Cyber-Risk Oversight

Raising the Bar for Cyber-Risk Management Oversight and Reporting

By Sandra Herrygers and Gaurav Kumar

Perhaps no area of risk management presents a greater challenge to boards than that of cyber risk. With the proliferation of cybercrime and recently proposed legislation related to cyber-risk reporting and disclosures, organizations are under intense pressure from stakeholders to respond to inquiries on the effectiveness of their cyber risk management programs. Even though cyber risk is on many boardroom agendas, there is a growing need for much greater transparency around an organization's cyber-risk management program.

Boards rely on a variety of cyber-risk monitoring and reporting mechanisms, including, but not limited to, risk and control self-assessments, internal audits, and crisis management simulation exercises. Yet there seems to be a lack of clarity on the role the board should play to address cyber risk for their organizations. This is compounded by the reality that there is no single approach for reporting on an entity's cyber-risk management program and related controls.

In response to this need, the American Institute of Certified Public Accountants (AICPA) is developing new attestation guidance specifically focused on reporting on an entity's cyber-risk management program. The proposed AICPA cybersecurity examination engagement is intended to expand cyber-risk reporting to address expectations of greater stakeholder transparency by providing a range of stakeholders, both internal and external, with information about an entity's cyber-risk management program effectiveness.

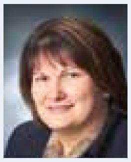
Organizations may realize the following benefits of undertaking a cybersecurity examination engagement:

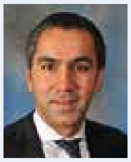
- Independent and objective reporting, providing a higher degree of assurance to key stakeholders.
- Operational efficiencies from having a single reporting mechanism addressing the information needs of a broad range of users.
- Greater transparency around the effectiveness of the entity's cyber-risk management program to internal and external stakeholders (e.g., boards, regulators, etc.).
- Greater economic value for intended users of the report by obtaining information about an entity's cyber-risk management program that would be useful in making informed and strategic decisions.

Due to the rapidly evolving nature of cyber risks and the varying levels of maturity of entities' cyber-risk management programs, organizations should consider performing a cybersecurity examination readiness assessment prior to transitioning to an independent third-party cybersecurity examination engagement. A cybersecurity examination readiness assessment consists of:

1. Selecting an appropriate cyber-control framework (e.g., the National Institute of Standards and Technology's cybersecurity framework) that can be utilized in a future cybersecurity examination engagement.
2. Evaluating the effectiveness of the current state of internal controls included within the entity's cyber-risk management program, and leveraging the cyber-control framework adopted by management.
3. Identifying potential gaps in and enhancement opportunities for key cyber-risk processes and related internal controls.
4. Developing a remediation plan and subsequent execution of key remediation activities.

A comprehensive cyber-risk management program is integral to an organization's ability to achieve its business objectives. An active board is critical to such a program's success. This entails holding the organization accountable for cyber-risk management, helping shape expectations for improved cyber-risk reporting, and advocating for greater transparency around the effectiveness of the program. In light of mounting pressure on organizations to report on the effectiveness of their programs, the time to act is now. Investing in a comprehensive cybersecurity examination readiness assessment can help you prepare management for a future independent, third-party cybersecurity examination engagement.





Sandra Herrygers is a partner at Deloitte & Touche LLP and is the Global Assurance Leader; Gaurav Kumar is a principal at Deloitte & Touche LLP, specializing in Assurance and Risk and Controls Transformation services.

This article contains general information only, and Deloitte LLP and its subsidiaries ("Deloitte") are not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.