April 2017

AICPA®

SOC for cybersecurity

a backgrounder

Acknowledgments

Special thanks to Francette Bueno, Senior Manager, Advisory Services, Ernst & Young LLP and Chris K. Halterman, Executive Director, Advisory Services, Ernst & Young LLP and Chairman of the AICPA's Trust/Information Integrity Task Force, for substantial contribution in developing this backgrounder on behalf of the AICPA's Assurance Services Executive Committee (ASEC).

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. In pursuit of this mission, the committee develops technical guidance and criteria, thought leadership, tools, and other deliverables to help members provide high quality, value-added, innovative assurance and advisory services to their clients and organizations.

Contents

Introduction

In recognition of the needs of management and boards of directors of diverse organizations, and for the benefit of the public interest, the American Institute of CPAs (AICPA) has developed a cybersecurity risk management reporting framework. Using it, organizations can communicate pertinent information regarding their cybersecurity risk-management efforts and educate stakeholders about the systems, processes and controls they have in place to detect, prevent and respond to breaches. The reporting framework also enables a CPA to examine and report on the management-prepared cybersecurity information, thereby increasing the confidence that stakeholders may place on an organization's initiatives.

Background

High-profile cybersecurity attacks compromising critical data of major corporations, governments, not-for-profits and private companies have brought attention to the business effects that a major breach at an organization can cause, including:

- Reputational damage
- Loss of intellectual property
- Disruption of key business operations
- Fines and penalties governments assess
- Litigation and remediation costs
- Exclusion from strategic markets

The risk of such effects has led to significant attention on cybersecurity by entity investors, customers, business partners and regulators. As a result, cybersecurity risk management has become a major business issue facing the senior management and boards of directors of most organizations.

Managing this business issue is especially challenging because even an organization with a highly mature cybersecurity risk management effort will still retain a residual risk that a material cybersecurity breach can occur and not be detected in a timely manner. Furthermore, the need for cybersecurity risk management is unlikely to change in the foreseeable future because of a combination of factors, including: organizations' dependency on information technology; the complexity of information technology networks; and the extensive reliance on third parties and human nature (e.g., susceptibility to social engineering).

Need for information to drive decision-making

Because of the importance of cybersecurity risk management, organization stakeholders are interested in obtaining useful information about it to enable them to make informed decisions. For example:

- Board members/directors need information about the cybersecurity risks an entity faces and the cybersecurity risk management program that management implements to help them fulfill their oversight responsibilities. They also want information from an independent third-party evaluator that will help them evaluate management's effectiveness in managing cybersecurity risks.

- Analysts and investors may benefit from information about an entity's cybersecurity risk management program. This information is intended to help them understand the entity's cybersecurity risks that could threaten the achievement of the entity's operational, reporting, and compliance (legal and regulatory) objectives and consequently, have an adverse impact on the business's value and stock price.

Business partners may benefit from information about an entity's cybersecurity risk management program as part of their overall risk assessment. This information is intended to help business partners determine matters such as whether there is a need for multiple suppliers for a good or service and the extent to which they choose to extend credit to the entity.

- Some industry regulators may benefit from information about an entity's cybersecurity risk management program to support their oversight role.

Accordingly, corporate directors and senior management have begun requesting reports on the effectiveness of their cybersecurity risk management programs from independent third-party assessors.

Disparate cybersecurity frameworks and standards create confusion

Today, there is no widely accepted approach or professional standard for providing security assessments; instead, the demand for effective organizational cybersecurity risk management and information on organizations' cybersecurity risk management efforts has led to the development of disparate cybersecurity frameworks and standards, including:

- Numerous risk management frameworks that provide guidance to organizations on how to manage cybersecurity risk (e.g., ISO/IEC 27001, NIST Cybersecurity Framework)
- A confusing array of control frameworks that specify compliance with a set of controls that should be implemented to reduce cybersecurity risk to an appropriate level (e.g., ISO/IEC 27002 NIST 800-53)
- Assurance programs intended to create confidence regarding the effectiveness of organizations' cybersecurity risk management programs in the minds of customers, business partners, investors and regulators (e.g., ISO/IEC 27001 certification)

The existence of such multiple, disparate frameworks and programs, and different stakeholders' preferences for each has created a chaotic environment that only increases the burden placed on organizations trying to design and implement an effective cybersecurity risk management programs.

A natural extension of the CPA role and specialized knowledge

The public accounting profession (i.e., CPAs) has long been active in assisting organizations in addressing information security and cybersecurity risk management.

Beginning in 1974, CPAs were required to consider the effects of information technology on financial statements during an audit of those statements. That requirement led to the development of system and organization control (SOC) reporting for service organizations (SOC 1® and SOC 2®). It also resulted in tremendous growth in the market for information security consulting services. Today, four of the leading 10 information security/cybersecurity consultants are CPA firms.

Information security and cybersecurity services that CPA firms offer are shown in the chart below:

Third-party reporting services	Cybersecurity governance advisory services	Information security/cybersecurity program advisory services
SOC for Service organization examination reports (e.g., SOC 1® and SOC 2® reports) • ISO 27001 certification • HITRUST assessment • Federal Information Security Modernization Act of 2014 reporting		
Cloud security advisory services	Information security/cybersecurity regulatory and compliance services	Security training services
Security policy development advisory services	Security threat management services	Security solution design and implementation services
Privacy advisory services	Managed security services	

Objective

The objective of the reporting framework is to provide a means by which organizations can communicate useful information regarding their cybersecurity risk-management programs to stakeholders and CPAs can examine and report on such information, thereby increasing the confidence stakeholders can place on such information.

The reporting framework, and in particular the cybersecurity report resulting from its use, is intended to:

- **Provide a common criteria for disclosures about an entity's cybersecurity risk management program** — Through the use of a common description criteria for disclosures about cybersecurity, the report reduces the information burden on organizations by providing a broad range of users with sufficient decision-useful information regarding the cybersecurity risk management efforts of an organization.
- **Provide a common criteria for assessing program effectiveness** — Prior to this reporting framework, independent assessments focused on the effectiveness of controls to meet a variety of disparate security control frameworks and standards. For managements that elect to use the trust services criteria for security, availability, and confidentiality as the control criteria, the cybersecurity report provides an independent assessment of the effectiveness of the entity's program controls in addressing cybersecurity risk.
- **Reduce communication and compliance burden on organizations** — The report reduces the number of information requests from stakeholders and the amount of information sought if such requests are made.
- **Provide useful information to a broad range of users, while minimizing the risk of creating vulnerabilities** — Information provided in the report would meet the shared needs of a broad spectrum of users.
- **Provide comparability** — The report would provide users with information that could be used to compare both with other organizations and for the same organization across time.
- **Permit management flexibility** — The framework would not constrain management to a particular security management framework or control framework.
- **Connect the dots on best practices** — The reporting framework should help management by enabling them to consider best practices encouraged by most commonly used control and cybersecurity frameworks, regardless of which framework(s) management has chosen to follow internally.
- **Be voluntary** — The framework should be sufficiently valuable to organizations and their stakeholders who would drive adoption in the marketplace.
- **Be scalable and flexible** — The framework should be useful to organizations of varying sizes and across all industries.
- **Evolve to meet changes** — The framework should be updated and modified over time based on experience, a changing environment and organization and stakeholder needs.

The intent of this framework is to support cybersecurity attestation engagements that meet the informational needs of a broad range of potential report users and to leverage the core competencies of CPAs as providers of examination-level services on such information in accordance with the Code of Professional Conduct and Professional Standards.

Process

The AICPA established a working group under the auspices of the Assurance Services Executive Committee (ASEC) to develop the reporting framework. The key steps undertaken by the working group included the:

- Identification of existing cybersecurity reporting frameworks
- Development of an approach to cybersecurity reporting
- Development of the contents of a description of an organization's cybersecurity risk-management program
- Identification of criteria for assessing whether the cybersecurity risk management program controls are effective
- Development of an illustrative description of an organization's cybersecurity risk management program
- Solicitation of feedback from key stakeholders, through a series of focus groups, presentations and exposure of criteria for public comment
- Publication of a cybersecurity attestation guide to provide practitioner with performance and reporting guidance for a cybersecurity examination

Three reporting levels

After analyzing the needs of users, the AICPA concluded that three separate types of reports were needed to address the information security reporting needs of market constituents. These reports are at three specific reporting levels:

Reporting levels	Intended audience	Benefit (entity and recipient)
Entity Description Opinion Assertion	• Board/audit committee • Management • Investor • Regulators • Analysis	• Provides transparency to key elements of the entity's cybersecurity risk management program • Improves communications • Enhances confidence in the integrity of the info presented
Service provider Testing Description Opinion Assertion	• Business unit management • Vendor risk management • Accounting/internal audit • CISO • BCP	• In addition to entity-level benefits, provide sufficient, detailed information to address the user vendor risk management needs
Supply chain Testing Description Opinion Assertion	• Business unit management • Vendor risk management • CISO • BCP	• In addition to entity-level benefits, provides sufficient, detailed information to address the user's supply chain risk management tools

The AICPA determined that the entity reporting framework should be developed first. The remainder of this document addresses the entity reporting framework. The AICPA is in the process of revising the SOC 2® guide for service organizations.
Once that project has been completed, the AICPA will develop a new supply-chain/vendor-risk management guide to address the supply-chain level.

Components of the entity-level cybersecurity reporting framework

The entity-level cybersecurity reporting framework provides three key sets of information that, taken together, are intended to meet the objectives discussed previously. They are:

1. **Management's description** — The first component is a management-prepared narrative description of the entity's cybersecurity risk-management program. This description is designed to provide information about how the entity identifies its sensitive information and systems, 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 information and systems against those risks.

   This provides the context needed to enable users to understand the conclusions management expressed in its assertion, and by the auditor in its opinion, about the effectiveness of the controls included in the entity's cybersecurity risk management program.

2. **Management's assertion** — Management makes 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. Both sets of criteria are discussed in the next section.

3. **The practitioner's opinion** — The final component in this approach is a CPA's opinion on the description and on the effectiveness of controls within that program to achieve the entity's cybersecurity objectives.

Two sets of criteria

To implement the reporting framework, the AICPA developed two sets of different but complementary criteria to be used in a cybersecurity engagement:

- Description criteria management uses when preparing a description of its cybersecurity risk management program and by the CPA when evaluating the presentation.

- Control criteria management uses when assessing the effectiveness of controls within that program to achieve the entity's cybersecurity objectives.

Management may select the criteria to use in the examination, as long as it is suitable in the circumstances.

The description criteria were formally exposed in late 2016. Because of concerns that the exposure process might not have resulted in comments from all-important classes of stakeholders, the AICPA, working with the Center for Audit Quality (CAQ), created a CAQ Cybersecurity Advisory Panel and sponsored a series of focus group sessions with representatives from key stakeholder classes.

In addition to the opinion on management's description of its cybersecurity risk management, the cybersecurity examination includes an opinion on the effectiveness of the cybersecurity controls. Since 1997, the AICPA has maintained a set of criteria used to evaluate the security, availability, processing integrity, confidentiality and privacy of entity systems. These criteria, known as the Trust Services Criteria, were revised for use as control criteria in the cybersecurity examination. The AICPA also formally exposed the revised trust services criteria in late 2016. Both sets of criteria were issued in April 2017.

In addition to the two sets of criteria, the AICPA Assurance Services Executive Committee (ASEC) Cybersecurity Working Group, working in conjunction with the AICPA Auditing Standards Board (ASB), has developed an attestation guide (referred to as the cybersecurity guide), which provides guidance to CPAs on how to perform cybersecurity examinations are in accordance with the AICPA attestation standards. This guide does not require the use of the AICPA developed description criteria and Trust Services Criteria as control criteria; rather, management and the auditor may use any suitable description criteria and control criteria. Publication of the cybersecurity guide is mid-May 2017.

Conclusion

The AICPA believes that an entity, its board of directors and its stakeholders will be best served if a defined set of information intended to meet their common needs addresses cybersecurity concerns. The information reported needs to be:

- Transparent
- Consistent across time
- Comparable between entities
- Reasonably complete
- Scalable
- Flexible

The cybersecurity examination could go far in meeting those information needs.