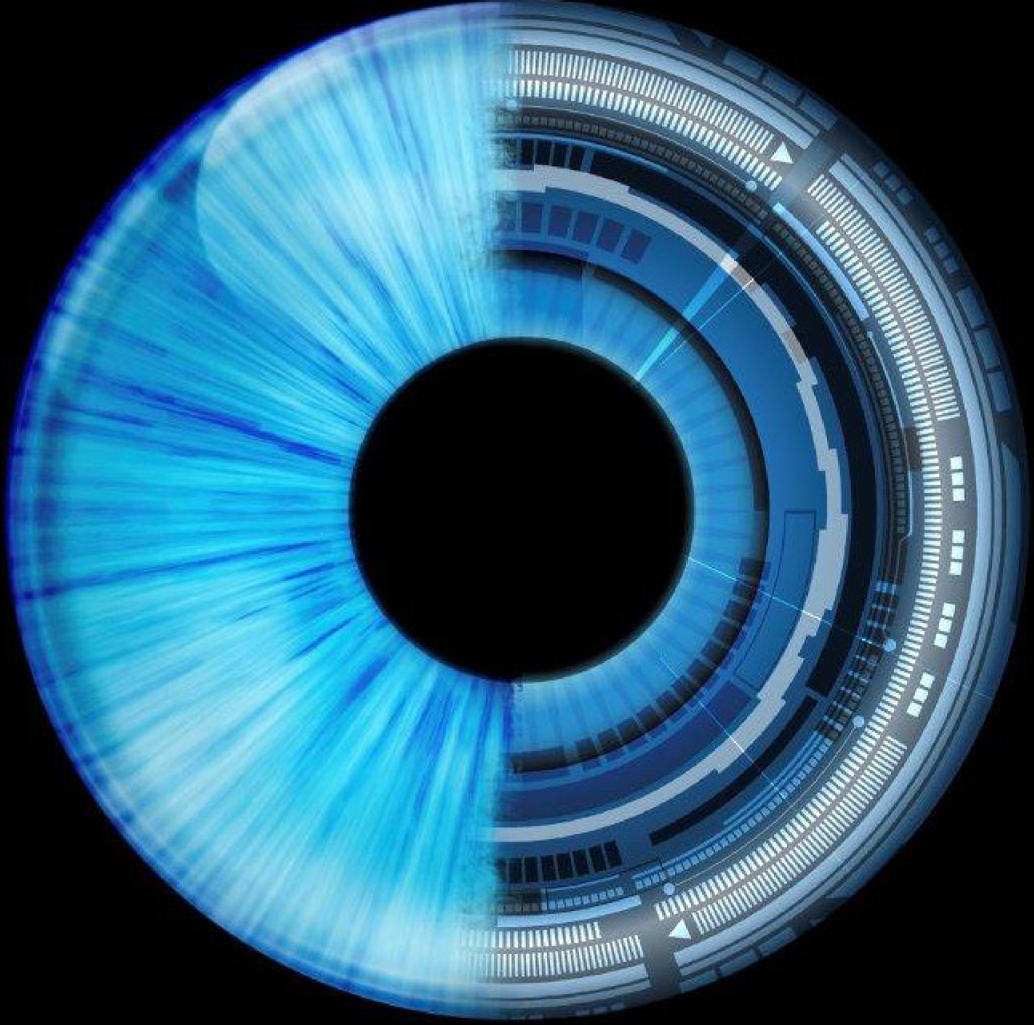
Deloitte.



Focusing the lens on cyber reporting

The AICPA cybersecurity risk management examination one year later

Contents

Introduction

The cyber risks associated with operating in an interconnected, digital world are well known. Recent headlines demonstrate how rough the ride can be if these risks are not managed effectively, as company after company have been reluctantly thrust into the spotlight as a result of security breaches and incidents. The expectations of boards, executives, and other stakeholders continue to mount, especially in the wake of recent regulations and guidance, such as the statement and interpretive guidance from the Securities and Exchange Commission (SEC) related to cybersecurity disclosures. This raises two important questions: how do organizations know if their cybersecurity controls are truly effective and how can they demonstrate the efficacy of their cybersecurity risk management programs to the stakeholders who are demanding greater transparency?

More than a year ago, on April 24, 2017, the American Institute of Certified Public Accountants (AICPA) released its cybersecurity attestation reporting framework to help organizations focus the lens on cyber reporting and answer the questions being posed by board members and other stakeholders. The AICPA framework provides a standardized, yet flexible, blueprint for evaluating, reporting, and communicating the effectiveness of an organization's cybersecurity risk management program down to the control level. It also promotes independent and objective assurance from a third party, inspiring greater confidence among recipients of the report. While it is a voluntary solution designed to enhance public trust in reporting over the effectiveness of an entity's cybersecurity risk management program, the AICPA's framework can be applied to any cybersecurity control structure that management has adopted as long as the criteria are appropriate in accordance with the AICPA's attestation standards.

Year in review

On its one-year anniversary, the AICPA cybersecurity attestation reporting framework is more relevant than ever. Companies across all industry sectors are continually being asked about the state of their cybersecurity risk management programs, and they need a more efficient way to answer the onslaught of inquiries.

Over the last year, organizations have discussed the merits of the framework, including its ability to reduce the reporting burden, promote comparability, and fulfill the long sought-after mantra of "test once and satisfy many." They have also debated the best ways to implement it, and some have embarked on readiness activities to prepare for a future attestation. The framework has even assumed a few aliases along the way, including "SOC for Cybersecurity," "Cybersecurity Examination," and "Cyber Attestation." But, no matter what you call it, the AICPA cybersecurity attestation reporting framework is now on the radar for many organizations. Growing awareness of the framework across industries and business models implies the time is right to share some lessons learned, common misconceptions, and insights from the front lines.

It's all about the crown jewels

The first step in meeting the raised bar on cybersecurity reporting set by the AICPA is to identify the organization's most critical information technology (IT) assets or "crown jewels." These could be physical or logical assets, and range from a few lines of code to customer master data encompassing millions of records. It is no surprise that an effective cybersecurity risk management program needs to take a risk-based approach and focus on what's important if it is going to be effective. What has been a surprise to many is what a challenge this presents. "What and where are the crown jewels?" may sound like a simple question, but it is deceptively difficult to answer. Even organizations that view themselves as having mature cyber programs often cannot answer this question clearly and concisely. Nonetheless, it cannot be side-stepped when designing and measuring the effectiveness of a cybersecurity risk management program.

Taking a thorough inventory of IT assets and assigning criticality is often the first challenge that needs to be addressed in identifying and locating the crown jewels.

Common questions to ask include:

- Of everything we have, what could prevent us from satisfying customer and shareholder expectations if it were lost or stolen?
- Does our asset discovery process reach into every corner of the enterprise? Are there applications we don't know about?
- Do we have information maintained outside of the four walls of our organization hosted by vendors, business partners, or other third parties?

Once a complete and accurate inventory has been established, the next step involves determining the business context and quantifying the inherent risk:

- Does the organization use a common taxonomy for assessing risk?
- Are there legal and compliance requirements associated with the information assets that have been identified?
- Do you have appropriate resiliency procedures in place to respond and recover from a cyber event in a timely manner that minimally disrupts business operations?

Answering questions such as these can help to quantify and contextualize the risk as well as to establish the scope of the cybersecurity risk management examination.

> “Understanding where critical data resides is a key to being able to protect the company’s crown jewel assets.”
>
> —Maria Filipakis | Former New York State Department of Financial Services Executive Deputy Superintendent, Capital Markets Division

Assessment vs. attestation

One common misconception about the cybersecurity attestation is that it is just a traditional security assessment. Accordingly, many people think it is composed of a series of diagnostic questions and peer comparisons based on one or more industry standard frameworks. This couldn't be further from the truth. Indeed, security assessments have been around for a long time—even dating back to when cybersecurity was only referred to as "information security." Today, they continue to play a pivotal role in a holistic cybersecurity risk management program since they are useful in establishing capability maturity, prioritizing initiatives, and identifying opportunities for investment.

In contrast, the AICPA cybersecurity attestation is an extension of a maturity assessment wherein the organization will obtain an independent and objective view into the design and operating effectiveness of the company's existing cybersecurity processes and controls. It is broad enough to provide meaningful information to diverse stakeholders in a consistent way, and it is distinctly supported by both an assertion from management as well as the opinion of an independent public accounting firm. By facilitating independent and objective reporting, the cybersecurity attestation can provide a high degree of assurance around effectiveness of controls to a broad range of stakeholders.

> "Cybersecurity needs to have a common language that can be spoken across the organization. The AICPA's cybersecurity reporting framework is doing just that—creating a common, digestible language that can be understood by a multitude of stakeholders, including the board and audit committee."
>
> —Collin Harrison | Vice President of Finance and Information Technology, Alliance Data Systems Corporation

A complement, not a replacement

Many organizations already have mature reporting mechanisms in place, including Service Organization Control reports (SOC 1 / SOC 2) designed to provide focused assurance to customers of service providers. These reports, which are also governed by the AICPA and widely accepted across industries, have been very effective in fulfilling their designated objectives.

However, these reports (SOC 1 / SOC 2) should not be considered a silver bullet for addressing the information requirements of every constituent. Given the flexibility and scaleability that a cybersecurity attestation report offers (e.g., general use report, applicable to any entity, flexibility in the use of a cybersecurity control framework by management, entity-wide or business unit / segment specific attestation report, etc.), many organizations are evaluating their existing reporting mechanisms and stakeholder needs and are testing the waters by embarking on a readiness assessment to prepare for a future cybersecurity attestation report as a complement and extension to existing third-party assurance reports.

The moral of the story is: don't upset the apple cart by eliminating existing reports without a thoughtful evaluation of stakeholder requirements, including what regulators need, and how those requirements are being addressed.

Tough questions, thoughtful answers

Boards of directors clearly are a critical stakeholder group whose information requirements continue to elevate. Questions from the board keep getting tougher, and business and IT leaders are feeling the heat. Inquiries have morphed from the obligatory probe into whether or not there have been any incidents into a more sophisticated exploration of crown jewels, risk appetites, capability maturity, and program effectiveness as it relates to being secure, vigilant, and resilient. In general, board members are no longer satisfied with hearing programmatic updates from the IT and information security organizations. They want insights into what is happening within the business and risk functions in order to obtain an enterprise view of preparedness. Here are a few questions that leaders should be ready to answer before stepping into the boardroom:

1. What are our most critical assets and do we have the appropriate measures in place to protect them?
2. Are we investing in the right processes and controls, and how do we evaluate the results of our decisions?
3. Do our cybersecurity risk management capabilities and competencies align to industry standards and how do they compare with peer organizations?
4. How do we evaluate the effectiveness of our cybersecurity risk management program, and how do we determine if it aligns with our risk appetite?

> “We will need … to make sure that information from technologists on the front lines of this war reaches senior management—and, where necessary, the board and investors.”
>
> —Corporate Governance: On the Front Lines of America's Cyber War, Commissioner Robert J. Jackson, Jr., New Orleans, Louisiana, March 15, 2018
>
> Source: https://www.sec.gov/news/speech/speech-jackson-cybersecurity-2018-03-15

Ready, set, go

Pursuing a communication vehicle such as the cybersecurity risk management examination report without starting with the fundamentals is a lot like playing baseball without first learning how to catch and throw; it’s probably not going to end well. Successful early adopters have developed a thoughtful business case for leveraging the reporting framework to address stakeholder demands for transparency, and most have vetted their hypotheses about value realization through a readiness assessment. This assessment commonly has two phases: first, the organization establishes a holistic inventory of assets and evaluates their criticality through a common structure (e.g., identifying what and where the crown jewels are); and second, it evaluates the effectiveness of the controls within the cybersecurity framework the company has adopted (e.g., determining if the crown jewels are being adequately protected). The main goal of the readiness assessment is to proactively identify gaps as well as opportunities to strengthen controls before pursuing an attestation.

Conclusion

The cyber threat landscape continuously morphs and the velocity of technological change is sometimes paralyzing, but one thing has remained steady throughout the storm—the demand for information and transparency. Until recently, this demand has only been partially addressed by a supply of point solutions and ad-hoc approaches. Even with its limited tenure, the AICPA's attestation reporting framework has been a welcome addition to the cyber war chest of many organizations. By viewing their cybersecurity risk management programs through the focused lens of the AICPA framework, organizations can obtain a high-resolution picture of the effectiveness of their controls that simply wasn't available before.

"Reputational damage isn't limited to the cyber breach alone; it's often about how vigilant and resilient the company is in identifying and responding to it. This comes down to having the right processes and controls in place and knowing how effective they're operating within the context of the overall cybersecurity risk management program."

—Raymond Kyan | Corporate Vice President,
Head of Risk Assessments, New York Life Insurance Company

Is undertaking a voluntary readiness assessment worth the effort?

Insights from the recent Cybersecurity Risk Management Examination Roundtable suggest the answer is likely yes.

Marking the one-year anniversary of the issuance of the AICPA attestation guidance, Deloitte hosted a roundtable in New York City to share perspectives on the cybersecurity risk management examination and to explore the drivers for undertaking a readiness assessment.

Speakers outlined three underlying tenets of the cybersecurity risk management examination that differentiate it from other types of reporting:

1. Proactive risk assessment
2. Cyber-program control effectiveness
3. Board-level reporting

They further explained that one of the big advantages of the AICPA attestation framework is that it provides a uniform language, similar to US GAAP for financial reporting, for communicating the effectiveness of an organization's cybersecurity risk management program to a variety of stakeholders, including the board and third parties.

While beneficial, several participants questioned whether these attributes were enough to create a compelling value proposition.

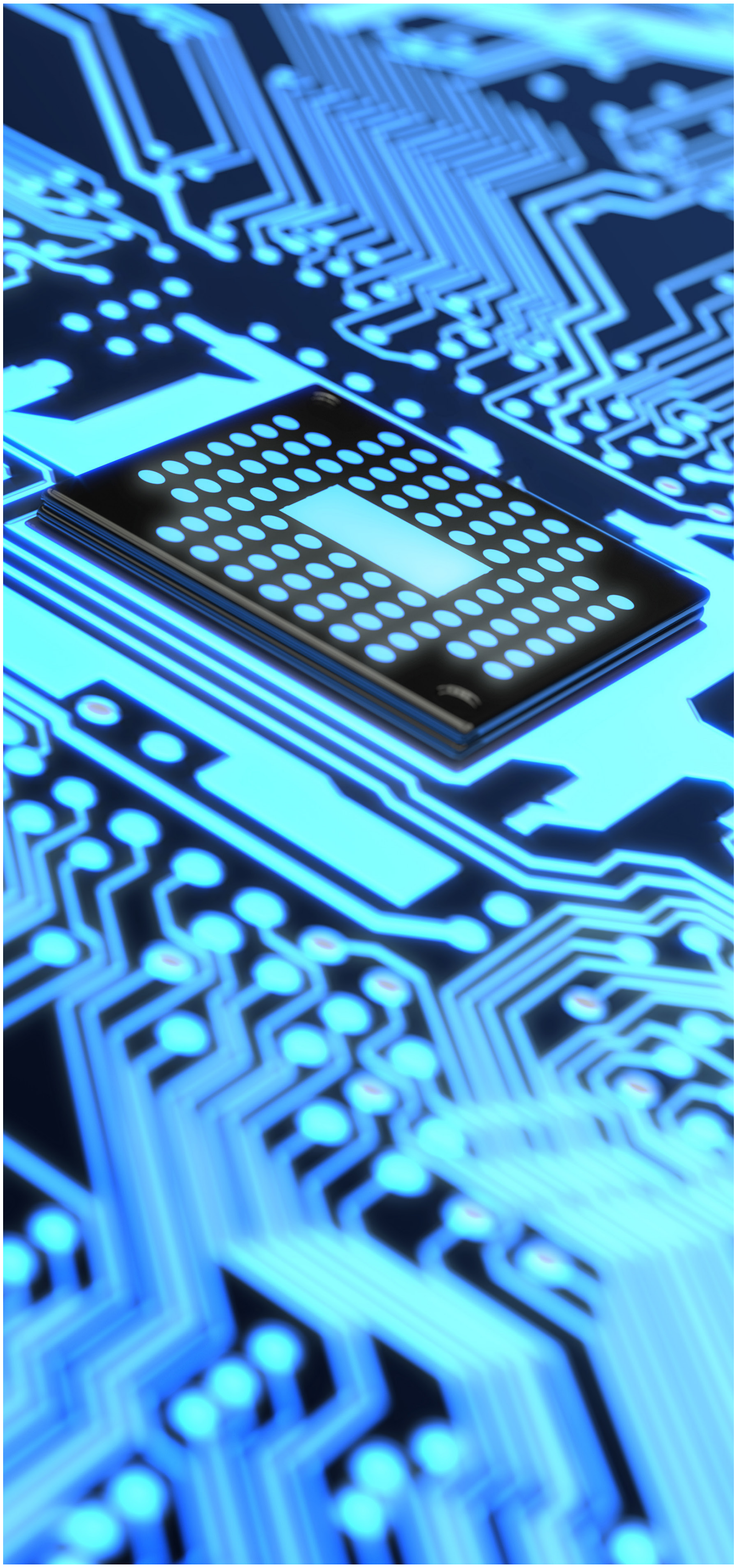
Or put another way, since the examination is voluntary and not mandatory, why should they do it? This opened up a broad discussion around current approaches to cybersecurity reporting and the evolving regulatory environment. Ultimately, speakers and participants enumerated several possible motivations for undertaking a readiness assessment and subsequently an attestation.

These include:

- Giving the board greater visibility into the organization's risk posture and cybersecurity preparedness
- Providing a non-technical report that can be easily consumed by an array of stakeholders
- Offering comparability
- Achieving operational efficiencies by streamlining the process of responding to the mounting number of cybersecurity questionnaires
- Identifying gaps in incident response to reduce reputational risk
- Positioning the company as a vendor/supplier of choice
- Negotiating with insurance carriers on cyber liability policy terms and premiums
- Offering an independent perspective on the effectiveness of cybersecurity controls

In pursuing these benefits, speakers emphasized that the cybersecurity risk management examination is intended to complement, not replace, internal audit reports or other reviews. And, because the output of the examination addresses certain regulatory requirements, such as the new Securities and Exchange Commission (SEC) disclosure obligations and the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, it can be useful in streamlining compliance efforts and responding to external audits and inspections.

Speakers additionally emphasized the importance of having specific objectives in mind before pursuing a cybersecurity risk management examination. The report is consistent, yet flexible, thus focus is required to achieve the desired benefits. "Cyber security remains a top risk for nearly every organization and it's not going away," said Gaurav Kumar, Principal, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP. "Is your organization prepared to answer the tough questions?" he concluded.



Contacts

Gaurav (GK) Kumar
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 212 436 2745
gukumar@deloitte.com

Jeff Schaeffer
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 973 602 5518
jschaeffer@deloitte.com

Sandy Herrygers
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 313 396 3475
sherrygers@deloitte.com

Emily Mossburg
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 571 766 7048
emossburg@deloitte.com

Chad Murphy
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 816 802 7248
chadmurphy@deloitte.com

Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.