Overview of Cybersecurity Risk Management Reporting Framework

Market need

Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world — large and small, public and private. Managing this business issue is especially challenging because even an organization with a highly mature cybersecurity risk management program still has a residual risk that a material cybersecurity breach could occur and not be detected in a timely manner.

Organizations and their stakeholders need timely, useful information about organizations' cybersecurity risk management efforts. Corporate directors and senior management have begun requesting reports on the effectiveness of their cybersecurity risk management programs from independent third-party assessors. In response to such requests, the AICPA developed a voluntary, market-based solution to enhance public trust in entity-prepared communications about the effectiveness of their cybersecurity risk management programs.

Our intent is to establish a common, underlying language for cybersecurity risk management reporting — almost akin to U.S. GAAP or IFRS for financial reporting. In doing so, we recognize that cybersecurity is not just an IT problem; it's an enterprise risk management problem that requires a global solution. We've developed a robust reporting framework and related criteria that may be used by both management and CPAs to enhance cybersecurity risk management reporting.

The reporting framework, including the related criteria, are used to perform an examination-level attestation engagement, known as a cybersecurity risk management examination (SOC for Cybersecurity).

Cybersecurity risk management examination and report

The framework for reporting on an entity's cybersecurity risk management program calls for management to prepare certain information about the entity's cybersecurity risk management program and for the CPA to examine and report on that information in accordance with the AICPA's attestation standards.

The resulting cybersecurity report includes the following three key sets of information:

1. Management's description — The entity's cybersecurity risk management program (the subject matter of the engagement)
2. Management's assertion — The presentation of the description and the effectiveness of the controls to achieve the cybersecurity objectives
3. The practitioner's opinion — The presentation of the description and the effectiveness of the controls to achieve the cybersecurity objectives

Two sets of criteria

As part of the reporting framework, the AICPA developed two distinct but complementary sets of criteria for use in the examination to enhance the comparability of entity-prepared communications about cybersecurity matters.

Description criteria is used by management when preparing a narrative description of the entity's security risk management program. CPAs can also use the description criteria when reporting on the description.

Control criteria is used when evaluating the effectiveness of the controls within the program. Management may use the revised Trust Services Criteria for Security, Availability, and Confidentiality (2017) (trust services criteria) as the control criteria by which the effectiveness of those controls may be evaluated.

However, our reporting framework is flexible in that it permits management to use criteria other than the trust services criteria as control criteria (such as the NIST Critical Infrastructure Cybersecurity Framework and ISO 27001/27002) as long as such criteria are appropriate for the engagement in accordance with the AICPA's attestation standards.

Cybersecurity guide

In addition to developing the two sets of criteria described above, the AICPA Assurance Services Executive Committee (ASEC) Cybersecurity Working Group collaborated with the AICPA Auditing Standards Board (ASB) to develop Reporting on an Entity's Cybersecurity Risk Management Program and Controls, an attestation guide to assist CPAs on how to perform and report on cybersecurity risk management examinations, in accordance with the AICPA attestation standards.

The cybersecurity guide may also be helpful to a CPA engaged to provide cybersecurity advisory services to an organization, i.e., helping an organization improve its cybersecurity risk management program.

Conclusion

We believe our cybersecurity risk management reporting framework is a critical first step to enabling a consistent, market-based, business-based solution for companies to effectively communicate with key stakeholders on how they are managing cybersecurity risk. As the maturity of entities' cybersecurity risk management programs increases, the reporting framework can also serve as the foundation for a high-quality, examination-level attestation engagement, known as a "cybersecurity risk management examination" (SOC for Cybersecurity), performed by an independent CPA. Ultimately, use of the reporting framework and related criteria may enhance the confidence that stakeholders place on the entity's cybersecurity communications.

To learn more and download the framework, visit aicpa.org/cybersecurityriskmanagement.

AICPA