The major revisions and the key points to note for GL20

The Hong Kong Insurance Authority (IA) announced the release of its revised Guideline on Cybersecurity (GL20), effective 1 January 2025. It sets the standard for cybersecurity that the authorized insurer should have in place and the general guiding principles in assessing the effectiveness of the authorized insurer's cybersecurity framework.

The revised GL20 introduces three parts: Inherent Risk Assessment, Cybersecurity Maturity Assessment, and Threat Intelligence Based Attack Simulation (TIBAS).

Inherent Risk Assessment and Cybersecurity Maturity Assessment should be conducted at least every three years or upon IA request on an ad-hoc basis. Authorized insurers may conduct the assessment if a new product launch is expected to result in any major changes to the business nature or technologies.

TIBAS should be conducted at least every three years or after significant system, technology, third-party, or business changes that could lead to a material increase in the associated risks, particularly the security risk and system availability of the service.

Major revision to GL20

Compared to the first version of GL20, effective from 1 January 2020, a Cyber Resilience Assessment Framework (CRAF) has been introduced in the revised GL20. CRAF provides a structured assessment framework to help authorized insurers assess inherent cybersecurity risks and the maturity level of their cybersecurity. CRAF covers three key components:

Inherent Risk Assessment

- The authorized insurers' risk rating will be determined using 40 assessment criteria across five categories.
- A three-tier inherent risk level (high, medium, low) will be assigned.

Cybersecurity Maturity Assessment

- A set of 90 to 221 control principles, spanning seven domains, will be used to evaluate expected cybersecurity controls.
- This evaluation will be conducted in accordance with the authorized insurers' overall inherent risk level.

Threat Intelligence Based Attack Simulation (TIBAS)

- Authorized insurers with medium and high inherent risk levels must simulate real-life attack scenarios.
- These simulations, conducted by competent adversaries, will test the insurers' cyber incident response capabilities.

Next steps for authorized insurers

- Authorized insurers should perform the Inherent Risk Assessment, Cybersecurity Maturity Assessment and TIBAS as follows:

Item	Low inherent risk rating	Medium or high inherent risk rating	
		Assessor requirement	Validation requirement
Inherent Risk Assessment	Inherent Risk Assessment and Cybersecurity Maturity Assessment should be conducted by the Assessor (Note 1).	Inherent Risk Assessment should be conducted by the Assessor who must possess at least one of the prescribed qualifications.	Result of the Inherent Risk Assessment must be independently validated by the Validator (Note 2) if the assessment is conducted by internal staff as the Assessor.
Cybersecurity Maturity Assessment		Cybersecurity Maturity Assessment should be conducted by the Assessor who must possess at least one of the prescribed qualifications.	Result of the Cybersecurity Maturity Assessment must be independently validated by the Validator if the assessment is performed by internal staff as the Assessor.
TIBAS	Not required	Required	

Note 1: Assessor refers to the internal staff of the insurer or an external consultant appointed by an insurer.
Note 2: Validator refers to an external consultant appointed by the insurer.

- For sample-based testing of controls, samples from at least the preceding 6-12 months should be covered.
- If any issues are identified, remedial action should be completed in a timely manner, but no later than when the next assessments are due.

Inherent Risk Assessment

The updated GL20 introduces five categories with 40 assessment criteria to identify the inherent risk level of authorized insurer. These are:

1. **Technologies and connection types**
2. **Delivery channels**
3. **Online/mobile products and technology services**
4. **Organizational characteristics**
5. **External threats**

Cybersecurity Maturity Assessment

Ninety to 221 cybersecurity control principles across seven domains will be evaluated, in accordance with authorized insurers' inherent risk levels.

Key control requirement areas that are newly added or enhanced compared to the previous GL20 requirements are as follows:

Governance	▪ Roles, responsibilities and accountabilities of the board of directors and senior management ▪ Cyber risk management function and the audit function
Identification	▪ Structured cyber risk management framework and IT asset management control
Protection	▪ Managing physical and logical user account accesses ▪ Infrastructure protection, secure development and end point data security controls, patching, change and remediation management
Detection	▪ Antivirus and anti-malware, penetration testing and simulation ▪ Vulnerability and anomalies activity detection, cyber incident, cyber threat intelligence
Response and recovery	▪ Governance and preparation of incident response and recovery, cyber forensics management ▪ Continuous cyber incident response and recovery improvement
Situational awareness	▪ Internal and external cyber threat intelligence and sharing
Third-party risk management	▪ Structured approach to perform third-party risk management

Threat Intelligence Based Attack Simulation

In order to test the cyber incident response handling capability of the authorized insurer, Threat Intelligence Based Attack Simulation (TIBAS) is required for authorized insurer with **medium** and **high** inherent risk rating to simulate real-life attack scenarios conducted by competent adversaries.

The GL20 guideline has the following key requirements for TIBAS:

Threat intelligence analysis should be used to formulate end-to-end cyber attack testing scenarios tailored to the authorized insurers and the insurance sector generally

Production environment/ close replica of the actual production component should be used for the exercise

Simulation testing should be conducted in several phases (e.g., scoping; identifying potential threat actors and tactics, techniques and procedures; developing testing scenarios, conducting testing, and preparing documentation)

Independent experts with necessary skills and expertise, and industry-recognized qualifications across red team and threat intelligence, should be engaged to conduct the testing

Attack simulation exercise should be kept secret to provide a more accurate assessment of the insurer's defense and incident response capability

How can EY teams help?

1. Support your readiness preparation to comply with the new GL20 requirements.
2. Perform Inherent Risk Assessment and Cybersecurity Maturity Assessment for you to meet IA's GL20 requirements by deadline.
3. Undertake TIBAS exercise for medium-risk and high-risk insurers.

EY contacts

Jeremy Pizzala
EY Asia-Pacific Cybersecurity Consulting Leader

+852 2846 9085
jeremy.pizzala@hk.ey.com

Alan Lee
Partner, Financial Services, Cybersecurity Consulting
Ernst & Young Advisory Services Limited

+852 2629 3160
alan.lee@hk.ey.com

Thomas Zhou
Partner, Financial Services, Cybersecurity Consulting
Ernst & Young Advisory Services Limited

+852 2846 9754
thomas.zhou@hk.ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG no. 000580-25Gbl
ED None

ey.com/china