April 2017

AICPA

Cybersecurity risk management reporting

fact sheet

Acknowledgments

The AICPA's cybersecurity risk management reporting framework was developed by its Assurance Services Executive Committee's (ASEC) Cybersecurity Working Group for issuance by the ASEC and the AICPA's Auditing Standards Board (ASB).

The ASEC's mission is to support the ongoing relevance of the CPA profession by continuously exploring and addressing emerging market needs and demand for assurance and advisory services. Its focus is to continuously identify, assess and address significant developments and opportunities relating to emerging assurance and advisory needs, and to determine and execute on approach that is most responsive, including thought leadership, guidance and criteria, tools, or other support in furtherance of the public interest.

The ASB's mission is to serve the public interest by developing, updating and communicating comprehensive standards and practice guidance that enable practitioners to provide high-quality, objective audit and attestation services to nonissuers in an effective and efficient manner.

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 American Institute of CPAs (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 US 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*.

Role of the CPA

As a profession, we have decades of experience in providing information security services. Today, four of the leading 10 information security and cybersecurity consultants are public accounting firms. Auditors are experts at risk and control assessment.

Many public accounting firms already are providing cybersecurity advisory engagements, helping clients identify key risk areas, design and develop cybersecurity risk management programs, and assess the readiness of those programs. This is an opportunity for the profession to meet evolving market needs by combining its information security expertise with the discipline inherent in the external audit process. CPAs will be able to provide a cybersecurity risk management examination designed to meet the needs of a broad range of potential report users seeking relevant, useful information about an entity's cybersecurity efforts.

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 first component is a management-prepared narrative description of the entity's cybersecurity risk management program (the description). This description is designed to provide information about how the entity identifies its most sensitive information, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks. The description provides the context report users need to understand the conclusions, expressed by management in its assertion and by the CPA in the opinion, about the effectiveness of the controls included in the entity's cybersecurity risk management program.

2. **Management's assertion** — Management provides an assertion about whether the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the *control criteria*. (These criteria are discussed below.)

3. **The practitioner's opinion** — The final component in the reporting framework is the CPA's opinion on the description and on the effectiveness of controls within that program.

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. Use of common criteria enhances the comparability of entity-prepared communications about cybersecurity matters.

Management uses the description criteria when preparing a narrative description of the entity's cybersecurity risk management program (the description); it uses the control criteria when evaluating the effectiveness of the controls within the program.

Since 1997, the AICPA has maintained a set of criteria, used to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy over information and systems. Organizations 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. Organizations may use other criteria (such as the NIST Critical Infrastructure Cybersecurity Framework and ISO 27001/27002) as control criteria, 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, which will be published in the second quarter of 2017. The guide will assist CPAs on how to perform and report on cybersecurity risk management examinations, in accordance with the AICPA attestation standards.

While the performance and reporting guidance included in the guide related primarily to an entity-wide cybersecurity risk management program, it may also be helpful for a CPA engaged to report only on a portion of an entity's program (such as a division or business unit's program).

Because an examination involves an evaluation of the effectiveness of controls within the cybersecurity risk management program, many companies will find that they have not yet reached the necessary level of maturity to undergo a cybersecurity risk management examination. For that reason, the performance and reporting guidance in the cybersecurity guide may also be helpful to a CPA engaged to report only on the suitability of the design of the controls implemented within the program. The cybersecurity guide may also be helpful to a CPA engaged to provide cybersecurity advisory services to an organization. Such services may involve helping an organization improve its cybersecurity risk management program, including the design of better controls within that program. In addition, use of the description criteria and control criteria may assist management in establishing a common approach and language to use when communicating with their boards and other stakeholders about the entity's cybersecurity risk management efforts.

Related efforts

The cybersecurity risk management examination is part of the AICPA's suite of Service Organization Controls — or SOC — reporting. Through a SOC engagement, a CPA provides an opinion on a service organization's system controls (SOC 1, 2 and 3) or on entity-wide controls (SOC for cybersecurity).

In 2017, the AICPA also plans to release an updated version of the SOC 2® *Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, that will be revised for the clarified attestation standards and for the 2017 Trust Services Criteria on which the engagement is based.

Also in 2017, the AICPA will begin work on a new attestation engagement guide addressing supply-chain cybersecurity risk, which will enable CPAs to provide reports to customers of manufacturers and distributors on the processes and controls they have designed, implemented and operate to manage the cybersecurity risk in their supply chain and distribution networks. The vendor/supply chain guide is expected to be issued during 2018.

Both of these engagements will focus on system-level assurance, as opposed to the new cybersecurity risk management examination described in the preceding section, which is intended to cover cybersecurity risk at the entity level.

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,* 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.