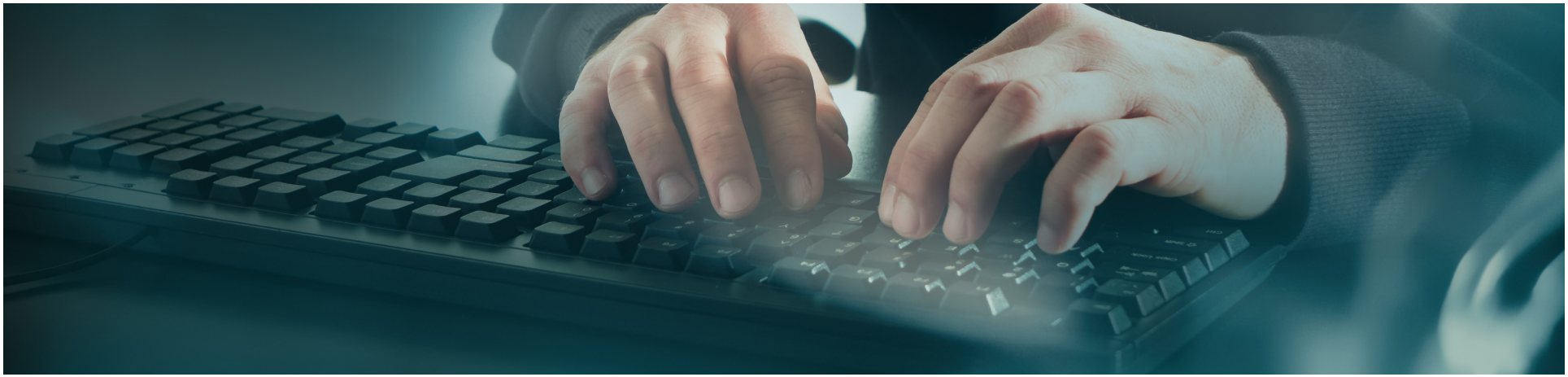
Deloitte.

Deloitte Risk and Financial Advisory



Cybersecurity risk management oversight and reporting

Better standards and independent scrutiny for increased transparency

What implications might the new American Institute of Certified Public Accountants' (AICPA) cybersecurity attestation reporting framework have for your company?

Read the transcript to learn how your organization can use enhanced cybersecurity risk management reporting to increase transparency; gain credibility, confidence, and trust over the entity's cybersecurity risk management program; and realize competitive advantage. The attestation reporting framework addresses the needs of a variety of key stakeholder groups and, in turn, limits the communication and compliance burden placed on those groups. Organizations that view the new cybersecurity reporting landscape as an opportunity can use it to lead, navigate, and even disrupt in the ever-evolving marketplace.

Whether it's the relentless wave of breaches or the ongoing saga of cybercriminals targeting some of the world's largest financial services firms, organizations are constantly trying to defend and safeguard against the next cyberattack. Reuters Solutions recently conducted an interview with Gaurav Kumar and Jeff Schaeffer from Deloitte Risk and Financial Advisory to better understand how the cybersecurity reporting landscape is evolving with the introduction of the AICPA cybersecurity attestation reporting framework. Kumar is a principal at Deloitte & Touche LLP, specializing in Assurance and Controls Transformation services. Schaeffer is a senior manager in the Cyber Risk Services practice at Deloitte & Touche LLP.

Reuters Solutions: Mr. Kumar, understanding that you sit on the AICPA's task force that helped to craft the framework and guidance, what do you believe is driving these changes and the increased focus on cybersecurity risk management program reporting?

Kumar: With the influx of data theft and breaches in the news nearly every day, organizations are under intense pressure to demonstrate they're doing everything in their power to protect customers, employees, and the large amounts of data in their possession. We've seen complete distractions for organizations that are constantly being inundated with requests. Organizations are receiving a lot more scrutiny and pressure from both internal and external stakeholders (See "The benefits of change"), and there needs to be improved reporting and greater transparency around an organization's cybersecurity risk management program. The AICPA's new cybersecurity risk management examination reporting framework will aid in this and provide organizations, particularly boards in their oversight role, with an internal reporting mechanism to effectively challenge management's certifications.

Reuters Solutions: Cybersecurity isn't a new risk domain or concept for organizations. Haven't they been addressing this concern for a number of years?

Schaeffer: Organizations have access to and utilize various cyber-risk monitoring and reporting mechanisms, such as risk and control self-assessments, internal audits, and simulation exercises. And each one addresses a very specific need. Board members, for example, typically want information regarding the overall posture of the cyber risk management program and how well the organization meets regulatory requirements. A client, or a prospective client, may be more concerned about how the organization is protecting its information. Yet there's no single approach or mechanism that addresses all stakeholder questions and needs and that also allows entities to report on the effectiveness of their cybersecurity risk management program.

Kumar: Expanding cybersecurity risk management reporting is addressing a marketplace need for greater transparency by providing a broad range of users with information about an entity's cybersecurity risk management program that would be useful in making informed decisions. Because of the recent activity, including the growing number of high-profile cyber-related attacks and breaches and the recent legislations related to cybersecurity, a single, standardized reporting mechanism—based on the evaluation of an organization's cybersecurity risk management program [including the controls within that program] by an independent third-party firm—is essential for increasing organizational transparency and would be a more effective mechanism for stakeholders to use in making informed decisions.

"The AICPA's cybersecurity examination report is a huge opportunity for organizations struggling to provide stakeholders with meaningful information related to their cybersecurity programs. And by demonstrating their commitment to cyber risk management, these organizations can enhance their brand and reputation in the marketplace and encourage investor confidence."

Gaurav Kumar, principal, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP

Reuters Solutions: The AICPA also governs the Service Organization Control (SOC) 2 report. How is the cybersecurity risk management examination report different?

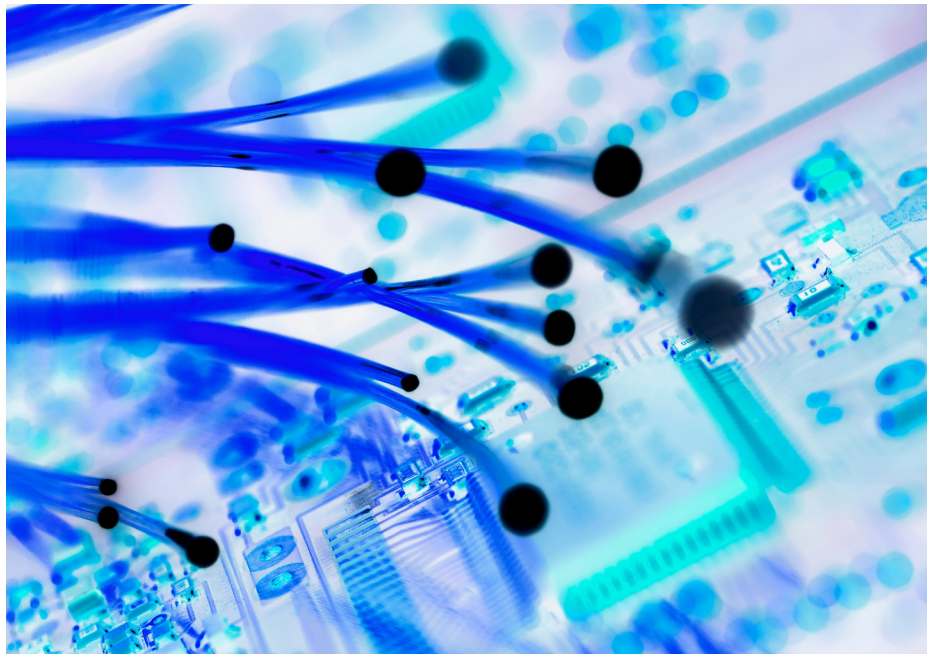
Schaeffer: There are distinct differences between the two. For example:

- The reporting framework can be applicable to all entities and not just limited to outsourced and third-party service organizations.
- Management also has flexibility in selecting the control criteria, as long as it's considered suitable and available, for designing and evaluating the organization's cybersecurity risk-management program and controls.
- The examination report can be appropriate for general use and meet the needs of a broad range of stakeholders, but management can also restrict the report distribution, if needed.
- While the cybersecurity risk management examination engagement is an entity-wide report, it can be applied to specific business units or segments. A cybersecurity risk management examination report will usually have a broader scope for the examination (e.g., typically higher number of critical IT assets, higher number of IT risks and controls for the assessment, etc.).

Reuters Solutions: This seems like a significant undertaking for companies. What benefits can be expected from a report of this magnitude?

Schaeffer: Given the importance of cybersecurity, organizations will continue to face intense pressure from their key stakeholders to respond to inquiries on the effectiveness of their cybersecurity risk management programs and related controls. We expect companies to realize a number of benefits beyond what current reporting mechanisms provide:

- Greater transparency around the effectiveness of the entity's cybersecurity risk management program to both internal and external stakeholders.
- Independent and objective reporting, providing a higher degree of assurance to key stakeholders. This is essentially obtained by having an independent third-party audit firm express an opinion on the effectiveness of an entity's cybersecurity risk management program and controls.
- Operational efficiencies gained from having a single reporting mechanism that addresses the information needs of a broad range of users.
- Greater economic value for intended users of the report by obtaining information about an entity's cybersecurity risk management program that would be useful in making strategic decisions.
- A strategic competitive advantage and enhancement of the entity's brand and reputation by being one of the early adopters of the cybersecurity examination engagement report.
- A single, unified reporting mechanism that covers a more comprehensive set of criteria covering internal controls, as well as commonly used cybersecurity frameworks.



Kumar: This should also give each of the constituents the information it needs to make thoughtful decisions. The AICPA's cybersecurity examination report is a huge opportunity for organizations struggling to provide stakeholders with meaningful information related to their cybersecurity programs. And by demonstrating their commitment to cyber risk management, these organizations can enhance their brand and reputation in the marketplace and encourage investor confidence. The same information demonstrates to regulators that the organization is complying with appropriate laws, regulations, and guidance. Risk management becomes another way for organizations to create value, not just protect it.

Reuters Solutions: What do you say to a company that's on the fence about the AICPA's cybersecurity attestation reporting framework and guidance?

Kumar: First off, it's not a requirement, so companies can decide on their own if they have an appetite to invest in this. However, the cyber threat landscape continues to rapidly evolve and organizations can't afford to be complacent. Just look at the statistics from Gartner[1] or the latest Verizon "Data Breach Investigations Report." More than 3,000 reported breaches in 2016 and an estimated yearly total cost exceeding $125 billion.[2,3] The numbers are staggering. Not to mention the recently published 2017 edition of the "NACD Director's Handbook on Cyber-Risk Oversight," which emphasizes the board's role in understanding and approaching cybersecurity risk management at the enterprise level. Organizations are going to continue to face pressures to demonstrate the effectiveness of their cybersecurity risk management programs and controls.

Schaeffer: I would add that the regulatory scrutiny is not diminishing either—especially for organizations in highly regulated industries like financial services where there may be penalties and fines for non-compliance. The latest set of cybersecurity requirements from the New York Department of Financial

The benefits of change

Using the new AICPA cybersecurity reporting framework to lead, navigate, and disrupt

The AICPA cybersecurity attestation reporting framework was developed to establish a standardized reporting mechanism to provide a broad range of users with useful information about an entity's cybersecurity risk management program to support informed and strategic decision making.

Stakeholders can benefit from the new AICPA cybersecurity risk management examination engagement in the following ways:

- Greater transparency
- Independent and objective reporting
- Useful in making informed and strategic decisions
- Strategic competitive advantage and enhancement to brand and reputation
- Operational efficiencies
- A comprehensive set of criteria

[1] "Gartner Worldwide IT Spending Forecast," Gartner, Inc., http://www.gartner.com/newsroom/id/3672818.

[2] "2016 Data Breach Investigations Report," Verizon, 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

[3] "2016 Cost of Data Breach Study: Global Study," Benchmark research on the global trends and costs of data breaches, sponsored by IBM, independently conducted by Ponemon Institute LLC, June 2016, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN.

Services (NYDFS), which became effective as of March 1, 2017, is a strong example of heightened regulation that's requiring organizations to establish and maintain an effective cybersecurity risk management program and certify that they have achieved or complied with a prescribed set of regulatory requirements. The NYDFS is also requiring a certification [from the board or a senior officer] that organizations have adhered to the requirements and maintain documentation to support their certification for up to a period of five years.

Reuters Solutions: Do you anticipate further state or federal cybersecurity legislations?

Kumar: What's interesting about the NYDFS requirements is how prescriptive they are. The introduction of a risk-based approach was also included in the finalized regulation. For those regulated by the NYDFS and considered a "covered entity," there are certain minimum regulatory standards to ensure appropriate cybersecurity programs are in place, including an annual certification of compliance by either the board or senior executive officer(s) responsible for the entity's cybersecurity program. The updated proposal does set forth transitional periods ranging from six months to two years with respect to certain components of the regulation, which gives organizations time to prepare.

Reuters Solutions: You mentioned "time to prepare." With the cybersecurity risk management examination framework and guidance now final, are you expecting companies to take action now and get their cyber programs in order?

Kumar: The pressure is going to continue to mount for stakeholders to report on the effectiveness of their [cybersecurity] programs and the related controls. Given the varying degrees of maturity, we encourage organizations to prepare for a future attestation by comprehensively assessing the current state of their program. The following activities should be contemplated:

- Define the boundaries of the program by taking a risk-based approach to identify the most critical IT assets.
- Select an appropriate cyber control framework (e.g., NIST CSF, ISO 27001, AICPA's Trust Services Criteria, etc.) that can be used in a future cybersecurity risk management examination engagement.
- Evaluate the effectiveness of current state internal controls included within the entity's cyber risk management program, leveraging the cyber control framework adopted by management.
- Identify potential gaps in, and enhancement opportunities for, key cyber risk processes and related internal controls.
- Develop a remediation plan and subsequently execute on key remediation activities.

"The increased level of pressure and scrutiny from stakeholders should be viewed as an opportunity for organizations to take a fresh look at their programs and really focus on the higher risk areas and significant gaps they may have."

Jeff Schaeffer, senior manager, Deloitte Risk and Financial Advisory, Deloitte & Touche LLP

Schaeffer: Keep in mind that the increased level of pressure and scrutiny from stakeholders is in some respects forcing organizations to change how they report on the effectiveness of their cybersecurity risk management programs and controls. This should be viewed as an opportunity for organizations to take a fresh look at their programs and really focus on the higher risk areas and significant gaps they may have.

Reuters Solutions: Any final thoughts?

Kumar: First, we appreciate your taking the time to speak with us on such an important and game-changing topic as the AICPA's cybersecurity risk management examination. This has been a huge focus for a number of the public accounting firms. The success and effectiveness of this kind of program needs active involvement and oversight from the board to hold the organization accountable for cybersecurity risk management, shape expectations for improved risk reporting, and advocate for greater transparency and assurance. The AICPA's cybersecurity risk management attestation reporting framework can provide the level of transparency and assurance required and cater to the information needs of a broad range of users. It can also allow the board and C-suite executives to have a finger on the pulse of the entity's cybersecurity risk management program and overall risk posture and controls within the program. Today, it's this knowledge and the subsequent actions taken to improve cybersecurity risk management oversight and reporting that elevate a company's brand and reputation in the marketplace.

Contacts

Gaurav Kumar
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
gukumar@deloitte.com

Jeff Schaeffer
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
jschaeffer@deloitte.com

To learn more about Deloitte Risk and Financial Advisory, visit:
www.deloitte.com/us/rfadvisory