

Insurance Authority Guideline on
Cybersecurity (GL20) Revision
What are the impacts on insurers?

January 2024 For POV Publication Online

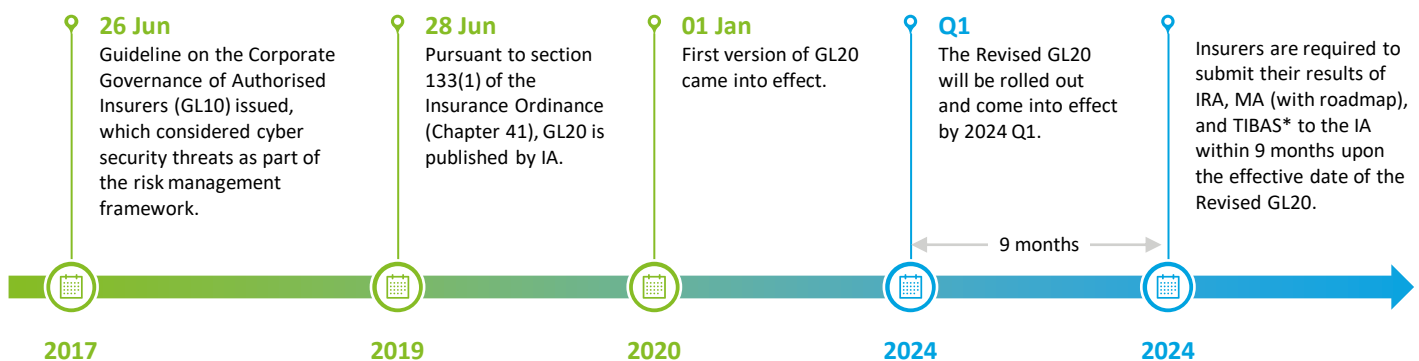


Summary of Guideline on Cybersecurity (GL20) Revision

Pursuant to section 133(1) of the Insurance Ordinance (Cap. 41) (the Ordinance), the Insurance Authority (“IA”) published the **Guideline on Cybersecurity** (“GL20”) in 2019, which came into effect since 1 January 2020, to regulate and supervise the insurance industry to protect all policy holders from cyber threats. It sets the minimum standard for cybersecurity that Authorised 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. However, in response to the fast changing landscape of emerging technologies and cybersecurity threats, the IA has proposed an updated framework in **October 2022**. And the **revised GL20** will be rolled out soon in 2024 Q1. The revised guideline will require Authorised Insurers to complete a set of assessments including Inherent Risk Assessment (“IRA”), Maturity Assessment (“MA”) and Threat Intelligence Based Attack Simulation (“TIBAS”)* **by 2024 Q4**.

*TIBAS is only applicable for Authorised Insurers with high or medium inherent risk level.

Timeline of the GL20 Assessments



What you should know about the GL20 Assessments

Requirements on Documentation Submission to the Insurance Authority

Inherent Risk Assessment

The report should include the overall results and individual results for each Indicator with justifications.

Maturity Assessment

The report should include the outcome of each Control Principle, the justification for the outcome and the **remediation roadmap** to close any gaps identified.

Threat Intelligence Based Attack Simulation

Authorised Insurers with medium and high inherent risks would be required to submit TIBAS along with MA results. The TIBAS should reflect real-life attack scenarios based on threats applicable to the authorised insurer.

Scope of Applicable Companies

All Authorised Insurers which carry on insurance business in or from Hong Kong, with the exception of Lloyd’s, captive insurers, special purpose insurers and marine mutual insurers.

Scope of Assessment

All systems, infrastructure (both on-premises and cloud infrastructure), processes, and people supporting the Authorised Insurers’ business in Hong Kong.

Requirement to Engage External Consultant

GL20 assessments must be performed by external consultants for Authorised Insurers with high and medium inherent risk level, while it’s optional for involving external consultants for low inherent risk Authorised Insurers.


Qualification of the Assessors

All assessors must be qualified (either by internal or external parties) with one of the following certifications: CISA, CISSP, CISM, CRISC, CSX-F & CISP-HK.


Completion Deadline

Results of the first IRA, MA and remediation roadmap are required to be submitted to the IA within 9 months upon the effective date of the Revised GL20. Submission of TIBAS results are also required for Authorised Insurers with medium/high inherent risks.

Inherent Risk Assessment

 **Inherent Risk Assessment**

 **Maturity Assessment**

 **Threat Intelligence Based Attack Simulation**

Authorised Insurers are required to perform the IRA to evaluate the Inherent Risk rating of the Authorised Insurers according to the indicators and assessment criteria within the GL20 Appendix: Annex A, which will result in the Authorised Insurers' overall inherent Risk rating. The Inherent Risk rating determines the expected maturity level of cyber resilience for the Authorised Insurer. The guideline is as below:

1 Compute the Risk Profile

Compute the inherent risk profile of a company according to the 5 categories and 40 risk indicators* ("RI") defined by the IA.



*RI: Each category encompasses a certain number of risk indicators, and each risk indicator has its assessment criteria to indicate the correspondent inherent risk level of an entity.

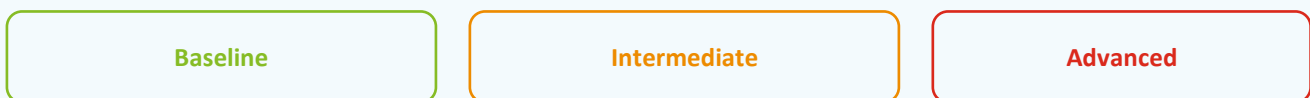
2 Define Inherent Risk Level

Define the overall inherent risk level by applying the formula stated in the GL20 Appendix with the total number of RIs at different inherent risk levels.



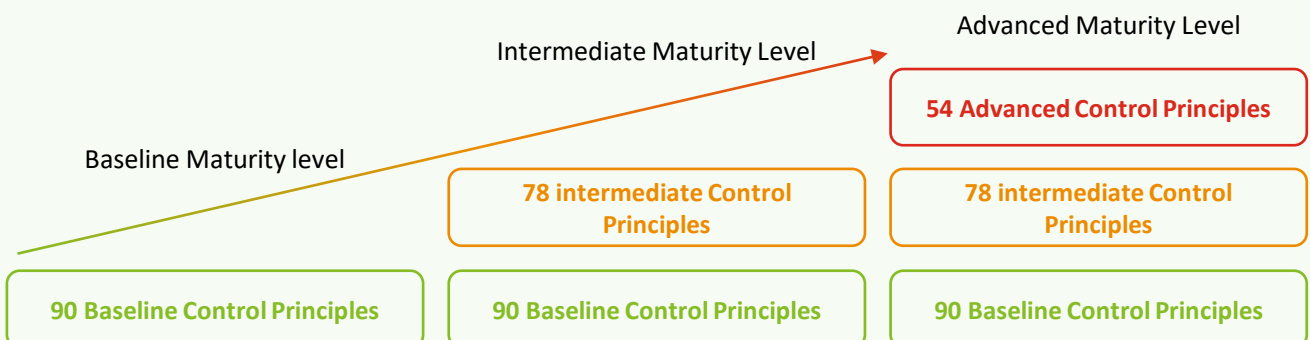
3 Assess Maturity Level

Match the overall inherent risk level to the minimum required maturity level in the assessment. Authorised Insurers with high, medium and low inherent risk levels are expected to achieve advanced, intermediate and baseline maturity level respectively.



4 Apply the Control Principles in accordance to the Maturity Level

Different levels of control principles should be applied in accordance to the maturity level.



Maturity Assessment

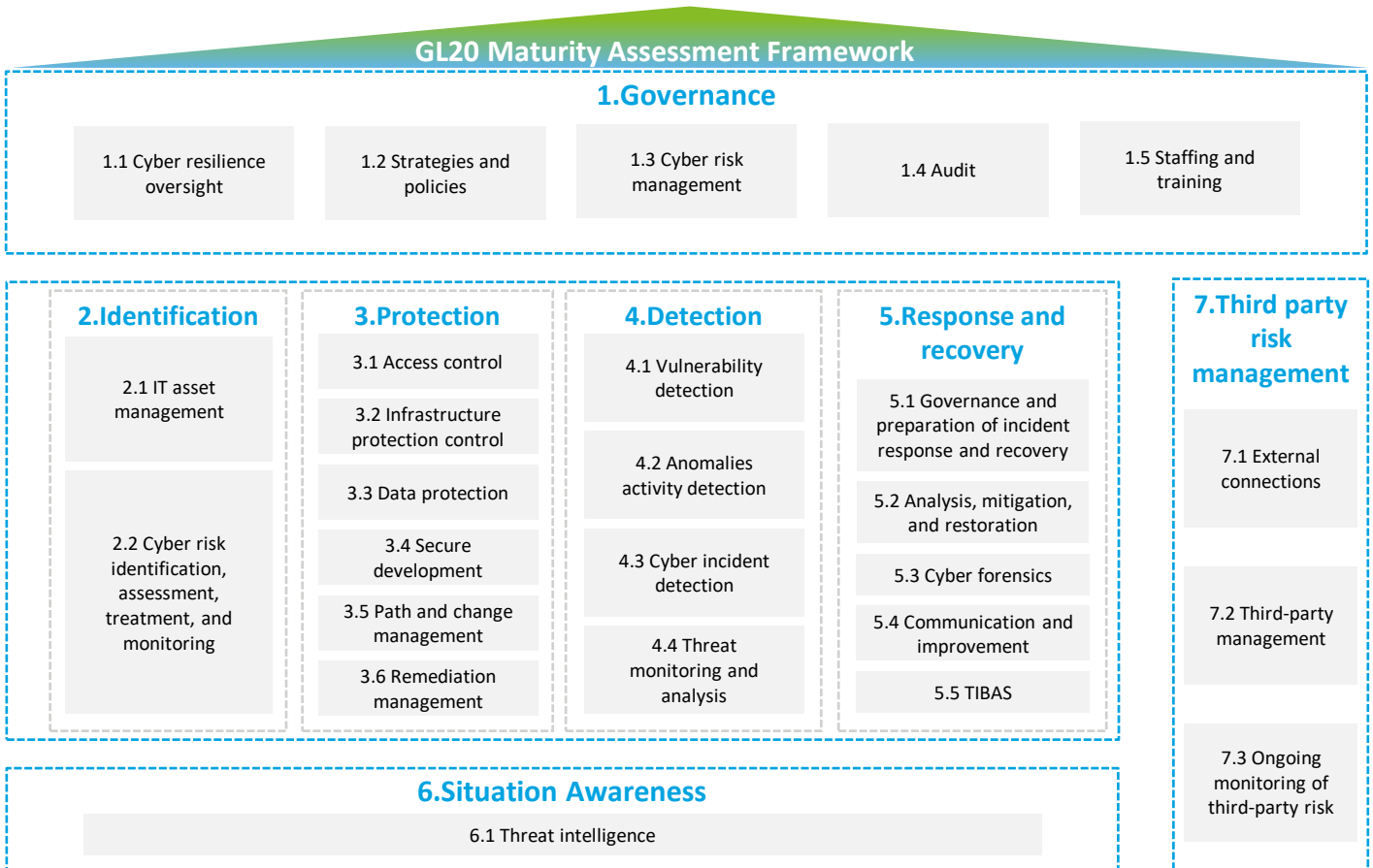
 Inherent Risk Assessment

 Maturity Assessment

 Threat Intelligence Based Attack Simulation

Authorised Insurers are required to assess the maturity of their cybersecurity posture according to the list of control principles within the GL20 Appendix: Annex B (the Maturity Assessment, “MA”) and identify the maturity gaps. Authorised Insurers are also required to submit the remediation roadmap and commit to improve the control maturity level.

There are **7 domains** and **26 components** in the GL20 MA Framework.



Key Takeaways of MA

1 100 % Attainment of Control Principles

- All in-scope Authorised Insurers must meet the applicable number of control principles per its inherent risk level with **100% compliance**. Compliance means required controls established, alternative controls implemented, and risk accepted for that control principle with risk-mitigating measures and valid justifications.

2 Sample-based Assessment

- Sampling-based testing** is a must for MA.
- Sampling should cover a period of the recent past **6 months** for the first-time assessment and **12 months** thereafter in subsequent assessments.
- Sample size should be **representative and risk-based**.


3 Roadmap

- Plans to close gaps between current maturity level and desired maturity level** should be established and submitted to IA along with MA results.
- All planned remediations must be implemented **before Authorised Insurers’ next GL20 assessment** which is typically 3 years after the current assessment.

4 Alternative Cyber Assessment

- In case any Authorised Insurer wishes to leverage other assessment, such assessment should be conducted by **qualified independent assessor in the past year** from the submission date.
- Mapping** is required to match the alternative assessments (e.g. C-RAF) to GL20 MA. Additional assessment should be supplemented if not fully matchable.

Threat Intelligence Based Attack Simulation

 Inherent Risk Assessment

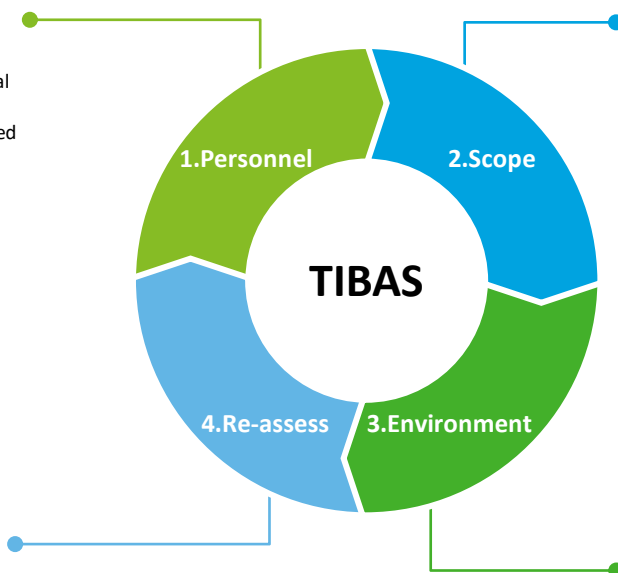
 Maturity Assessment

 Threat Intelligence Based Attack Simulation

In order to test the cyber incident response capability of the Authorised Insurers, TIBAS is required with real-life attack scenarios based on the applicable threats to the Authorised Insurers. The cybersecurity systems, people and process would be evaluated as part of this exercise. This simulation is **mandatory for all Authorised Insurers with medium and high inherent risks**. Below is the full cycle of TIBAS:

1. Personnel

- The personnel performing testing must be **Independent** (e.g. external consultant), and possess industry-recognised **qualifications** across red team and threat intelligence (e.g. OSCP).



2. Scope

- A **minimum of three end-to-end cyber-attack** scenarios shall be covered in the simulation for Authorised Insurers with medium inherent risks, and **five** for those with high inherent risks.
- Attack scenarios should be determined **based on threat intelligence applicable to the Authorised Insurer**.
- Human and process element** should be assessed atop of technological components.

4. Re-assess

- Relevant attack scenarios should be tested at least **every 3 years** or **after significant system, technology, third-party, or business changes**.

3. Environment

- Testing should be performed in **Production environments**.
- Simulation exercise and testing should be **performed confidentially** and only known to the essential stakeholders during the testing.
- Generate **report** to record the outcomes of the simulation testing components.

How can Deloitte help

Our Extended Service Offerings



Advise

- Gap Analysis and Readiness Assessment on the new GL20 Cybersecurity Framework
- Support IRA and MA
- Support TIBAS

Operate

- Design and Implement Cybersecurity Framework, Cyber Strategy and Governance Structure, including Risk Assessment
- Draft Policies and Procedures to facilitate putting in place formal process documentation
- Improve and test Incident Response Plans to handle incidents timely and effectively
- Tailor and deliver Training and Table-top Exercise for Crisis Management

Implement

- 24x7 Managed Security Service – Identify and Response to Cyber Incident
- Backup as a Service (BaaS), DR as a Service (DRaaS), Desktop as a Service (DaaS)
- Data Loss Prevention (DLP) support including Policy/Rule Review, Implementation and Monitoring

Our Success Stories

Our Deloitte Cyber professional team has the experience and knowledge to get you prepared for getting compliant with the new GL20 assessment requirements. Below are some recent successful stories of our cybersecurity assessments similar to the newly proposed GL20 appendix, which may also apply to you:

- Cyber Resilience Assessment Framework ("C-RAF 2.0"):** Deloitte team was engaged by various local/overseas banks and multiple virtual banks to perform cyber security assessment against C-RAF 2.0, **covering the scope similar to GL20 Assessments**, including **IRA, MA and Intelligence-led Cyber Attack Simulation Testing ("iCAST")**.
- Intelligence-led Cyber Attack Simulation ("iCAST"):** Deloitte team was engaged by several leading banking clients to plan, conduct and execute an **iCAST, akin to TIBAS**, to emulate various prevalent and compelling threats facing the bank based on a cyber threat intelligence analysis against their critical functions and Hong Kong financial industry sector, which in turn provides the organization with an opportunity to assess maturity of cyber resilience.

Our Professionals' Qualifications for GL20 Assessment



Contacts



Brad Lin
Partner, Risk Advisory
Cyber

bradlin@deloitte.com.hk
+852 2109 5353



Hatty Siu
Director, Risk Advisory
Cyber

hattysiu@deloitte.com.hk
+852 2852 5898



Philip Mok
Director, Risk Advisory
Cyber

phmok@deloitte.com.hk
+852 2740 8829



Becca Leong
Associate Director, Risk Advisory
Cyber

beleong@deloitte.com.hk
+852 2258 6266

**MAKING AN
IMPACT THAT
MATTERS**

since 1845

About Deloitte

Deloitte China provides integrated professional services, with our long-term commitment to be a leading contributor to China's reform, opening-up and economic development. We are a globally connected firm with deep roots locally, owned by our partners in China. With over 20,000 professionals across 31 Chinese cities, we provide our clients with a one-stop shop offering world-leading audit & assurance, consulting, financial advisory, risk advisory, tax and business advisory services.

We serve with integrity, uphold quality and strive to innovate. With our professional excellence, insight across industries, and intelligent technology solutions, we help clients and partners from many sectors seize opportunities, tackle challenges and attain world-class, high-quality development goals.

The Deloitte brand originated in 1845, and its name in Chinese (德勤) denotes integrity, diligence and excellence. Deloitte's global professional network of member firms now spans more than 150 countries and territories. Through our mission to make an impact that matters, we help reinforce public trust in capital markets, enable clients to transform and thrive, empower talents to be future-ready, and lead the way toward a stronger economy, a more equitable society and a sustainable world.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which is a separate and independent legal entity, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Bengaluru, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Mumbai, New Delhi, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

© 2024. For information, contact Deloitte China.

Designed by CoRe Creative Services. RITM1626777