CHARTERED GOVERNANCE
Hong Kong

Issue 24 • October 2025

HKCGI Technology Guidance Note (Twenty-fourth Issue) on Overview of Technology Risk (Part 1)

The governance professional plays a pivotal role in ensuring that their organisation is well-prepared to identify, manage, and mitigate all forms of technology risks as part of director oversight. However, given other forms of director oversight, there is a need to prioritise to maximise effective technology risk oversight and technology risk metrics. The purpose of this guidance note is to focus on technology risk, assisting directors, governance professionals, and others supporting them in discharging the requisite oversight.

Introduction

Our lives, both professionally and personally, are increasingly digital. Computers, phones, banking, transportation, manufacturing, education, healthcare – it's difficult to avoid technology applications and digital communications – and certainly our future likely includes even more reliance on technology.

In 2024, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) reported handling 12,536 cyber risk incidents, marking a five-year high [1]. While significant, this represents only one type of technology risk. With increased digital transformation, we face an increase in technology risks – for example:

- **Cyberattacks and Data Breaches**
  Sophisticated threat actors target global enterprises to steal sensitive data, exploit misconfigurations, disrupt operations, or demand ransom. Employees are frequently targeted with deceptive communications designed to steal credentials or deploy malware. All these could erode customer trust, impact stock prices, and damage long-term brand equity.

- *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.*

- **Third-Party, Supply Chain and Concentration Risks**
  Vulnerabilities in vendors or partners can become entry points for attackers, compromising your organisation's security posture. The concentration of risk in centralised technological ecosystems is a top risk for many organisations.

- **Insider Threats**
  Malicious or negligent employees can cause significant damage by leaking data or misusing access privileges.

- **Regulatory Non-Compliance**
  Failure to comply with evolving global data protection laws (e.g., PDPO, GDPR) can result in heavy fines and reputational damage.

- **Industrial Control System (ICS) or Operational Technology (OT) Vulnerabilities**
  In sectors like manufacturing or energy, legacy OT systems are increasingly connected to IT networks, creating new attack surfaces, and increased risk for critical infrastructure operators.

- **AI and Deepfake Threats**
  Emerging technologies like deepfakes and AI-generated content are being weaponised to impersonate executives or manipulate public perception.

Assessing Technology Risk Oversight Effectiveness

The governance professionals' role in technology risk oversight is multifaceted. It involves helping directors to set the tone at the top, ensuring that technology risk is integrated into the organisation's overall risk management framework, and providing strategic direction. Boards should view technology risk not merely as a technology issue but as a strategic, enterprise-wide risk.

Five Key Questions for Assessment

To evaluate the board's technology oversight effectiveness, the governance professional should help directors to consider the following key questions:

- **What is the threat environment we face (technology literacy):** Can all directors effectively contribute to discussions about the company's technology risk? Are there gaps in their understanding that need to be addressed? Is the board aware of the legal and regulatory requirements related to all forms of technology risk? Is there a broad understanding of all forms of technology risks, or over-reliance on media-influenced reporting on ransomware for example?

- **What is the technology risk profile, as defined by Management?** How are we performing against basic cyber hygiene requirements (passwords, patching, etc)? What percentage of our Supply Chain failed our security assessment? Do we measure Supply Chain risk based only on questionnaires? How frequently does the board receive updates on technology risk from management? Are these updates comprehensive and actionable?

- **What is our risk profile looking like from the outside looking in?** What are the findings of our most recent security assessment (functional and technical)? How much have we improved since our last assessment? Is there a clear incident response plan in place, for all forms of technology risks – or only a few? Does the board understand its role in the event of a technology risk incident? Does the organisation practice regularly?

- **What is our loss exposure in economic terms?** What is the probable frequency and magnitude of our top technology risks? What level of risk can we tolerate? Is our spending on cyber controls sufficient?

- **Are we making the right business and operations decisions?** What is the technology risk of new initiatives? What is the risk reduction, in economic terms, for various security improvement initiatives? How much cyber insurance do we need?

Tools for Assessment

The governance professional should raise the awareness that directors could ask relevant members of the management team, for example, the CIO, to consult technology risk professionals, or leverage the use of tools like the NACD's Cyber-Risk Oversight Handbook [2] or UK NCSC Toolkits Toolbox [3] to guide an effectiveness assessment. These handbooks provide a numerical scale for evaluating the board's cyber-risk oversight effectiveness.

Technology Risk Metrics

Metrics are essential for tracking the effectiveness of technology risk efforts and informing strategic decisions. The governance professional should ensure that their boards have access to relevant and actionable technology risk metrics. In the second part of this guidance note, we will consider the types of metrics and other liability issues associated with technology risks.