Deloitte.

The value of visibility

Cybersecurity risk management examination

Welcome to the "new normal"

Cyberattacks are inevitable. In fact, it's no longer a question of "if" a breach will occur but "when."

Cybercriminals are becoming more sophisticated and the cost of cybercrime is becoming increasingly intolerable. And stakeholders—including boards, regulators, investors, analysts, business partners, and customers—expect greater visibility into an organization's cybersecurity risk management program. Taking a cursory look at what your organization is doing today to guard against cyberattacks is no longer enough to prove the readiness of your program and the effectiveness of your controls and processes.

That alone should be reason enough to act. But taking a proactive approach to cyber preparedness offers additional benefits beyond providing stakeholders with reasonable assurance that your risk management program is both designed appropriately and operating effectively. It's a means to help your stakeholders gain confidence and improve business performance as well.

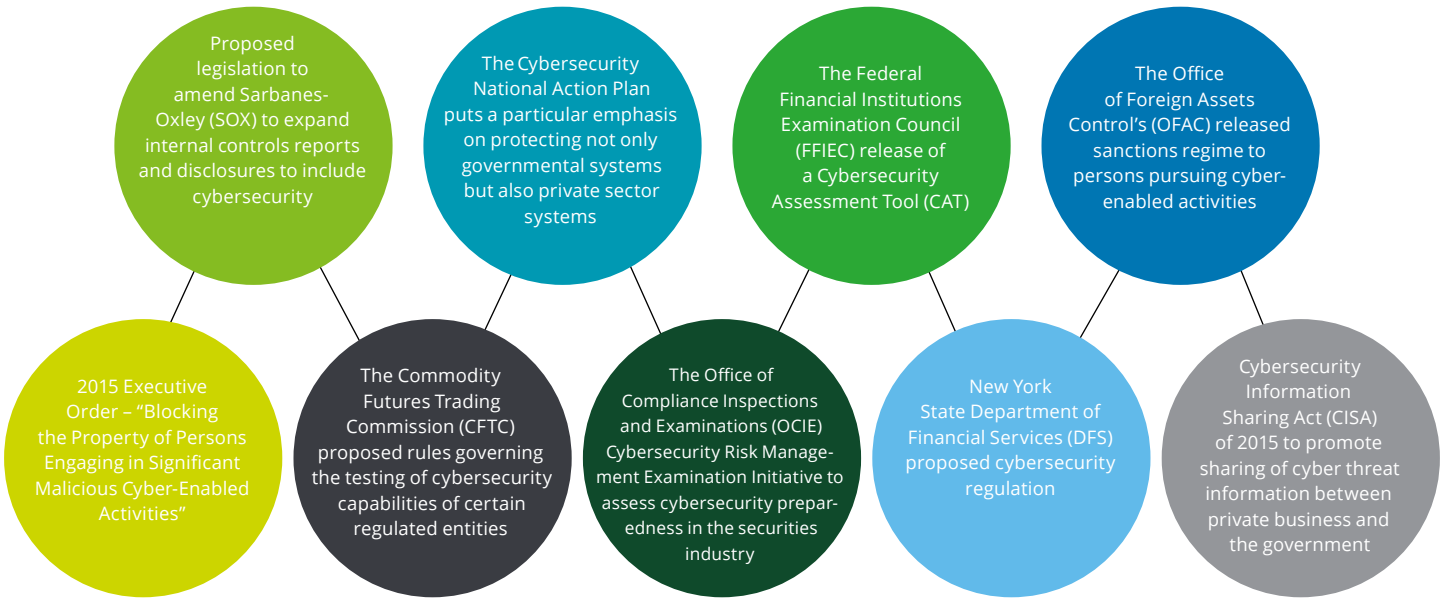
Implementing a sound cybersecurity risk management program is essential to protecting your brand. It's also critical for advancing your brand in the marketplace by empowering executives, including boards and audit committees, to make better informed and strategic decisions. Such a program can give your organization a jump in addressing mounting regulatory requirements regarding cybersecurity risk management reporting. (See the sidebar, "Regulation on the horizon.")

In short, when it comes to evaluating and reporting on your organization's cybersecurity risk management program and related controls, greater transparency and uniformity is becoming "the new normal."

Regulation on the horizon

A number of regulations are being developed in parallel with the AICPA's cybersecurity examination guidance. (See Figure 1.) The NYDFS is a recent participant in this movement, having issued a cybersecurity proposal on September 13, 2016. Among other actions, the proposed regulation would require banks, insurance companies, and other NYDFS-regulated entities to establish a cybersecurity program, adopt a written cybersecurity policy, and designate a chief information security officer, who must report to the board at least biannually to provide an assessment of the information systems. The NYDFS's proposal is just one example of increasingly broad regulatory pressure to tighten controls and visibility around cyber risks.

Figure 1. Recent US regulatory and compliance drivers



There's no single approach for providing this level of transparency and uniformity today. Therefore, a new standard—one that goes well beyond the types of reports and mechanisms currently available—is needed to gain visibility into an organization's cybersecurity risk management practices. (See the sidebar, "A closer look: Cybersecurity risk management examination versus SOC 2 engagement.") In response to stakeholders' increasing "need to know" about cybersecurity preparedness, the American Institute of Certified Public Accountants (AICPA) is developing new attestation guidance that focuses on evaluating and reporting on an entity's cybersecurity risk management program.[1] The proposed cybersecurity risk management examination is intended to expand reporting to address stakeholder expectations for greater transparency, providing in-depth information about what a company is doing to address cyber threats and improve responsiveness in the event of an incident. (See the sidebar, "Satisfying the needs of a variety of users.")

A closer look: Cybersecurity risk management examination versus SOC 2 engagement

While the AICPA governs both the SOC 2 engagement and the proposed AICPA cybersecurity risk management examination engagement, there are distinct differences between the two. In general, the proposed cybersecurity risk management examination, which applies to the management of any entity and is appropriate for general use, will be broader and more robust than a SOC 2 examination. A SOC 2 examination applies to the management of a service organization and can only be distributed to certain parties. The following table further articulates these and other distinctions:

	Cybersecurity risk management examination engagement	SOC 2 engagement
Purpose	Provide a variety of users with information about an entity's cybersecurity risk management program	To provide existing or prospective customers (system users) with information about controls at a service organization related to the Trust Services Criteria
Intended users	Management, directors, regulators, analysts, and third parties	Management of the service organization and other specified parties with sufficient knowledge and understanding of the system
Criteria	Flexible (National Institute of Standards and Technology's Cybersecurity Framework - NIST CSF, 800-53, ISO 27001, Revised Trust Services Criteria, etc.)	Trust Services Criteria
Responsible party	Management of any entity	Management of a service organization
Appropriate for general use?	Yes	No
Report contents	Description of the cybersecurity risk management program, management assertion, practitioners opinion	Description of the service organization's system, management assertion, practitioners opinion, description of tests of controls and results

[1] AICPA Cyber Security Initiative, American Institute of Certified Public Accountants, http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/aicpacybersecurityinitiative.aspx

Mind the gap

In their risk oversight role, boards today are using a variety of cyber risk monitoring and reporting mechanisms, such as risk and control self-assessments, internal audits, and cyber crisis simulations. But these mechanisms only partially meet the needs of an ever-growing audience of stakeholders, and they may not provide adequate visibility and enough relevant information for both internal and external parties to make well-informed decisions about an organization's cyber risk posture.

The proposed AICPA cybersecurity risk management examination engagement aims to address this information gap through independent and objective reporting on the effectiveness of cyber security processes and controls throughout an organization. These reports, which will describe and assess a company's efforts to manage cybersecurity risk, won't completely replace existing mechanisms, nor will they provide guarantees that an organization won't be breached in the future. But they will use broader and more flexible criteria, provide greater objectivity, and be more widely distributable. They will also be more flexible in scope, and they can be conducted for certain business units or segments. These characteristics are relevant to various stakeholders, including the C-suite and the board.

A cybersecurity risk management examination may offer a number of potential benefits, such as:

- Greater stakeholder transparency into the effectiveness of an organization's cybersecurity risk management program
- Independent and objective reporting, providing a higher degree of assurance to key stakeholders
- Greater economic value for users of the report, as obtaining more and higher quality information about an organization's cyber risk management program can drive better informed and strategic decisions
- Strategic competitive advantage and enhancement of the organization's brand and reputation in the marketplace, obtained by proactively establishing a strong foundation for addressing cybersecurity, before protocols are mandated by regulation or a crisis hits
- Operational efficiencies derived from a single reporting mechanism that addresses the information needs of a broad range of users

"Directors don't need to be technologists to play an effective role in cyber-risk oversight—but every board can take the opportunity to improve the effectiveness of their cyber-oversight practices."

***NACD Director's Handbook on Cyber-Risk Oversight*, National Association of Corporate Directors (NACD), 2017**

Satisfying the needs of a variety of users

The proposed AICPA cybersecurity risk management examination engagement guidance is being developed to establish a standardized reporting mechanism. This mechanism is designed to provide a broad range of users with valuable information about an entity's cybersecurity risk management program to support informed decision making.

- **Internal stakeholders.** Boards, audit committees, and management have an important oversight role relative to cybersecurity. They need to understand a company's cybersecurity risk posture, monitor ongoing compliance with internal and external requirements and regulations, and gauge the effectiveness of cybersecurity controls.
- **Regulators/federal agencies.** Companies will need to demonstrate to regulators that they're complying with applicable cybersecurity laws, regulations, and guidance (e.g., New York Department of Financial Services (NYDFS), Executive Order 13636[2]).
- **Existing and prospective clients.** Existing and potential clients of service organizations want to be sure they're engaging an organization that takes cybersecurity seriously, including addressing the cybersecurity risks inherent in outsourcing functions to a third party.
- **Vendors and business partners.** Vendors and business partners want to be able to assess and manage the risk to their business operations when working with a particular company. To do this, they need in-depth information about its cybersecurity risk management processes and controls.
- **Media/general public.** Cyberattacks, which continue to be high-profile and costly for companies, have become a mainstream media issue. The media and the public alike are asking companies about their cybersecurity environments, including any history of breaches, preparedness to respond to the current threat environment, and potential impacts upon customers.
- **Investors and analysts.** The financial impact of cyberattacks and the perception of how well executives are managing cybersecurity risks can affect investor and analyst behavior and, potentially, their confidence.

[2] New York State Department of Financial Services Proposed 23 NYCRR 500, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf

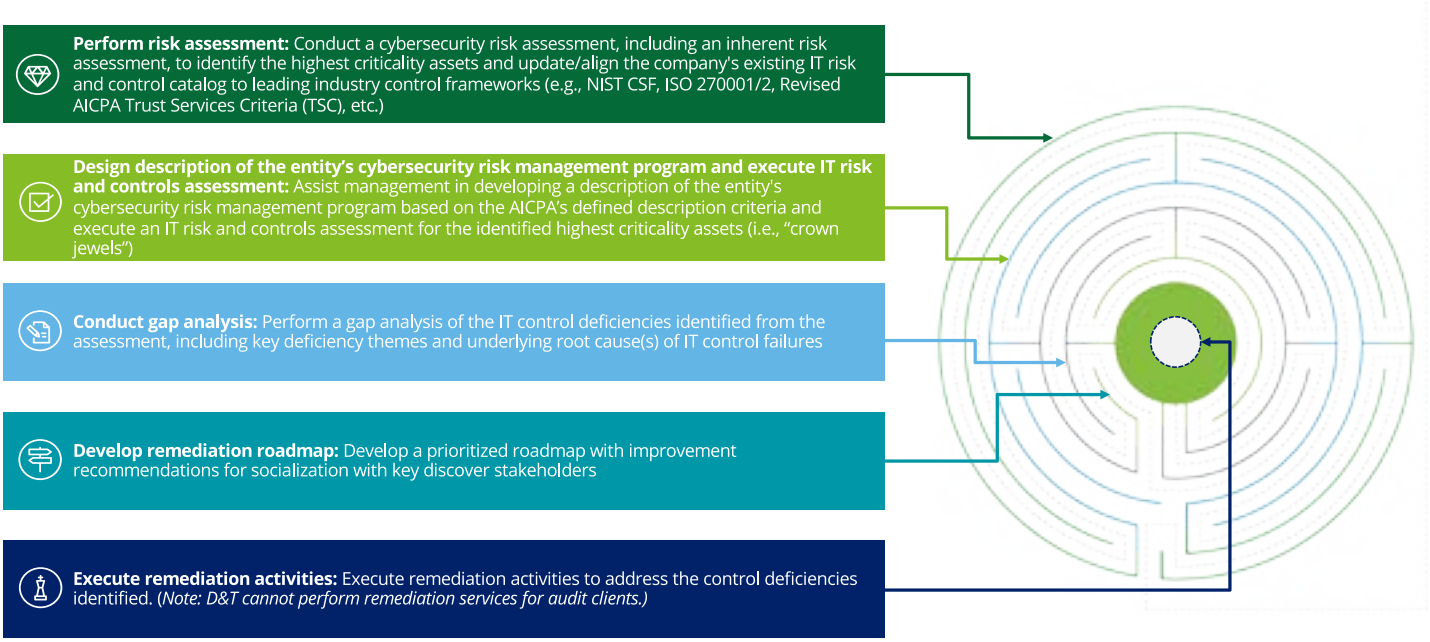
Ready or not, here it comes

The exact timeline has yet to be determined. But the final cybersecurity risk management examination engagement guidance is coming, and organizations should begin to prepare now to gain maximum competitive advantage. This advantage will diminish over time, as the visibility afforded by the examination transitions from a differentiating benefit to a "must-have."

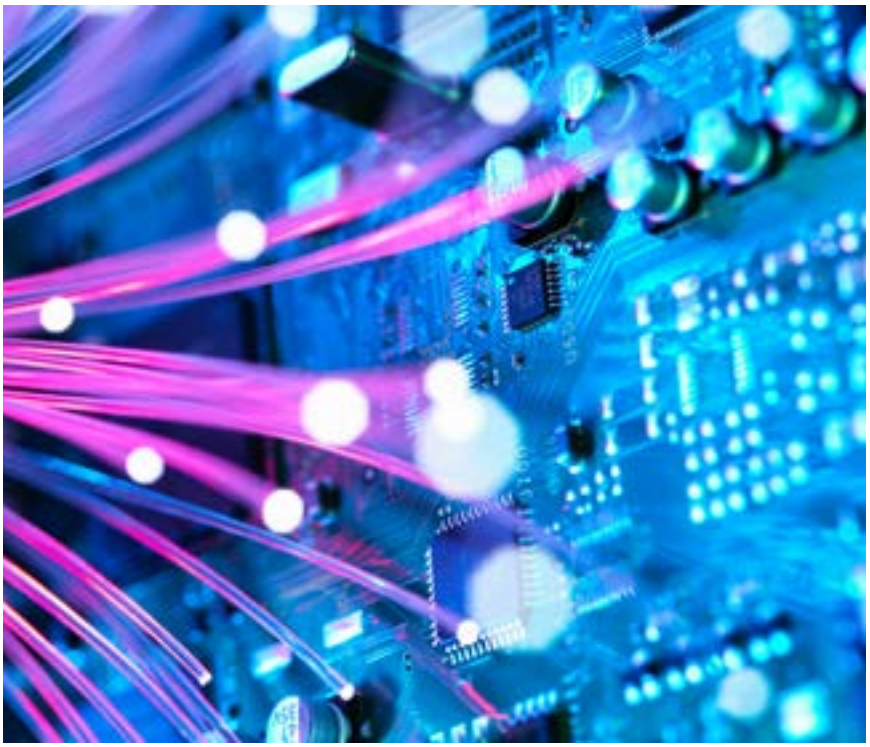
Every organization is at a different place when it comes to the maturity of its cybersecurity risk management program. In addition, the nature and magnitude of cyber risks are continuously evolving—and so are practices for staying ahead of these threats.

That's why it's important to understand where you stand today by proactively investing in a readiness assessment. This assessment can help you gauge the maturity of your controls and processes and determine how well they're functioning across multiple security domains. More specifically, it can help you select an appropriate cyber-control framework, identify gaps, highlight improvement opportunities, and develop a remediation plan. (See Figure 2.)

Figure 2. Recommended approach for performing a readiness assessment



Under the proposed cybersecurity examination engagement guidance, an organization should be able to demonstrate that its cybersecurity risk management program has been designed to mitigate risk to a level that's acceptable to a broad range of stakeholders. While a sound governance structure is the glue that holds a cybersecurity risk management program together, an active board and engaged leadership must supply the energy to enliven it. This means holding the organization accountable and helping to shape expectations for improved cybersecurity risk management reporting. Without both structure and oversight, a cybersecurity risk management program will fall short of its full potential to deliver the visibility expected by stakeholders and create value by aligning with corporate strategy and elevating business performance.



"Imagine a world in which all types of entities could convey the effectiveness of their cybersecurity risk management in a standardized, non-technical way, appropriate to each entity's size and other business characteristics. Think about the power of such assurance. Boards, shareholders, customers, counterparties, and regulators could gauge the relative effectiveness of organizations' cybersecurity and resiliency. If done right—with independence, objectivity, appropriate expertise, and professional skepticism—such an assurance process would be a vehicle by which greater cybersecurity and resilience could be achieved."

Remarks by Deputy Secretary Sarah Bloom Raskin at the Public Company Accounting Oversight Board International Institute on Audit Regulation, December 14, 2016

Get ahead of the curve

Starting on a cybersecurity examination readiness assessment today can help your organization understand the current state of its cybersecurity risk management program and be better prepared for a future state examination. It can also put you ahead of the curve in addressing the requirements of expanding regulations around cybersecurity risk management reporting. Such an assessment serves to both protect and create value by improving operational efficiencies and strengthening brand image—helping your stakeholders gain confidence and obtain reliable information to support informed and strategic decision making.

The cyber threat landscape remains exceptionally complex, and your organization's brand and reputation are at stake. The time to act is now.

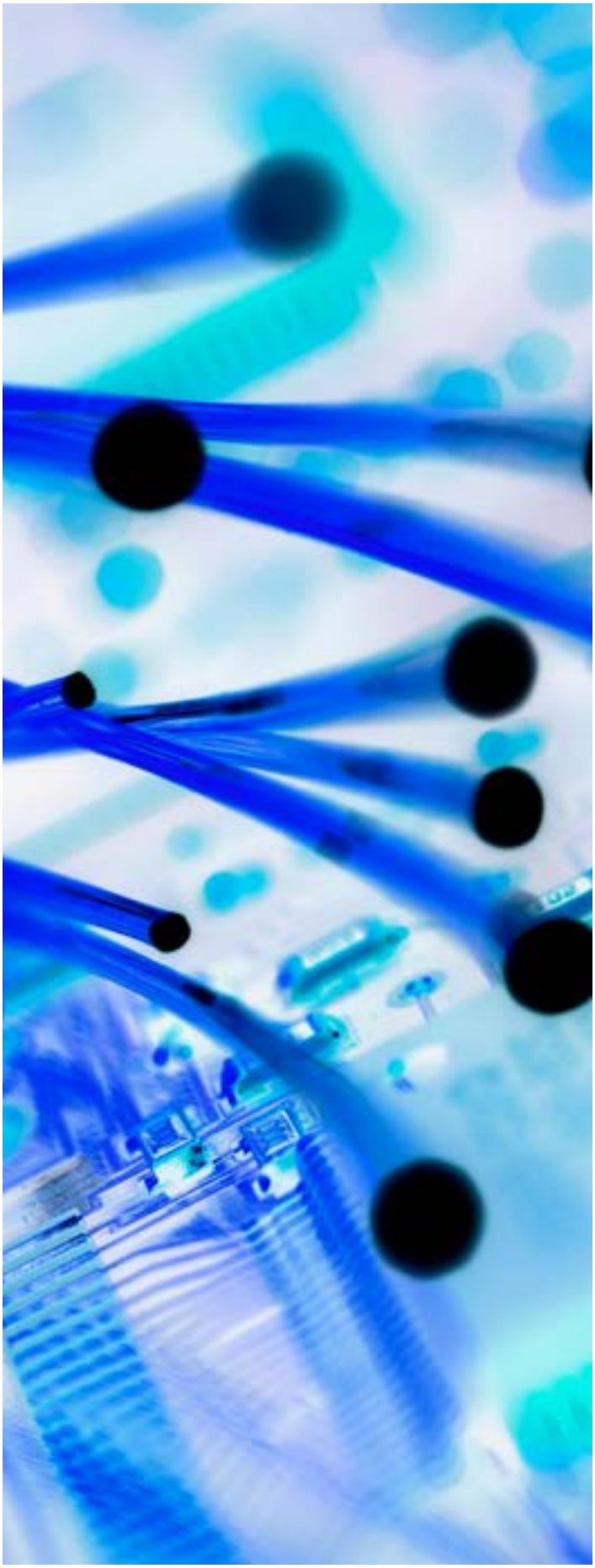
Contacts

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

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

John Clark
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
johclark@deloitte.com
+1 312 486 3985

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



Deloitte.