January 2025

MOORE NEWSLETTER

Requirements on Documentation Submission on GL20 Assessment

INTRODUCTION

The Insurance Authority's Guideline on Cybersecurity (GL20) outlines three key requirements for documentation submission related to the GL20 assessments that authorised insurers must complete:

1. INHERENT RISK ASSESSMENT (IRA)

1.1 OBJECTIVES

Risk identification

IRA helps insurers identify and categorise their inherent risks associated with cybersecurity. Insurers are classified into three risk categories: low, medium, and high.

Control evaluation

IRA evaluates the effectiveness of existing controls in mitigating identified risks.

1.2 KEY COMPONENTS

Assessment criteria

Insurers must use specific criteria to assess their inherent risks. This includes analysing factors such as:

- nature of the business and operations
- types of data handled (e.g. personal, sensitive)
- historical data breaches or incidents
- regulatory requirements and industry standards.

Insurers must also utilise a set of indicators that cover the following aspects:

- technologies and connection types
- delivery channels
- online/ mobile products and technology services
- organisational characteristics
- external threats.

Insurers must apply control principles in accordance with the Maturity Level, which is divided into three levels, from baseline, intermediate, to advanced.

- **Baseline Maturity Level** includes 90 baseline control principles.
- **Intermediate Maturity Level** includes 90 baseline control principles and 78 intermediate control principles.
- **Advanced Maturity Level** includes 90 baseline control principles, 78 intermediate control principles and 54 advanced control principles.

Documentation requirements

- **Report outcomes**: Insurers are required to document the outcomes of their assessment of each control principle.
- **Remediation roadmap**: A clear roadmap must be provided to address any gaps identified during the assessment. This roadmap should outline specific actions, timelines, and responsible parties for remediation.

Submission timeline

The results of the IRA must be submitted to the Insurance Authority within **nine months** after the effective date of GL20, ensuring timely compliance with regulatory expectations.

2. MATURITY ASSESSMENT (MA)

2.1 OBJECTIVES

Evaluate cybersecurity posture

The MA assesses the actual maturity level of an insurer's cybersecurity practices against established control principles.

Identify gaps

Insurers must identify discrepancies between their current maturity levels and the expected levels determined by their IRA.

2.2 KEY COMPONENTS

Maturity levels

- **Baseline**: For insurers with low inherent risk.
- **Intermediate**: For insurers with medium inherent risk.
- **Advanced**: For insurers with high inherent risk.

Control principles

The assessment is based on a set of control principles spanning from seven domains, including:

- governance
- identification
- protection
- detection
- response and recovery
- situational awareness
- third-party risk management.

Document requirements

- Insurers must document their current maturity level, and the expected maturity level based on their IRA.
- A remediation roadmap must be developed to address any identified gaps, detailing specific actions, timelines, and responsible parties.

Sampling-based testing

- For initial assessments, sampling should cover a representative period of the past six months, while subsequent assessments require a twelve-month review.
- The sample size must be risk-based and representative to ensure accurate assessment results.

Submission timeline

Results from the MA must be submitted to the Insurance Authority within **nine months** following the rollout of the revised GL20, with subsequent assessments required every three years.

3. THREAT INTELLIGENCE-BASED ATTACK SIMULATION (TIBAS)

3.1 OBJECTIVES

Simulate real-world attacks

TIBAS aims to replicate real-life cyber-attack scenarios that insurers might face, enabling them to assess their preparedness and response capabilities.

Evaluate cybersecurity systems

The simulation evaluates the effectiveness of the insurer's cybersecurity systems, personnel, and processes in a controlled environment.

3.2 KEY COMPONENTS

Scope of simulation

- Insurers categorised as having **medium inherent risks** must conduct a **minimum of three** end-to-end attack scenarios.
- Those with **high inherent risks** are required to simulate **at least five** scenarios.
- Scenarios should be tailored based on threat intelligence relevant to the specific insurer, ensuring they reflect realistic threats.

Assessment criteria

- The simulations must assess both technological components and the human and process elements involved in incident response.
- The testing personnel should be independent, often involving external consultants with recognised qualifications in red teaming and threat intelligence.

Frequency of simulations

TIBAS simulations should be conducted at least every three years or after significant changes in systems, technology, third-party relationships, or business operations.

Document requirements

- Insurers must document the results of the simulations, including evaluations of their cybersecurity posture and any identified weaknesses.
- A report summarising the findings and recommendations for improvement must be submitted to the Insurance Authority within nine months following the rollout of the revised GL20.

Submission timeline

TIBAS results should be included with MA submissions within the same **nine-month** timeframe.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SMEs to listed companies from a wide variety of industry, and public sectors including government bureaus and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

To find out more, please contact one of our experts below:

PATRICK ROZARIO
Managing Director
T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal
T +852 2738 4631
E kevinlau@moore.hk

www.moore.hk