CHARTERED GOVERNANCE Hong Kong

Issue 25 • October 2025

HKCGI Technology Guidance Note (Twenty-fifth Issue) on Overview of Technology Risk (Part 2)

In the earlier part of this guidance note, we have provided, by way of example, and as an overview, several technology-related risks, and some high-level questions boards need to ask to assess their effective oversight. We now turn to some related metrics and liability issues in this guidance note, along with an introduction to cyber insurance.

Types of Metrics

Technology risk metrics can be categorised into strategic, operational, financial, and benchmark metrics. Each type serves a different purpose in helping the board understand the organisation's technology risk posture. Directors and governance professionals need to ask and seek answers to assess the related director oversight over technology-related issues, as there is no one-size-fits-all approach to managing technology-related risks as part of enterprise risk management.

- **Strategic Metrics**

  Strategic metrics focus on the organisation's approach to technology risk and risk management. Questions include:

  - **Risk Appetite:** What level of technology risk is the organisation willing to accept in pursuit of its strategic objectives?

  - **Investment in technology risk:** How much is the organisation investing in technology risk measures? Is Management using Cyber Risk Quantification (CRQ) to compare the cost of security initiatives vs. the reduction in risk? Is the investment aligned with industry standards?

- *Authors: **Melody Qian**, Senior Vice President, Lockton and **Greg Sinclair**, Partner, Control Risks, Asia Pacific, with contributions from **Mohan Datwani FCG HKFCG(PE)**, Institute Deputy Chief Executive*
- *Technology Interest Group: **Dylan Williams FCG HKFCG** (Chairman), **Ricky Cheng**, **Harry Evans**, **Gabriela Kennedy**, and **Philip Miller FCG HKFCG**.*
- *Comments and suggestions: mohan.datwani@hkcgi.org.hk.*

- **Operational Metrics**

  Operational metrics provide insights into the day-to-day effectiveness of technology risk controls. Questions include:

  - **Incident Response Times:** How quickly does the organisation detect and respond to cyber incidents?

  - **Patch Management:** How effectively is the organisation managing software vulnerabilities through regular patching?

- **Financial Metrics**

  Financial metrics quantify the economic impact of technology risks. Questions include:

  - **Cost of Cyber Incidents:** What is the financial impact of recent cyber incidents on the organisation?

  - **Return on Investment (ROI):** How effective are the organisation's technology risk investments in reducing risk?

- **Benchmark Metrics**

  Benchmark metrics compare the organisation's technology risk performance against industry peers. Examples include:

  - **Security Ratings:** How does the organisation's security posture compare to others in the industry?

  - **Compliance Metrics:** How well is the organisation adhering to relevant technology risk standards and regulations?

- **Implementing Metrics**

  - The governance professional should work with management to implement a robust system for tracking and reporting technology risk metrics. This system should provide the board with clear, concise, and actionable insight.

  - A critical component of effective technology risk management is the need for continuous improvement. The dynamic and changing threat landscape, changes in the technology ecosystem, and more effective controls require ongoing oversight and validation that changes are incorporated and that our organisations are well-prepared to protect their assets and maintain resilience in the face of evolving technology threats.

Liabilities Associated with Technological Risks

Apart from understanding the relevant metrics, for director and governance professionals, and as an added overview, there are two main categories of companies in the technological world: one is the IT /Technology service providers, and the other is the end-users. The IT / Technology service providers focus on producing IT products or services (such as systems, software, hardware, platforms, social networking companies, etc.) while end-users utilise those products and services to perform specific tasks and functions without developing their own technologies.

Common Risks

Whilst these two categories are fundamentally different in business services, they would face some common risks. One of the risks that stands out and could lead to significant financial losses, reputational damage, and operational disruption for all businesses is cyber risks.

According to the 14th Allianz Risk Barometer issued in 2025 which incorporates the views of 3,778 respondents from 106 countries and territories, 38% of respondents pick cyber risks as the top business risk for 2025, 7% points ahead of business interruption in #2. Ten years ago, cyber risk ranked only #8 globally with just 12% of responses.

In today's digitalised world, it is crucial to make continuous investment in IT / cyber security; however, there is no such thing as a "perfect" cyber security, as it is an ongoing process of defence against evolving threats. Cybersecurity is not about achieving flawless invulnerability, but about managing risk, ensuring resilience, minimising damage and transferring risk.

Cyber insurance is an economic way of risk transfer, as it could cover a wide range of potential financial losses:

- First-party (Reimbursement) Coverages, such as net profit losses from business / net interruption, ransom payment, costs associated with data recovery, forensic investigations, public relations, etc. Insurers will also provide incident response services led and coordinated by Breach Counsel / Coach.

- Third-party (Liability) Coverages, such as defence costs and damages (or settlement fees) arising from third-party claims as a result of cyber incidents, as well as the regulatory investigations followed by regulatory fines and penalties.

Technology / IT Risks

For IT / Technology service providers, they are also exposed to risks of mistakes, errors or omissions, failure to deliver services as promised or failure to perform to specification. Even when they deliver correctly, they may find themselves facing legal claims – often from clients looking for someone to hold responsible when a project runs into a problem.

When selecting technology service providers and vendors, whilst it is crucial to assess their technical expertise, track record and financial strength, end-users can also require them to have proper insurance in place to recourse the loss.

IT / Technology Companies can purchase Professional Indemnity (PI) insurance to transfer this type of risk. PI insurance covers claims alleging negligence, errors or omissions, or breach of contract out of professional services, i.e. costs associated with legal defence and damage if the clients suffer financial losses due to professional advice or services, or fail to deliver professional advice or services. Common examples for ITPI risks include:

- Design defects and errors in software or hardware development.

- Failure to deliver on promised timelines or meet deadlines for tech products or services.

- Improper documentation of services rendered, such as providing incorrect specifications or user instructions.

- Tech issues that cause financial losses for customers, such as data breaches, system failures, and more.

- Tech bugs and glitches that impact customer usability and satisfaction with a product or service.

- Tech issues that result in product recalls, refunds, or other financial penalties for your business.

- Negligence related to the testing of new technologies before they are released to the public.

- Any other mistakes or oversights in the development and implementation of your tech product?

In conclusion, technology risk management is a critical responsibility for governance professionals to facilitate board oversight. By raising awareness of the need to assess the effectiveness of technology risk oversight and implementation of robust technology risk metrics, governance professionals can help their organisations navigate the complex landscape of technology threats. Further, there is scope for liability mitigation through cyber risk insurance.

The Hong Kong Chartered Governance Institute (HKCGI) 香港公司治理公會

(Incorporated in Hong Kong with limited liability by guarantee)