PICUS

Understanding GL20: Hong Kong's Cybersecurity Guideline for Insurers

What is the GL20?

On December 11, 2024, the **Hong Kong Insurance Authority** issued a revised Guideline on Cybersecurity (GL20). This guideline mandates that authorized insurers operating in or from Hong Kong adopt the Cyber Resilience Assessment Framework (CRAF) to strengthen their cybersecurity posture.

Who is Covered by GL20?

GL20 applies to all authorized insurers conducting business in or from Hong Kong, with limited exceptions.

Key Updates in the December 11, 2024 Revision

The revised GL20 introduces new assessments and compliance requirements aimed at enhancing insurers' cyber resilience:

1. Inherent Risk Assessment

Insurers must evaluate their inherent cyber risk exposure based on predefined risk indicators. This assessment determines the insurer's overall inherent risk rating—categorized as low, medium, or high—which reflects their baseline level of cyber risk.

2. Cybersecurity Maturity Assessment

Building on the Inherent Risk Assessment, insurers must assess their cybersecurity maturity against a set of prescribed control principles. This assessment helps:

- Identify gaps in existing controls
- Guide the development of improvement plans
- Ensure compliance with the required cybersecurity maturity level

3. Threat Intelligence-Based Attack Simulation (TIBAS)

Insurers with a medium or high inherent risk rating must conduct intelligence-led simulated cyberattacks to assess the effectiveness of their cybersecurity controls. These simulations go beyond traditional penetration testing by replicating real-world, end-to-end attack scenarios.

Penalties for Non-Compliance

Failure to comply with the revised GL20 may result in financial penalties:

- Monetary fines ranging from HK$100,000 to HK$5,000,000, depending on the severity of the violation.
- Additional daily fines for continued non-compliance, proportional to the severity of the issue.

Insurers should take proactive steps to align with the revised GL20 to avoid penalties and enhance their cybersecurity resilience.

The Role of Breach and Attack Simulation – How Picus Can Help

Breach and Attack Simulation (BAS) platforms help insurers meet GL20's TIBAS requirement, which mandates at least three attack scenarios for medium-risk insurers and five for high-risk ones. BAS provides automated, intelligence-driven attack simulations that closely mirror real-world threats, enabling insurers to validate the effectiveness of their security controls without disrupting business operations.

How BAS Supports GL20 Compliance

- **Automated Attack Testing –** Simulates a range of cyber threats, including ransomware, insider threats, and advanced persistent threats (APTs), to assess an organization's detection and response capabilities.

- **Security Control Validation –** Continuously tests critical security controls such as firewalls, EDRs, and SIEMs to ensure they detect and block real threats while generating compliance-ready evidence.

- **Risk-Based Prioritization –** Correlates exposures with threat intelligence to reduce false positives and focus remediation efforts on the most critical weaknesses, aligning with GL20's risk-based methodology.

Why Picus for Breach and Attack Simulation?

Not all BAS platforms are created equal. Picus offers a comprehensive BAS solution that not only meets GL20's requirements but also enhances overall cyber resilience. More than just a compliance tool, Picus delivers continuous security validation to improve an insurer's cyber defense readiness.

Key advantages of Picus Security include:

- **Integrated Security Stack Support –** Seamlessly connects with SIEM, EDR, and XDR solutions to ensure attack simulations trigger relevant alerts and generate compliance-ready reports.
- **Ongoing Validation & Posture Tracking –** Detects configuration drift, misconfigurations, and security gaps through scheduled or on-demand simulations.
- **Prioritized Risk Mitigation –** Focuses remediation on exploitable, high-impact vulnerabilities, reducing unnecessary effort.
- **Targeted Remediation Guidance –** Provides precise mitigation recommendations to improve efficiency and align with GL20's security mandates.

By leveraging Picus BAS, insurers can continuously validate defenses, maintain GL20 compliance with confidence, and strengthen resilience against evolving threats. The result is not just regulatory adherence but a higher level of security preparedness to protect against modern cyberattacks.

About the Picus Security Validation Platform

Reduce your threat exposure with real-world attack simulations and AI-driven insights.

Security Control Validation

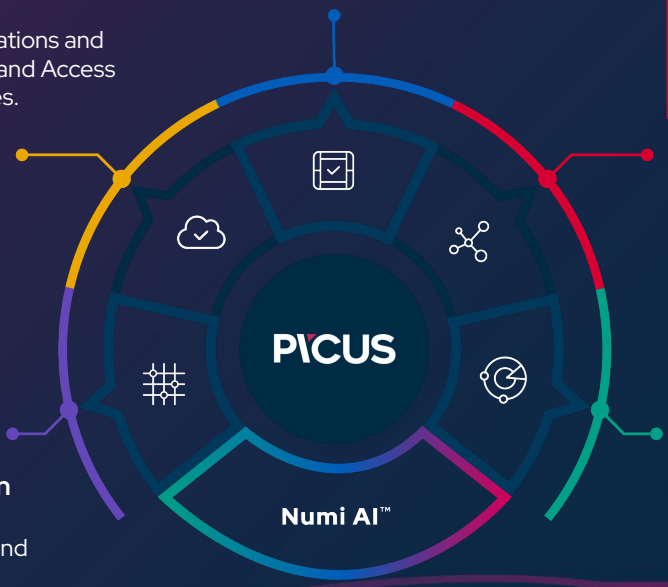
Measure and optimize the effectiveness of security controls with Breach and Attack Simulation.

Cloud Security Validation

Identify cloud misconfigurations and overly permissive Identity and Access Management (IAM) policies.

Attack Path Validation

Eliminate high-risk attack paths that attackers could exploit to compromise users and assets.



Attack Surface Validation

Enhance visibility of internal and external cyber assets and the security risks they pose.

Detection Rule Validation

Optimize detection efficacy by identifying performance issues affecting detection rules.

Elevate your security capabilities with the Picus Security Validation Platform

REQUEST A DEMO

PICUS

picussecurity.com

FROST & SULLIVAN FROST RADAR™ LEADER Global Breach and Attack Simulation 2022

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2023

GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2024

Gartner Peer Insights Customers' Choice 2024

4.8/5.0

Highest-rated vendor*

Breach and Attack Simulation

*Gartner, Voice of the Customer for Breach and Attack Simulation Tools, Peer Contributors, 30 January 2024