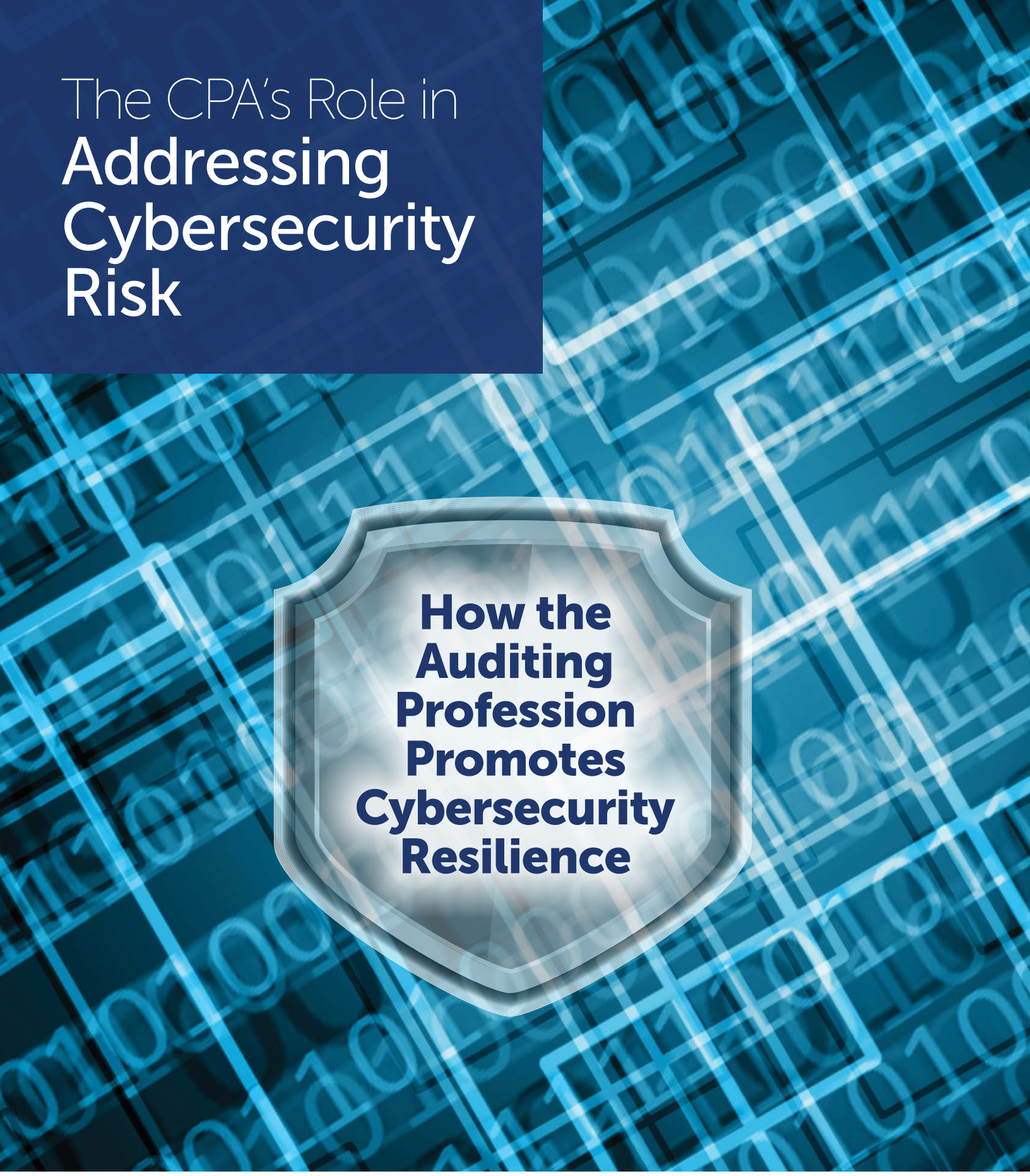
The CPA's Role in Addressing Cybersecurity Risk



How the Auditing Profession Promotes Cybersecurity Resilience

TEN YEARS
CENTER FOR AUDIT QUALITY

MAY 2017

Contents

1. Executive Summary

What is the nature of today's cybersecurity risks? What role do auditors play in cybersecurity, and how can that role evolve for the benefit of senior management, boards of directors, and other pertinent stakeholders? This publication provides perspective on these important questions.

As the discussion around cybersecurity has grown, so too has the Center for Audit Quality's engagement on the issue with key stakeholders, including auditors, audit committees, investors, insurance providers, financial executives, and regulators. These efforts have complemented the work of the American Institute of CPAs (AICPA) to develop a framework for cybersecurity risk management reporting.

THE CHALLENGING CYBERSECURITY LANDSCAPE

Cybersecurity brings extraordinary challenges. Organizations face varying threats with varying impacts—all in an environment marked by rapid technological change. What's more, various stakeholders must gather information and converse about cybersecurity between and among each other.

The nature of cybersecurity challenges requires that every sector of the economy play a role. While government policy and activity will be important in promoting cybersecurity resilience, the energy, agility, and innovation of the private sector must be harnessed as well. The auditing profession will do its part by playing a key role in helping organizations—public and private—adapt to this challenging landscape.

THE STRENGTHS OF AUDIT FIRMS IN ADDRESSING CYBERSECURITY CHALLENGES

In approaching cybersecurity, audit firms offer key strengths.

What is the nature of today's cybersecurity risks? What role do auditors play in cybersecurity, and how can that role evolve for the benefit of senior management, boards of directors, and other pertinent stakeholders?

This publication provides perspective on these important questions.

- **Core CPA values and attributes**: Adhering to core values of independence, objectivity, and skepticism, Certified Public Accountants (CPAs) are viewed by management and boards as trusted advisors who have a broad understanding of businesses, who receive appropriate annual training, who comply with a code of ethics, and who are subject to rigorous external quality reviews.
- **Experience in independent evaluations**: Audit firms have deep experience in independent evaluations, with the most common example being the financial statement auditor's opinions, required by US federal law for most public companies, on the audits of financial statements and internal control over financial reporting (ICFR). Additionally, most large- and mid-sized CPA firms have built substantial information technology (IT) practices that provide attestation and advisory services to entities on IT security-related matters and the effectiveness of IT security controls.

- **Multidisciplinary strengths**: Today's public accounting firms employ individuals with CPAs as well as other credentials specifically related to information technology and security. These include Certified Information Systems Security Professionals (CISSP), Certified Information Systems Auditors (CISA), and Certified Information Technology Professionals (CITP). Indeed, four of the leading 13 information security and cybersecurity consultants are CPA firms.[1]

THE CYBERSECURITY RISK MANAGEMENT REPORTING FRAMEWORK

The AICPA has developed an entity-level cybersecurity reporting framework through which organizations can communicate useful information about their cybersecurity risk management program to a broad range of stakeholders, including boards of directors, senior management, investors, and others.

The reporting framework consists of three key components that will assist stakeholders in monitoring an entity's cybersecurity risk management program.

- The first is **Management's Description** of the entity's cybersecurity risk management program based on suitable criteria for management to describe its cybersecurity risk management program.
- The second is **Management's Assertion** to the presentation of their description and that the controls management implemented are operating effectively to achieve the entity's cybersecurity objectives.
- The third component in this approach is the **CPA's Opinion** on that description and the effectiveness of the controls to meet the entity's cybersecurity objectives.

This reporting framework will 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.

1 See Martin Whitworth, "Information Security Consulting Services, Q1 2016," The Forrester Wave (January 2016).

2. The Landscape of Cybersecurity Risk

THE NEED TO FOSTER CONVERSATIONS AMONG VARIED STAKEHOLDERS

Given the high-profile nature of cyber-attacks on corporations, both the demand for information related to cybersecurity—and the need to facilitate robust conversations on these topics—have grown exponentially across major stakeholder groups.

- **Board members**: Boards of directors need information about the entity's cybersecurity program and the cyber threats facing the entity to help the boards fulfill their oversight responsibilities. They also want information that will help them evaluate the entity's effectiveness in managing cybersecurity risks.

- **Investors**: When making investment decisions, analysts and investors need information about an entity's cybersecurity measures. This information can help them understand the cybersecurity risk that could threaten the achievement of the entity's operational, reporting, legal, and regulatory objectives—which each can have implications for an entity's market value.

- **Regulators**: Regulators may benefit from information about an entity's cybersecurity risk management program to support their oversight role.

- **Business partners**: Business partners may need information about the entity's cybersecurity risk management program as part of its overall risk assessment. This information can help them determine matters such as the entity's ability to provide goods/services in the event of a disruption to its IT systems.

VARIED THREATS

Many organizations that transact business today are susceptible to a cybersecurity breach. Why? One key reason is that cybersecurity threats emerge from a diverse and growing number of sources.

- **Cybercriminals** seek to steal data from organizations to use it for quick, unlawful financial gain.

- **Nation-states** may launch cyber-attacks to conduct economic espionage or to fulfill geopolitical objectives (or both).

- **Employees**, unfortunately, are all too often a source of compromised security access. Even when organizations and employees have the best of intentions, unintentional security lapses can occur when employees use basic passwords or succumb to phishing emails and other seemingly genuine correspondence. These types of internal threats heighten the need for better internal controls, training, and monitoring of compliance within an organization's own system.

Complicating all these threats is the fact that technology continues to evolve rapidly. As organizations have hardened their security defenses, adversaries have shifted to new tactics and targets, requiring organizations to continuously evolve their cybersecurity risk management programs.

As threats multiply and technology evolves, the consequences for stakeholders vary in turn. For investors, consequences of a cybersecurity breach can include loss of business or public trust that can reduce the value of their investment. Customers and business partners

may face denial of access to products and services due to an attack or have to grapple with disclosure of their confidential information.

VARIED RESPONSES

Previously, most companies relegated all things "cyber" to the IT department. Today, the trend has shifted, and C-suites and boards of directors are increasing their oversight and accountability for cyber risk. As recognition grows that cyber risks also come from personnel practices, supply chain management, and operational decisions, a more enterprise-wide approach to managing these risks is evolving. Senior management, with board oversight, is taking on more of the challenging work of developing a comprehensive cybersecurity risk

Frameworks as Foundation

FRAMEWORKS TO ASSIST MANAGEMENT IN IMPLEMENTING AND EVALUATING A CYBERSECURITY RISK MANAGEMENT PROGRAM

- **National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity**.[2] A 2013 Presidential Executive Order called for the creation of a voluntary, risk-based cybersecurity framework that would provide a set of industry standards and best practices for all organizations. The resulting NIST framework came together with collaboration between industry and government. Organizations can turn to the C³ Voluntary Program, which was created to help organizations use the NIST Cybersecurity Framework to improve their cyber resilience.[3] According to the United States Computer Emergency Readiness Team, the program connects organizations with public and private sector resources that align to the NIST Framework's five functional areas: Identify, Protect, Detect, Respond, and Recover.

- **ISO/IEC 27001/27002**.[4] Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), this group of standards is intended to be used as guidance for securing financial information, intellectual property, employee data, and other information entrusted to the organization by third parties.

- **SEC Cybersecurity Guidelines**.[5] The SEC has published cybersecurity guidance for registered investment companies and investment advisers, including steps to consider to address cyber risk.

- **Trust Services Criteria (TSC)**.[6] The TSC align to the 17 principles presented in COSO Internal Control—Integrated Framework.[7] The TSC, as developed by the AICPA's Assurance Services Executive Committee, are designed for use in evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity, a division, or an operating unit of an entity or a particular type of information processed by one or more of an entity's system(s) or one or more systems used to support a particular function within the entity.

2 See National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." (2014) Available at https://www.nist.gov/sites/default/files/documents/cyberframework/ cybersecurity-framework-021214.pdf.

3 See https://www.us-cert.gov/ccubedvp/cybersecurity-framework.

4 See http://www.27000.org/.

5 See US Securities and Exchange Commission, Division of Investment Management. "IM Guidance Update: Cybersecurity Guidance." (2015) Available at https://www.sec.gov/investment/im-guidance-2015-02.pdf.

6 See AICPA. TSP Section 100: "2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy."

7 Changes in technology were among the reasons that COSO chose to replace its original 1992 framework with the updated 2013 framework that addresses controls.

management program, including an effective internal control structure that responds to the identified threats and the evolving cybersecurity risk environment.

As management and boards endeavor to determine their responsibilities related to cybersecurity, many organizations are still working to find the most comprehensive and effective cybersecurity risk management structure. Just a few years ago, management and boards had limited resources in designing a framework for risk identification, response, control design and implementation, assessment, and recovery. Now, there are several leading frameworks (see sidebar, "Frameworks as Foundation" on page 4), as well as numerous standards, methodologies, and processes that have been put forth by federal and state governments, industry specific groups, independent agencies, and other stakeholders.

These frameworks exist to aid companies in designing cybersecurity controls specific to cybersecurity risks. As discussed in greater detail in chapter 4 of this paper, the AICPA's cybersecurity reporting framework facilitates the ability of a company to describe, in a common language, their enterprise-wide cybersecurity risk management program.

THE NEED FOR A ROBUST PRIVATE SECTOR ROLE IN CYBERSECURITY

Cybersecurity is an issue with national security implications. As both public and private sectors grapple with the issue, the dynamic, free-market system can serve as a potent weapon. Improvements driven by the private sector significantly increase the opportunity to produce meaningful and timely improvements in current practices.

After all, even companies within the same industry are not identical. Hence, companies and stakeholders can benefit from a means to evaluate cybersecurity risk management in a manner tailored to their particular situation—and the evolving cybersecurity threats they face.

3. How CPAs Promote Cybersecurity Resilience

Given the immense scale and complexity of the cybersecurity challenge, every sector of the economy must do its part to promote cybersecurity resilience. With its core values and history of providing independent assessments in a variety of contexts—including information technology—the CPA profession has a critical role to play.

A LONG HISTORY OF STRONG VALUES AND RIGOROUS STANDARDS

To understand the CPA's role, one must start with the fundamental principles and standards of performance that have defined the accounting and auditing profession for over 125 years.

- Independence, objectivity, and skepticism are core CPA values.
- A CPA must have adequate and continuous technical training to perform an attest engagement.
- The CPA must have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users.
- Personnel working on an attest engagement must also exercise due professional care in the planning and performance of the engagement and the preparation of the report.

BRINGING TO BEAR DEEP EXPERIENCE IN IT SECURITY

Public accounting firms began building specialized IT audit practices in the early 1970s to address the risks that IT represented to accounting information. Over the years, firms have expanded these practices to address areas beyond the IT controls necessary for accounting systems. As a result, many firms now offer services which focus on IT controls that address the risks to the security, availability, and confidentiality of an entity's information and systems.

Today, large- and mid-sized CPA firms have thousands of IT security and audit specialists around the globe who focus on providing services to entities on IT security-related matters and provide reports on the effectiveness of IT security controls.

SETTING EXPECTATIONS: CYBERSECURITY AND THE FINANCIAL STATEMENT AUDIT

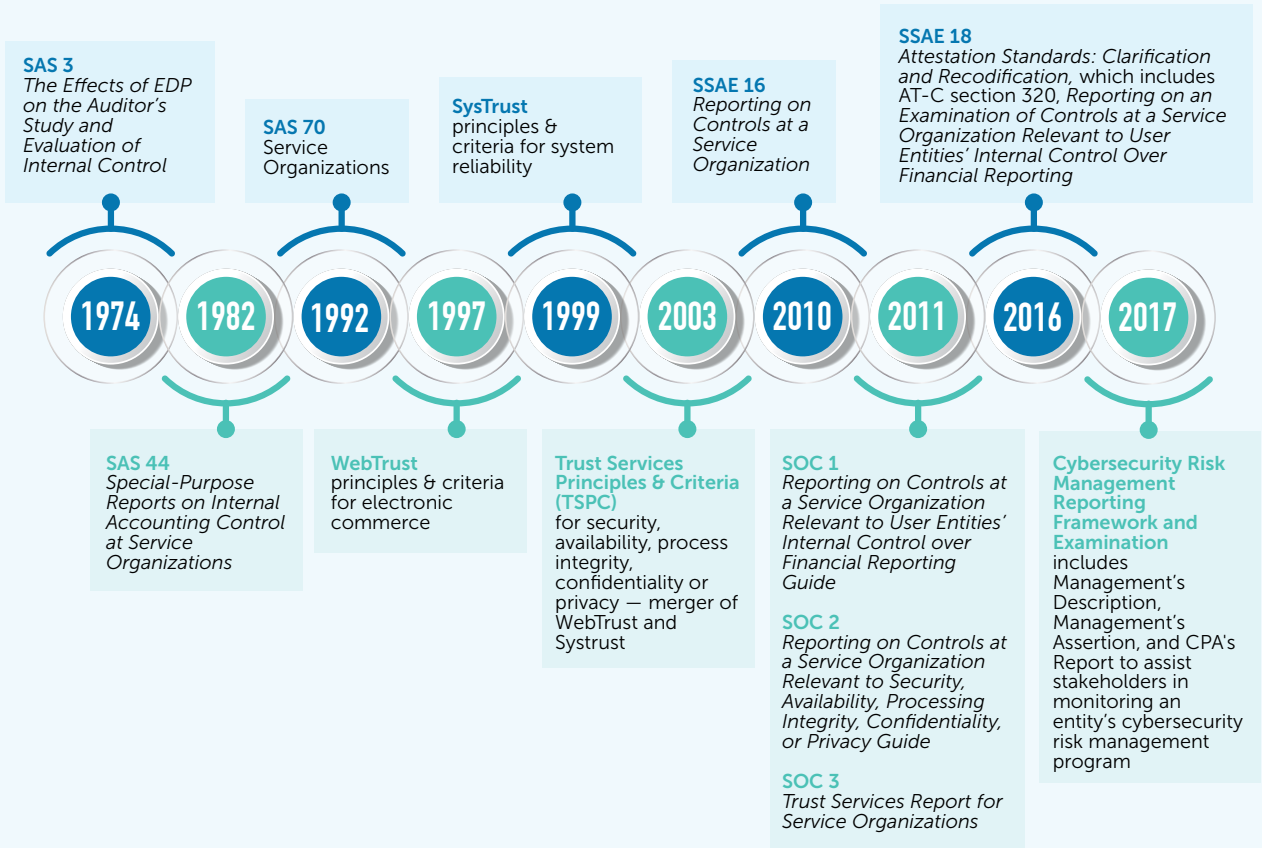
The most common example of an objective evaluation is the financial statement auditor's independent opinions on the audits of financial statements and ICFR. The Sarbanes-Oxley Act of 2002 (SOX) added a requirement, applicable to most public companies, that management annually assess the effectiveness of the company's ICFR and report the results to the public. In addition, SOX requires the audit committee of most large public companies to engage an independent auditor to audit the effectiveness of the company's ICFR.

It is important to understand cybersecurity considerations for the financial statement auditor in two key contexts: (1) the audits of financial statements and ICFR (where applicable) and (2) disclosures.[8]

8 According to Section 404(b) of the Sarbanes-Oxley Act, an ICFR audit "shall not apply with respect to any audit report prepared for an issuer that is neither a 'large accelerated' nor an 'accelerated' filer as defined in Rule 12b-2 of the Commission."

The CPA's Involvement with Auditing IT Controls

As shown in this timeline, auditors have been engaged to assess IT controls for decades. The new cybersecurity examination would be a continuation and outgrowth of this capability.



Source: AICPA

The financial statement auditor's procedures on controls in a financial statement audit cover only those controls that relate to financial reporting. Any cybersecurity controls that are a part of ICFR would only represent a subset of the company's enterprise-wide cybersecurity controls.

Under current guidance, a company may determine it is necessary to disclose cybersecurity risks in various places throughout its Form 10-K (e.g., risk factors, management's discussion and analysis, legal proceedings, business description, and/or financial statements). The financial statement auditor's responsibilities depend on whether the disclosure is included in the audited financial statements or elsewhere in the Form 10-K.

If the disclosure is in the financial statements, the financial statement auditor performs procedures to assess whether the financial statements taken as a whole are presented fairly in accordance with generally accepted accounting principles, in all material respects. Included in the financial statement auditor's assessment are procedures specific to the financial statement disclosures. For example, if a company had a material contingent liability for an actual cyber incident, in addition to performing audit procedures related to the reasonableness of the

liability recorded, if any, the financial statement auditor would also assess whether the disclosures in the footnote related to that liability were appropriate as it relates to the financial statements taken as a whole.

For cybersecurity risks that are included elsewhere in the Form 10-K, the financial statement auditor is not required to perform procedures to corroborate that information. Rather, the financial statement auditor reads this information and considers whether the information, or the manner of its presentation, is materially inconsistent with information appearing in the financial statements or a material misstatement of fact.[9]

Cybersecurity and Audits of Financial Statements and ICFR

Cybersecurity risks and controls are within the scope of the financial statement auditor's concern only to the extent they could impact financial statements and company assets to a material extent.

Auditing standards require the financial statement auditor to obtain an understanding of how the company uses IT and the impact of IT on the financial statements.

Financial statement auditors also are required to obtain an understanding of the extent of the company's automated controls as they relate to financial reporting, including the IT general controls that are important to the effective operation of automated controls, and the reliability of data and reports used in the audit that were produced by the company.

In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access and unauthorized use or disposition of company assets—financial statement auditors are required to take into account their understanding of the company's IT systems and controls.

If information about a material breach is identified, the financial statement auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR.

The financial statement auditor uses a top-down approach to the audit of ICFR to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to ICFR. The financial statement auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the financial statement auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements, including related disclosures.

Systems and data that are within the scope of most audits usually are a subset of the totality of systems and data used by companies to support their overall business operations. The auditor's focus is on access and changes to systems and data that could impact the financial statements and unauthorized use and disposition of assets; that is, matters within the defined boundary of ICFR.

A company's overall IT platform includes systems and related data that not only address financial reporting needs, but also operational and compliance needs of the entire organization. The financial statement auditor's primary focus is on the controls and systems that are in the closest proximity to the application data of interest to the financial statement and ICFR audit—that is, systems and applications that house financial statement-related data. It is important to note that cyber incidents usually first occur through the perimeter and internal network layers, which tend to be further removed from the application, database, and operating systems that are typically included in access control testing of systems that affect the financial statements.

9 PCAOB Auditing Standard 2710: Other Information in Documents Containing Audited Financial Statements.

4. Fostering Cybersecurity Conversations: A Cybersecurity Reporting Framework

The AICPA's cybersecurity reporting framework has been developed to provide the market with a common approach to reporting on and evaluating a company's cybersecurity risk management program. 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.

KEY COMPONENTS OF THE REPORTING FRAMEWORK

This reporting framework represents a major step forward in addressing cybersecurity challenges. The reporting framework provides the user with three key pieces of information that, taken together, can greatly enhance the confidence that a user can place on the cybersecurity information provided by management.

- **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

Of course, the Examination cannot prevent a cybersecurity threat or breach, nor is it designed to. It can, however, add substantial credibility to assertions made by management about their cybersecurity risk management program to protect information and data, thereby increasing stakeholder confidence.

for CPAs in evaluating the description. The AICPA's Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program (Description Criteria) has been designed to be suitable criteria. 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

Objectives of the AICPA's Reporting Framework

The AICPA's reporting framework for cybersecurity risk management was designed to enable organizations to communicate useful information regarding their cybersecurity risk management programs to stakeholders. The AICPA's framework seeks to:

- **Provide 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 cybersecurity risk management efforts of an organization.
- **Provide 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 management 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** — The framework 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 provides 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 cybersecurity description or control framework.
- **Connect the dots on best practices** — The framework enables management to consider best practices encouraged by most commonly used control and cyber frameworks regardless of which framework(s) management has chosen to follow internally.
- **Be voluntary** — The framework is valuable to organizations and their stakeholders to drive adoption in the marketplace.
- **Be scalable and flexible** — The framework is useful to organizations of varying sizes and across all industries.
- **Evolve to meet changes** — The framework will be updated and modified over time based on marketplace adoption, a changing environment, and organizational and stakeholder needs.

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 opinion.

- **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. One example of suitable control criteria is the 2017 Trust Services Criteria (criteria for security, availability, and confidentiality).
- **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 achieve the entity's cybersecurity objectives.

The cybersecurity reporting framework is objectives-based and voluntary. Companies do not need to implement all three components of the framework at once. For example, management may decide to only provide Management's Description of the entity's

cybersecurity risk management program. Based upon the needs of a company and its stakeholders, management and or the board of directors may take a phased approach to implementing each of the components of the reporting framework. For example, management or the board of directors may engage a CPA to examine and report only on the description and the suitability of design of controls. In the design-only examination, the CPA does not perform procedures to examine and report on the operating effectiveness of the entity's cybersecurity controls.

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 committee—to enable decision making, it is not enough to provide them merely with information. Decision makers need confidence in the cybersecurity information prepared and presented by management. The third component of 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 (the Examination): a new, comprehensive service that can only be performed by an independent, licensed public accounting firm to provide an opinion on Management's Description and on the effectiveness of the controls implemented as part of the cybersecurity risk management program.[10]

Of course, the Examination cannot prevent a cybersecurity threat or breach, nor is it designed to. It can, however, add substantial credibility to assertions made by management about their cybersecurity risk management program to protect information and data, thereby increasing stakeholder confidence.

The reporting framework and its accompanying Examination would be separate and apart from the existing financial statement audit process discussed in chapter 3.

AN EMPHASIS ON FLEXIBILITY

The cybersecurity reporting framework, including the Examination that the AICPA has developed, is entirely voluntary on the part of companies and audit firms. It provides flexibility in the sense that management and the auditor can choose to reference any suitable description and control criteria in the performance of the Examination.

STEPS IN AN EVOLUTION

The intent of the cybersecurity risk management framework is ultimately to support the voluntary Examination-level 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 these services in accordance with professional standards.

Some companies may not have reached the necessary level of maturity in their cybersecurity risk management to undergo an attestation engagement. For those companies, the framework can be utilized for non-attestation cybersecurity engagements—such as readiness engagements—and used directly by company management in communicating with their boards and investors, establishing a common approach and language for cybersecurity risk management and reporting.

10 The professional standards that govern these engagements are codified within AT-C Section 205, Concepts Common to All Attestation Engagements (AT-C-205) of the AICPA's professional standards. These standards detail the requirements for CPAs performing certain attest engagements outside the mandated audit.

5. FAQs: The Cybersecurity Risk Management Examination

AVAILABILITY

1. When will the Cybersecurity Risk Management Examination be available? What could companies do to prepare for the Examination?

CPA firms can start offering the Examination as of the release of AICPA's cybersecurity reporting framework in 2017. Check with your CPA firms to discuss availability.

Whether or not a company decides to have the Examination performed, the AICPA's Description Criteria and Trust Services Criteria, would provide companies and stakeholders a common language and approach to describing and assessing cybersecurity risk management. In addition to the guidance for CPAs, the AICPA is planning on publishing a companion document that explains the Examination for management and discusses management's responsibilities during such an engagement.

SCOPE OF THE ENGAGEMENT

2. Is the Examination voluntary?

Yes, the Examination is voluntary. If company management or a board of directors elects to have the Examination performed, the frequency of the Examination is also at the discretion of the engaging party.

CPA firms will choose whether they offer this service.

3. Is the scope of the Examination flexible?

Yes, the Examination can be performed on the entity-wide cybersecurity risk management program or on that of a division, business unit, or one or more specific types of information used by the entity.

4. Could a company use the same CPA firm for both the Examination and the financial statement audit?

Yes, the Examination could be considered a permissible service for financial statement auditors and in fact requires the CPA firm to meet independence requirements similar to those required for financial audits. It would require pre-approval from the audit committee for public companies and certain other entities subject to SEC independence rules.

5. What is the skillset of the engagement team that will provide this Examination? Do they need to have the technical expertise in cybersecurity to perform risk assessments and validate controls specific to cybersecurity?

The public accounting profession has decades of experience in providing information security services. Four of the leading 13 information and cybersecurity consultants are public accounting firms.[11] Auditors are experts at risk and control assessments—and have "boots on the ground" close to controls—which can yield efficiency gains when it comes to evaluation of a cybersecurity risk management framework.

Many public accounting firms are already providing cybersecurity advisory engagements, helping clients to identify key risk areas, to design and develop cyber risk management programs, and to assess cyber-readiness. There is an opportunity for the profession to meet evolving market needs by bringing a multi-disciplinary team that includes subject matter expertise and combining it with the discipline inherent in the external audit community, through an independent cybersecurity Examination.

MANAGEMENT'S DESCRIPTION

6. What is included in Management's Description?

Management's Description is intended to provide readers with information that will help them understand the entity's cybersecurity risks and how it manages those risks.

Key components of the AICPA's Description Criteria include:

Nature of Business and Operations. Disclosures about the nature of the entity's business and operations.

Nature of Information at Risk. Disclosures about the principal types of sensitive information the entity creates, uses, and stores that is susceptible to cybersecurity risk.

Cybersecurity Risk Management Program Objectives. Disclosures about the entity's principal cybersecurity objectives related to availability, confidentiality, integrity of data, and integrity of processing and the process for establishing, maintaining, and approving them.

Factors that Have a Significant Effect on Inherent Cybersecurity Risks. Disclosures about factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) environmental, technological, organizational, and other changes during the period covered by the description at the entity and in its environment.

Cybersecurity Risk Governance Structure. Disclosures about the entity's cybersecurity risk governance structure, including the processes for establishing, maintaining, and communicating integrity and ethical values, providing board oversight, establishing accountability, and hiring and developing qualified personnel.

Cybersecurity Risk Assessment Process. Disclosures related to the entity's process for (1) identifying cybersecurity risks and environmental, technological, organizational, and other changes that could have a significant effect on the entity's cybersecurity risk management program; (2) assessing the related risks to the achievement of the entity's cybersecurity objectives; and (3) identifying, assessing, and managing the risks associated with vendors and business partners.

Cybersecurity Communications and the Quality of Cybersecurity Information. Disclosures about the entity's process for communicating cybersecurity objectives, expectations, responsibilities, and related matters to both internal and external users, including the thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both.

11 See Martin Whitworth, "Information Security Consulting Services, Q1 2016," The Forrester Wave (January 2016).

Monitoring of the Cybersecurity Risk Management Program. Disclosures information related to the process the entity uses to assess the effectiveness of controls included in its cybersecurity risk management program, including information about the corrective actions taken when security events, threats, vulnerabilities, and control deficiencies are identified.

Cybersecurity Control Processes. Disclosures about (1) the entity's process for developing a response to assessed risks, including the design and implementation of control activities; (2) the entity's IT infrastructure and its network architectural characteristics; and (3) the key security policies and processes implemented and operated to address the entity's cybersecurity risks.

Please see the AICPA's website for more details on the Description Criteria and the illustrative Management's Description at: www.aicpa.org/cybersecurityriskmanagement.

7. Is it a requirement that the report be made publicly available?

The company, in consultation with their auditors, will decide whether it is appropriate in each case to make the report publicly available. The CPA guidance includes a sample Management Description that should help balance the need for a robust description, while not providing a roadmap for bad actors.

8. Many companies leverage the use of security service providers in their IT environment and cybersecurity risk management program. How will the use of security service providers impact Management's Description and the CPA's Opinion?

If the processes and controls performed by the security service providers are material to the achievement of the cybersecurity objectives, management should include the services in its Management's Description (for example, a summary of the controls performed by the service provider) and have a reasonable basis for relying on the services. Such a basis for reliance may include performing monitoring activities over the service provider or obtaining a Service Organization Control Reporting SOC 2® Examination report on the services.

9. Many companies leverage vendors or business partners (VBPs) as part of doing business. Would controls related to VBPs be in scope for the engagement?

If the entity has identified cybersecurity threats and vulnerabilities arising from interactions with a VBP, the entity needs to consider them in designing its cybersecurity risk management program. For example, vendors or business partners may have access to one or more of the entity's information systems, store confidential entity information on their systems, or otherwise transmit information back and forth between the entity and the VBP's employees. In these situations, the entity will likely need to implement monitoring activities related to the VBP and those activities would be evaluated as part of the Examination of the cybersecurity risk management program.

Additionally, the AICPA is developing separate guidance covering examinations related to vendor/supply chain risk management which is expected to be issued in 2018. Guidance for SOC 2® is expected to be issued in late 2017.

EXAMINATION AND CPA'S REPORT

10. What standards and frameworks will be used in the Examination?

This new cybersecurity risk management Examination engagement will be performed in accordance with clarified AICPA attestation standards. Those standards require that management be accountable for what is contained in the report.

In the case of the cybersecurity Examination, the report's subject matter will include: (1) a description of the entity's cybersecurity risk management program prepared in accordance with suitable description criteria; and (2) an assessment of the effectiveness of the controls in a cybersecurity risk management program based on suitable control criteria. Management and the auditor may choose any suitable criteria to be used in the engagement, however the AICPA has developed two distinct—yet complementary—sets of criteria to support the cybersecurity risk management Examination engagement.

The management-prepared narrative description of the entity's cybersecurity risk management program is designed to provide information about how the entity identifies its information assets, 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, thereby giving users comparable information for decision making, regardless of which framework(s) they have chosen to implement internally.

In addition to the opinion on whether Management's Description is presented in accordance with the description criteria, the examination engagement will include an opinion that the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. These control criteria, known as the Trust Services Criteria, have been updated for use in the Examination.

11. There is generally significant value in the substantive discussions audit committees and others at the company have with the external auditors as they complete their financial statement audits. Will the guidance for the cybersecurity risk management Examination prescribe similar required communications with the audit committee as public company audit standards do for the financial statement audit?

The attestation standards do not include required communications from the auditor performing the Examination to the audit committee or the board of directors. However, that does not preclude the auditor from providing observations related to the Examination. Any communications regarding the Examination will be made to the engaging party. In most cybersecurity Examination engagements, management is both the engaging party (client) and the responsible party; thus, management will accept responsibility for the subject matter (that is, management's description of the entity's cybersecurity risk management program and a conclusion about the effectiveness of the controls within that program). In some engagements, however, the engaging party may be someone other than management. For example, in a proposed acquisition, the engaging party might be the party interested in acquiring the entity. As part of its due diligence on the target company, the engaging party might want information about the entity's cybersecurity risk management program to evaluate the additional risks it might be taking on in the event of a security breach at the entity. If that evaluation is outside the audit committee, then the information would flow to the audit committee (or board) from the party most directly responsible for engaging the auditor.

12. Some management teams spend significant time supporting projects to comply with various state, industry, and other regulatory cyber requirements. Could this report help meet other regulatory cyber requirements?

One of the objectives of this Examination is to reduce communication and compliance burdens. The reporting framework could reduce the number of information requests from stakeholders and the amount of information sought, if such requests are made.

COST

13. Many company's cybersecurity risk management programs are extremely complex. Generally, the more complex the engagement, the larger the engagement fees. How expensive will this service be?

Due to the varied complexity and maturity of companies' IT environments, auditors will work with the audit committee and company management to understand the desired scope of the engagement. The fee will be dependent upon that scope and corresponding level of effort.

ABOUT THE CAQ

The Center for Audit Quality (CAQ) is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high quality performance by public company auditors, convenes and collaborates with other stakeholders to advance the discussion of critical issues requiring action and intervention, and advocates policies and standards that promote public company auditors' objectivity, effectiveness, and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs. For more information, visit www.thecaq.org.

ABOUT THE AICPA

The American Institute of CPAs (AICPA) is the world's largest member association representing the accounting profession, with more than 418,000 members in 143 countries, and a history of serving the public interest since 1887. AICPA members represent many areas of practice, including business and industry, public practice, government, education and consulting. The AICPA sets ethical standards for the profession and U.S. auditing standards for private companies, nonprofit organizations, federal, state and local governments. It develops and grades the Uniform CPA Examination, and offers specialty credentials for CPAs who concentrate on personal financial planning; forensic accounting; business valuation; and information management and technology assurance. Through a joint venture with the Chartered Institute of Management Accountants, it has established the Chartered Global Management Accountant designation, which sets a new standard for global recognition of management accounting.

CONTACT THE CAQ

The CAQ welcomes feedback and questions regarding this paper and the auditor's role in addressing cybersecurity risk.

Please contact:
Catherine Ide, CPA
Senior Director of Professional Practice
cide@thecaq.org
(202) 609-8054

WE WELCOME YOUR FEEDBACK

Please send comments or questions to info@thecaq.org.

THECAQ.ORG

WE WELCOME YOUR FEEDBACK Please send comments or questions to info@thecaq.org.