CYBERSECURITY
How CPAs and their Firms Are Addressing a Dynamic and Complex Risk

CPAs and their public accounting firms are fostering a conversation to drive a market-based solution to evaluating cybersecurity risk management programs. This solution is intended to enhance public trust in the effectiveness of a company's cybersecurity risk management program.

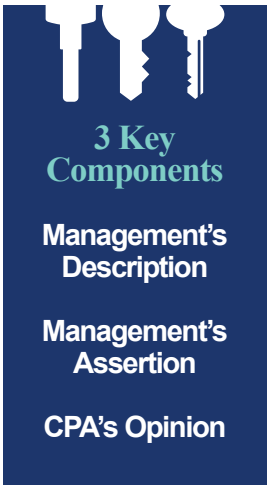
Evolving Cybersecurity Risks

Awareness continues to grow around the evolving cybersecurity threats to companies. Given the immense scale and complexity of the cybersecurity challenge, every sector of the global economy must do their part to promote cybersecurity resilience.

The public accounting profession is in a strong position to play an important role in fostering instructive conversations about cybersecurity risk management, bringing to bear the CPA's core values—including independence, objectivity, and skepticism—as well as the profession's deep expertise and skills in providing independent evaluations in a variety of contexts.

A Comprehensive Approach to Addressing Cybersecurity Risk Management Programs

Entity-Level Cybersecurity Reporting Framework



In response to growing challenges related to cybersecurity risk management, the American Institute of CPAs (AICPA)[1] developed an entity-level cybersecurity reporting framework that organizations can use to communicate useful information about their cybersecurity risk management program to a broad range of stakeholders. The reporting framework provides users with three key pieces of information that can be used to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of their organization's cybersecurity risk management program. The development of a cybersecurity reporting framework springs from the public accounting profession's commitment to continuous improvement, public service, and increasing investor confidence. The AICPA's cybersecurity reporting framework has been developed to provide the market with a common approach to evaluating and reporting on a company's cybersecurity risk management program. The approach is voluntary, flexible, and comprehensive.

There are three key components of the reporting framework that can assist stakeholders in understanding an entity's cybersecurity risk management program.

- **Management's Description of the entity's cybersecurity risk management program.** Management will provide potential users with a description of an entity's cybersecurity risk management program. Management will utilize suitable description criteria in developing Management's Description of the subject matter, and for CPAs evaluating the description. One such suitable criteria is the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program.* The Description Criteria are categorized into nine areas so that Management's Description provides users with information about an entity that will enable them to better understand the entity and its cybersecurity risk management program. Management's Description will include information about the entity's operations, how the entity identifies its sensitive information and systems, the ways in which the entity manages the cybersecurity risks that threaten it, and a summary of cybersecurity controls processes. Management's Description is intended to provide the context needed for users to understand the conclusions expressed by management in its assertion, and by the auditor in its report.

- **Management's Assertion.** Management will assert to the presentation of the Management's Description of the entity's cybersecurity risk management program in accordance with the description criteria, and whether the controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on a suitable set of control criteria. The Trust Services Criteria (criteria for security, availability, and confidentiality) have been designed to be suitable control criteria.

- **The CPA's Opinion.** The CPA's Report contains an opinion on the description of the entity's cybersecurity risk management program and the effectiveness of the controls within the program to meet the entity's cybersecurity objectives.

Independent Examination

While companies may not implement all three components of the reporting framework at once, the public accounting profession believes that when an entity provides information to stakeholders—such as the board of directors or audit committees—to enable decision making, it is not enough to provide them merely with information. Decision makers need confidence that the information they have been provided is presented in accordance with suitable criteria. The third component described above in the AICPA's cybersecurity reporting framework, the CPA's opinion, can enhance confidence in the cybersecurity information prepared and presented by management. CPAs will perform a Cybersecurity Risk Management Examination ("Examination"), inaccordance with AICPA attention standards, to provide an opinion on Management's Description and on the effectiveness of the controls implemented as part of the cybersecurity risk management program. For those companies that are not ready for an attestation Examination, the AICPA's cybersecurity reporting framework can be used for a non-attestation cybersecurity engagement, such as a readiness engagement.

The CPA Firm's Role in Cybersecurity Risk Management

Today, four of the leading 13 information security and cybersecurity consultancies are CPA firms. Many CPA firms have built substantial cybersecurity practices and capabilities that enable them to advise companies in all aspects of cybersecurity risk management. If CPA firms are engaged to perform the Examination for companies, CPAs will work in collaboration with individuals at their firms who also have credentials related to information technology and security, often in addition to their CPA. These include: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Technology Professional (CITP). Cybersecurity expertise and an understanding of controls will be required to complete the Examination, and both are present in CPA firms. As multidisciplinary firms, CPA firms routinely provide a diverse range of services, beyond the financial statement audit.

CPA firms also have quality control systems in place to monitor their engagement teams' adherence to professional standards, and are subject to oversight by the profession through peer reviews, further enhancing the quality of the services delivered.

Potential Benefits of the Proposed Cybersecurity Risk Management Framework

There are a number of potential benefits to a market-based solution to evaluating and reporting on a company's cybersecurity risk management program. They include:

- **Flexibility—**Companies, even within the same industry, are not identical. The cybersecurity reporting framework, including the Examination that the AICPA has developed is entirely voluntary on the part of companies and audit firms. This flexible approach will provide companies and stakeholders with an evaluation of their cybersecurity risk management program in a manner tailored to their particular situation, and the evolving cybersecurity threats they face.

- **Common approach—**A common and consistent approach for companies to report information about their cybersecurity risk management program, once established and accepted in the market, could potentially reduce industry and other regulatory compliance requirements that can (1) distract company resources away from cybersecurity risk management and (2) burden companies with checklist compliance exercises that are typically ineffective responses to advancing data security threats. Widespread market consensus around a given approach can aid in establishing a uniform, cross-industry methodology to evaluating a company's cybersecurity risk management program.

- **Innovative and sustainable solution—**The AICPA plans to adapt and advance the cybersecurity reporting framework according to feedback from users in the marketplace, with an emphasis on identifying opportunities to enhance efficiency and reduce compliance burdens.

1 The AICPA's mission is to power the success of global business, CPAs, CGMAs and specialty credentials by providing the most relevant knowledge, resources and advocacy, and protecting the evolving public interest. The AICPA develops standards for audits of private companies and other services performed by CPAs.