as an NTP server) is in place for the production environment. • Systems or devices are in place to detect anomalous behaviour by customers, employees, and third-parties during the authentication process.
	4.2.2 Security information and event management • Thresholds have been established to determine activity within logs that warrant management response. • Tools actively monitor security logs for anomalous behaviour (e.g. Endpoint Detection and Response ("EDR") solution) and provide alerts within established parameters.
Advanced	**4.2.1 Log monitoring and analysis** • Logging practices 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 • Measures for monitoring sensitive data or files have been implemented to prevent losses.
	4.2.3 Customer transaction monitoring • An automated tool triggers system alerts and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations.

4.3 Cyber incident detection

Maturity[5]	Control Principles
Baseline	**4.3.1 Event monitoring** • Responsibilities for monitoring and reporting suspicious systems activities have been assigned.
Intermediate	**4.3.1 Event monitoring**

[5] No control principles of Advanced grade are applicable to this component. As such, an insurer which has an overall "High" inherent risk rating is expected to fulfill 100% of the control principles of both Baseline and Intermediate grades of this component only.

	• A process is in place to correlate event information from multiple sources (e.g. networks, applications, firewalls, or endpoints). • A normal network activity baseline has been established.
	4.3.2 Detection and alert • A process is in place to discover infiltration, before an attacker can traverse across systems, establish a foothold, steal information, or cause damage to data and systems. • Resources are in place to achieve continuous detection and response (i.e. 24x7), including the detection, investigation, and root cause analysis of the sophisticated threat activity, to performing the appropriate response activities in a prompt manner.

4.4 Threat monitoring and analysis

Maturity	Control Principles
Baseline	• Processes are in place to monitor threat intelligence to identify emerging threats.
Intermediate	• The threat intelligence and analysis processes are assigned to a specific group or individual.
Advanced	• Threat intelligence sources that address 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. • The insurer uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and information about geopolitical events to predict potential future attacks and attack trends.

Domain 5 – Response and recovery

5.1 Governance and preparation of incident response and recovery

Maturity	Control Principles
Baseline	**5.1.1 Governance of incident response and recovery** • Clear accountability and responsibilities are defined to ensure that the appropriate stakeholders across the insurer are engaged should a cyber-incident occurs. • Relevant stakeholders are aware of their designated accountabilities, responsibilities, and roles in the event that the cyber incident response and recovery plans are triggered and have sufficient expertise and training to discharge the duties in the event of a crisis. • Processes are in place to describe the involvement of the insurer's functions in the cyber incident management process and define the procedures on the proper reaction and response to cyber incidents, including analysis, mitigation, restoration, digital forensics, improvement, coordination, and communication.
	5.1.2 Incident response and recovery preparation • Plans and playbooks that provide well-defined, organized approaches for Cyber Incident Respond & Recovery activities, including criteria for activating the measures, are established to expedite the insurer's response. Business impact analysis, business continuity, disaster recovery, crisis management plans, and data backup programmes are in place to recover critical activities and operations following a cyber incident and to continue critical activity in accordance with recovery objective(s) (e.g. Recovery Point Objective ("RPO"), Recovery Time Objective ("RTO")), restoration priorities and metrics. • Backup facilities are diversified geographically and isolated through network and system segmentation to avoid possible concentration risks.
Intermediate	**5.1.1 Governance of incident response and recovery** • Senior Management sponsorship is obtained, widely communicated, and their guidance readily accessible across the insurer, thereby promoting awareness and instilling the appropriate culture (e.g. staff are encouraged to report or escalate cyber incidents to management) and accountability for success.
	5.1.2 Incident response and recovery preparation

	• Plans are in place (e.g. re-route or substitute critical functions and/or services that may be affected by a successful cyber attack) for the resumption of essential missions and business functions in accordance with recovery objective(s) (e.g. RPO, RTO).
Advanced	**5.1.2 Incident response and recovery preparation** • Dependencies in supply chain (e.g. third-party service providers) are addressed and the contingency measures with relevant service providers are tested.

5.2 Analysis, mitigation, and restoration

Maturity	Control Principles
Baseline	**5.2.1 Analysis** • A process is in place to identify cyber security incidents relevant to the insurer. • A triage process is in place to classify cyber security incidents, prioritise incidents according to business impact, the type of incident, threat vectors, and repercussions, and assign incidents to relevant stakeholders in terms of their legitimacy, correctness, constituency origin, severity or impact.
	5.2.2 Mitigation • A process is in place to help contain, control, and eradicate cyber incidents, thereby preventing further unauthorized access to sensitive information (e.g. customer information) and mitigating the potential impact.
	5.2.3 Restoration and quality assurance testing • Processes are in place to validate that systems are operating as per intended and without the vulnerabilities that led to the initial compromise. • Business continuity and data recovery testing is conducted at least annually and involves collaboration with critical third parties where applicable.
Intermediate	**5.2.1 Analysis** • A severity assessment framework is established to help gauge the severity of the cyber incident. • Analysis of security incidents is performed in the early stages of an intrusion to minimise the potential impact of the incident on critical business processes.

	• Incident response and recovery objectives are in place to validate the insurer's ability to develop and execute plans to recover from known sophisticated attacks at other organisations.
	5.2.3 Restoration and quality assurance testing • Actions taken from the time the incident was detected to its final resolution are documented and timestamped. Tools and artefacts (e.g. scripts, configuration changes, etc.) used for restoration are recorded for future use or for the improvement of current process and/or systems. • Processes are in place to ensure that restored IT assets are appropriately reconfigured and thoroughly tested before re-using in operations.
Advanced	**5.2.2 Mitigation** • Separate containment strategies are developed for different types of major cyber attack, with criteria documented clearly to facilitate decision making.
	5.2.3 Restoration and quality assurance testing • All internal and external stakeholders are updated regularly and made aware of the conditions to be met, or restrictions, before resuming critical operations. • Testing exercise objectives have been developed that determine the coverage of plans to be taken, readiness to execute them, and any corrective actions. • Cyber incident escalations and resolutions are tracked and monitored, and updates are provided to the management regularly. • The insurer's critical online systems and processes are tested on their ability to withstand stresses for a reasonable period. • Resilience testing includes scenarios based on analysis and identification of realistic and highly likely new and emerging cyber threats.

5.3 Cyber forensics

Maturity	Control Principles
Baseline	**5.3.1 Process of collecting evidence** • Processes are in place to properly collect and preserve the integrity of the digital and forensic evidence prior to performing analysis.

	5.3.2 Process of investigating and analysing evidence • The digital and forensic evidence collected contains information that, at minimum, establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any user or subject associated with the event. • Root cause analyses are performed to identify the source or perpetrator of a cyber security incident.
Intermediate	**5.3.1 Process of collecting evidence** • Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.
	5.3.2 Process of investigating and analysing evidence • Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties.
	5.3.3 Protection of evidence • Controls are in place to protect digital and forensic evidence (e.g. applying the principle of least privilege, encryption, etc.) as well as forensic tools from unauthorized access, modification, and deletion (e.g. segregation of duties, role-based access controls, etc.). • Access to audit configurations and logging records are limited to authorized users.
Advanced	**5.3.3 Protection of evidence** • The information system employs cryptographic mechanisms to protect the integrity of evidence and audit tools where applicable.

5.4 Communication and improvement

Maturity	Control Principles
Baseline	**5.4.1 Escalation** • Communication and escalation channels exist that enable employees to report cyber events promptly. • Procedures are in place to notify (i) regulators and law enforcement agencies; (ii) customers; and (iii) third-party service providers as required or necessary (e.g. in cases of unauthorized access to or use of sensitive customer data, incidents that may result in the suspension or degradation of services, etc.). • Upon the detection of a relevant incident, the insurer should report the incident with the related information to the IA as soon as practicable, and in any event no later than 72 hours from detection.

	5.4.2 Incident reporting • All cyber incidents are classified, logged, and tracked.
	5.4.3 Improvement • There are continuous improvement processes in place to ensure improvement is an iterative and institution-wide process.
Intermediate	**5.4.1 Escalation** • Criteria have been established for escalating cyber incidents or vulnerabilities to Senior Management based on the potential impact and criticality of the risk.
	5.4.2 Incident reporting • Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the Board meeting package.
Advanced	**5.4.1 Escalation** • A list of internal and external stakeholders to be informed depending on identified scenarios and criteria is established. Insurers also prioritise and sequence information sharing activities with internal and external stakeholders upon incident outbreaks.
	5.4.2 Incident reporting • A process exists to regularly notify relevant internal stakeholders (e.g. Senior Management with an agreed communication frequency, relevant stakeholders with actionable measures, etc.) and external stakeholders (e.g. potentially impacted third parties).
	5.4.3 Improvement • The continuous improvement processes include proactive mechanisms such as the use of simulation testing exercises to further embed lessons learned across the insurer. • All security incidents are regularly referenced to perform trend analysis to identify common factors, determine the effectiveness of controls, and understand the costs and impacts associated with cyber security incidents and improve cybersecurity measures and policies.

5.5 Threat Intelligence Based Attack Simulation

Maturity[6]	Control Principles
Intermediate	• Insurers should use threat intelligence analysis to formulate end-to-end cyber attack testing scenarios tailored to them and the insurance sector generally, which is different and on top of performing security vulnerability and penetration testing of a single system or an isolated environment. A risk-based approach should be applied to identify the attack scenarios relevant to their organization, and ensure they are tested at least every 3 years or after significant system, technology, third-party, or business changes that could lead to material increase of the associated risks particularly the security risk and system availability of the service, to simulate real-life attacks conducted by competent adversaries. A minimum of three end-to-end cyber attack scenarios shall be covered in the simulation. • Simulation testing should be conducted in a production environment to simulate real-life attack scenarios, be representative of organisational cyber resilience characteristics and measures against real-world threats, and include an assessment of the readiness of human and process elements atop of technological components. If the potential operational impact of the simulation testing on specific components in the insurer's production environment during the exercise is considered to be unacceptable, the insurer may consider conducting the exercise on a simulated component that is a close replica of the actual production component. • Simulation testing should be conducted in several phases, including but not limited to scoping the critical functions mapped to key systems; leveraging threat intelligence to identify potential threat actors and Tactics, Techniques and Procedures that are most likely used in attacks on key systems; developing the testing scenarios according to insights gained from threat intelligence; conducting stealthy intelligence-led testing against the critical functions and target systems; and preparing relevant documents to record the outcomes of the simulation testing. • Independent threat intelligence and cyber attack simulation testing experts who have the necessary skills and expertise, as well as industry-recognised qualifications across red team and threat intelligence, should be engaged to deliver a controlled and effective cyber attack simulation testing.

[6] No control principles of Baseline grade and Advanced grade are applicable to this component. As such, an insurer which has an overall "Low" inherent risk rating is not expected to fulfill any control principles stated herein for this component. An insurer which has an overall "Medium" or "High" inherent risk rating is expected to fulfill 100% of the control principles of the Intermediate grade of this component only.

	• The attack simulation exercise should be kept secret to provide a more accurate assessment of the insurer's defence and incident response capability. Only selected groups of stakeholders should be made aware of the exercise details in order to prevent disruption to business or putting out false alarms to external parties.

Domain 6 – Situational awareness

6.1 Threat Intelligence

Maturity	Control Principles
Baseline	• The insurer subscribes to one or more a threat intelligence sharing sources that provide information on cyber threats, analysis of tactics, patterns, and risk mitigation recommendations. • The insurer uses threat intelligence to monitor relevant cyber threats and enhance its cyber risk management and control.
Intermediate	• Protocols have been implemented for collecting information from industry peers and government.
Advanced	• A centralised read-only repository of cyber threat intelligence is maintained.

6.2 Threat Intelligence sharing

Maturity	Control Principles
Baseline	• Law enforcement and regulator contact information is maintained and updated regularly. • Designated individuals have been appointed who are authorized to post information to external threat intelligence sharing sources and are trained to ensure that this does not include non-public information.
Intermediate	• A formal protocol is in place for sharing cyber threat intelligence and incident information with employees, based on their specific job functions.
Advanced	• A formal and secure process is in place to share threat and vulnerability information with other entities or via threat intelligence sharing sources, in a manner which does not violate any data privacy laws or regulations, or any internal data protection policies.

Domain 7 – Third party risk management

7.1 External connections

Maturity	Control Principles
Baseline	**7.1.1 Identify** • Policies are in place that sufficiently cover the insurer's external connections and network-connected third parties, excluding government, public utilities and financial market infrastructure. • Critical business processes that are dependent on external connections or network-connected third-parties have been identified.
Intermediate	**7.1.1 Identify** • Network and systems data flow diagrams have been created that identify all external connections and network-connected third parties, and these connections have been authorized by management. • Network and systems' data flow diagrams of external connections and network-connected third parties are updated after changes and reviewed annually.
Advanced	**7.1.2 Protect** • User outbound traffic (e.g. Internet, third party connections) is routed through predefined network choke-points (e.g. web proxy) with traffic limited to certain trusted domains (e.g. blacklisting/whitelisting). • The insurer has arrangements in place with third-party service providers that are network-connected and process, store or transmit sensitive or critical insurer data (e.g. Cloud service providers) to ensure information systems with external connections can failover safely and securely.

7.2 Third-party management

Maturity[7]	Control Principles

[7] No control principles of Intermediate grade are applicable to this component. As such, an insurer which has an overall "Low" or "Medium" inherent risk rating is expected to fulfill 100% of the control principles of Baseline grade of this component only. An insurer which has an overall "High" inherent risk rating is expected to fulfill 100% of the control principles of both Baseline and Advanced grades of this component only.

Baseline	**7.2.1 Contract management** • Contracts acknowledge that the third-party is responsible for the security and privacy of the sensitive or critical insurer data that it stores, processes, or transmits over secure connections.
	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 sensitive or critical insurer data. • A list of third parties that are network-connected and process, store or transmit sensitive or critical insurer data, is maintained.
Advanced	**7.2.1 Contract management** • A termination/exit strategy has been established for third parties that are network-connected and process, store or transmit sensitive or critical insurer data.

7.3 Ongoing monitoring of third-party risk

Maturity[8]	**Control Principles**
Baseline	• The cybersecurity assessments of third parties that are network-connected and process, store or transmit sensitive or critical insurer data are updated and reviewed regularly.
Intermediate	• A formal programme is in place that assigns responsibility for ongoing oversight of the access of third parties that are network-connected and process, store or transmit sensitive or critical AI data. • Monitoring of third parties that are network-connected and process, store or transmit sensitive or critical insurer data is scaled, in terms of depth and frequency, according to the risk of the third parties.

[8] No control principles of Advanced grade are applicable to this component. As such, an insurer which has an overall "High" inherent risk rating is expected to fulfill 100% of the control principles of both Baseline and Intermediate grades of this component only.

Annex C – Assessor/ Validator Qualifications

Role	Qualifications
Assessor/ Validator	• ISACA's Certified Information Systems Auditor (CISA); • (ISC)2's Certified Information Systems Security Professional (CISSP); • ISACA's Certified Information Security Manager (CISM); • ISACA's Certified in Risk and Information Systems Control (CRISC); • ISACA's Cybersecurity Fundamentals Certificate (CSX-F); and • China Information Technology Security Evaluation Centre's Certified Information Security Professional – Hong Kong (CISP-HK).

Annex D – Glossary of Key Terms and Abbreviations

Access Control	Means to ensure that access to assets is authorized and restricted based on business and security requirements. Source: ISO/IEC 27000:2018
Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity. Source: ISO/IEC 2382:2015
Agents	Licensed individual insurance agents and licensed insurance agencies act as agents of the authorized insurers which appoint them (i.e. the insurers are their principals). They promote, advise on and arrange insurance policies offered by their appointing insurers.
Alert	1. Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation’s information systems. Source: Adapted from NIST 2. Announcement of an abnormal situation or condition (from one or more cyber events) requiring attention. Source: Adapted from ISO 8468 2007
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals
Availability	Property of being accessible and usable on demand by an authorized entity. Source: ISO/IEC 27000:2018
BYOD	Bring-Your-Own-Device where staff may use their own personal devices for accessing the corporate network and systems.
Compromise	Violation of the security of an information system. Source: Adapted from ISO 21188:2018
Confidentiality	Property that information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems. Source: Adapted from ISO/IEC 27000:2018
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

	Source: Adapted from CPMI-IOSCO (citing NICCS)
Cyber Attack	Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorized access to assets. Source: Adapted from ISO 27100:2020
Cyber Event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring. Source: Adapted from NIST (definition of "Event")
Cyber Resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")
Cyber Threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security. Source: Adapted from CPMI-IOSCO
Defence-in-Depth	Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation. Source: Adapted from NIST and FFIEC
Denial of Service (DoS)	Prevention of authorized access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorized users. Source: Adapted from ISO/IEC 27033-1:2015
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cyber event. Source: Adapted from NIST Framework
Distributed Denial of Service (DDoS)	A denial of service that is carried out using numerous sources simultaneously. Source: Adapted from NICCS
EDR solution	Endpoint Detection and Response solution, which are tools that detect suspicious behaviour on an endpoint system level, and can be configured to provide automated responses such as blocking and alerting.

Exploit	Defined way to breach the security of information systems through vulnerability. Source: ISO/IEC 27039:2015
Identify (function)	Develop the organisational understanding to manage cyber risk to assets and capabilities. Source: Adapted from NIST Framework
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: Adapted from NICCS
Information System	Set of applications, services, information technology assets or other information-handling components, which includes the operating environment and networks. Source: Adapted from ISO/IEC 27000:2018
Integrity	Property of accuracy and completeness. Source: ISO/IEC 27000:2018
Intermediaries	Licensed insurance agents or licensed insurance brokers firms
IoT	Internet of Things refers to the collective of connected devices embedded with sensors and actuators, such as Internet connected security cameras, smart whiteboards, intelligent lightings, which are connected to the authorized insurer’s network or the Internet.
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems. Source: Adapted from ISO/IEC 27032:2012
Mobile device	Laptop computer, tablet, or phone used for accessing the corporate network and systems, regardless it is provided by the company or under BYOD programme where staff may use their own devices.
Multi-Factor Authentication	The use of two or more of the following factors to verify a user’s identity: - knowledge factor, “something an individual knows”; - possession factor, “something an individual has”; - biometric factor, “something an individual is or is able to do”. Source: Adapted from ISO/IEC 27040:2015
Patch Management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.

	Source: NIST
Penetration testing	A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. Source: NIST
Personal information	Any information that can be used to be identify, locate, or contact an individual.
Phishing	A digital form of social engineering that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication. Source: Adapted from ISO/IEC 27032:2012 and NICCS
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents. Source: Adapted from NIST Framework
Recover (function)	Develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired due to a cyber incident. Source: Adapted from NIST Framework
Remote access	The scenario where an end-point device is controlled by another end-point device (e.g., Remote Desktop Connection provided by Windows)
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cyber event. Source: Adapted from NIST Framework
Situational Awareness	The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: CPMI-IOSCO
Social Engineering	A general term for trying to deceive people into revealing information or performing certain actions. Source: Adapted from FFIEC.
Tactics, Techniques and Procedures (TTPs)	The behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

	Source: Adapted from NIST 800-150
Third party	Third parties which an insurer has external connections established, such as cloud service providers, business partners such as hospitals and clinics which store customer and transaction data of the insurer, service providers the insurer engages for outsourcing of certain data processing workflows.
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: Adapted from STIX
Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: NIST 800-150
TIBAS	Threat Intelligence Based Attack Simulation
Threat Vector	A path or route used by the threat actor to gain access to the target. Source: Adapted from ISACA Fundamentals
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. Source: Adapted from CPMI-IOSCO and ISO/IEC 27000:2018