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] is developing a reporting framework that organizations can use to communicate useful information about their cybersecurity risk management program to a broad range of stakeholders. The entity-level reporting framework has three key components 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 reporting framework springs from the public accounting profession's commitment to continuous improvement, public service, and increasing investor confidence. The profession is working to provide a common approach for evaluating cybersecurity risk management that could enhance public trust in the effectiveness of a company's cybersecurity risk management program. The approach will be voluntary, flexible, and comprehensive.

3 Key Components

Management's Description

Management's Assertion

CPA's opinion on Management's Description

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. This management prepared narrative description is designed to provide potential users with 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 controls implemented and operated to protect the information and systems against those risks. Management's Description is intended to provide the context needed to understand the conclusions expressed by management in its assertion, and by the auditor in its report, about the effectiveness of the controls included in the entity's cybersecurity risk management program.

CENTER FOR AUDIT QUALITY

OCTOBER 2016

- **Management's Assertion** Management will also assert to the presentation of their management description, and that the controls implemented as part of the cybersecurity risk management program are effective to achieve the entity's cybersecurity objectives.

- **CPA's opinion** on the description of the entity's cybersecurity risk management program (i.e. completeness and accuracy) and the effectiveness of the controls within the program to achieve the entity's cybersecurity objectives.

Independent Examination

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 fairly presented. The third component described above in the AICPA's approach to a cybersecurity risk management program framework, the CPA's opinion, is the component that can enhance confidence that Management's Description is fairly presented. CPAs will perform a cybersecurity risk management program examination ("examination") in order to provide an opinion on Management's Description and on the effectiveness of the controls implemented as part of the cybersecurity risk management program.

The CPA Firm's Role in Cybersecurity Risk Management

Today, four of the leading 10 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 choose 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 ensuring that 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 a company's cybersecurity risk management program. They include:

- **Flexibility—**Companies, even within the same industry, are not identical. As designed, the proposed examination will be voluntary and principles-based. 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, 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 acceptance of the examination could aid in establishing a uniform, cross-industry approach to evaluating a company's cybersecurity risk management program

- **Innovative and sustainable solution—**The AICPA plans to adapt and advance the examination 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.