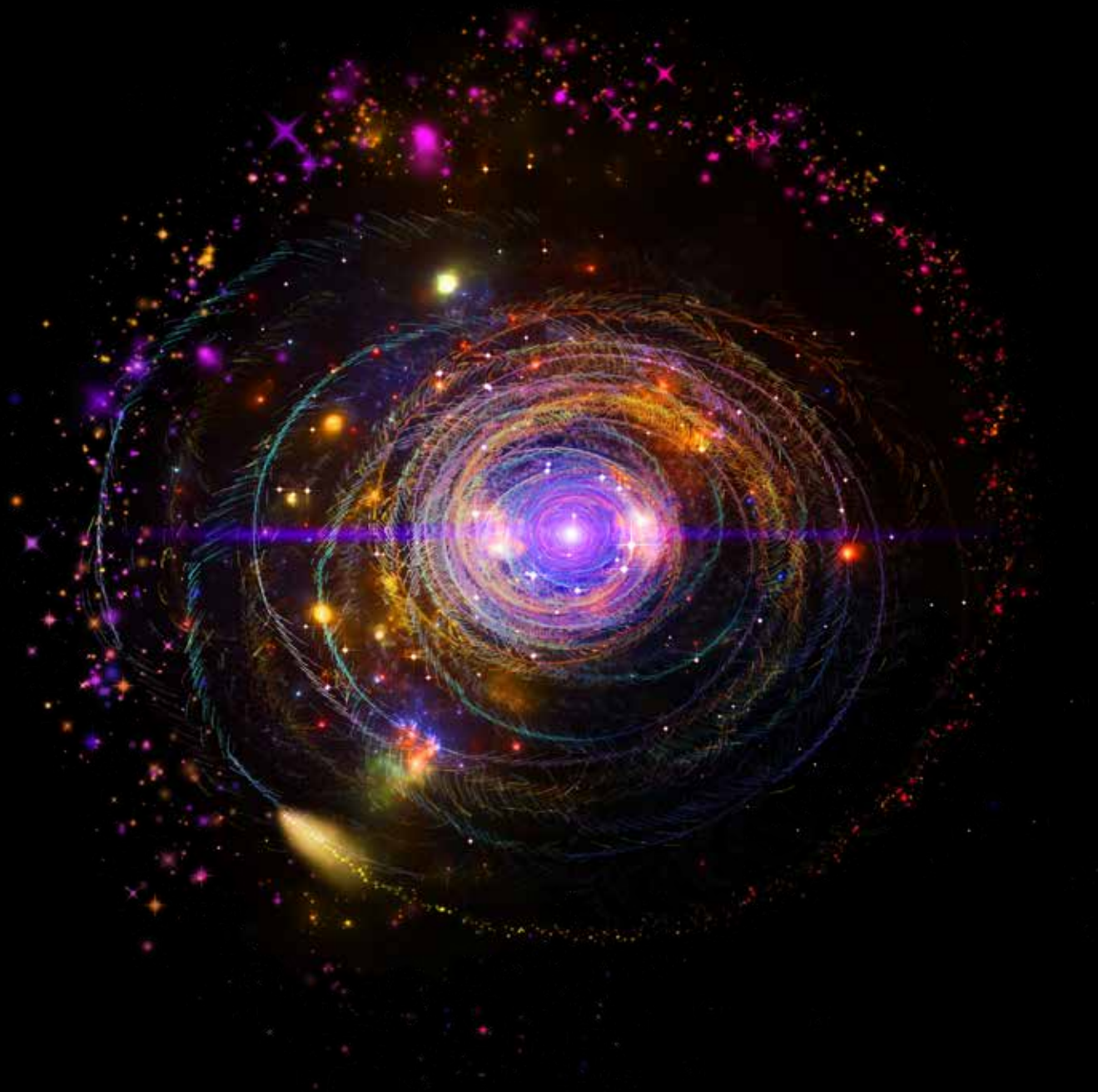
Deloitte.



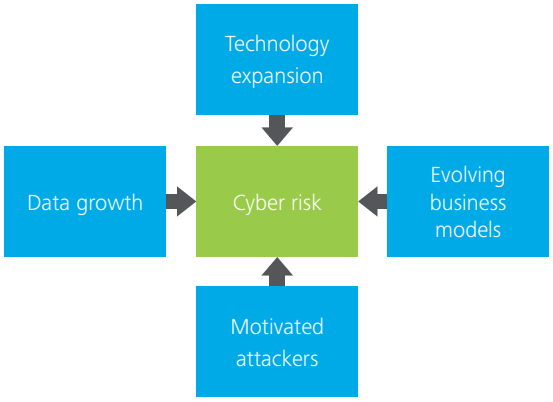
Where insights lead

Cybersecurity and the role of internal audit:
An urgent call to action

Our experience shows that an effective first step for internal audit is to conduct a cyber risk assessment and distill the findings into a concise summary for the audit committee and board, which will then drive a risk-based, multi-year cybersecurity internal audit plan.

The threat from cyberattacks is significant and continuously evolving. One estimate suggests that cyber crime could cost businesses over $2 trillion by 2019, nearly four times the estimated 2015 expense. Many audit committees and boards have set an expectation for internal audit to understand and assess the organization's capabilities in managing the associated risks.

Figure 1. Forces of cyber vulnerability



An ascending agenda item

The forces driving business growth and efficiency contribute to a broad attack surface for cyber assaults (Figure 1). Internet, cloud, mobile, and social technologies, now mainstream, are platforms inherently oriented for sharing. Outsourcing, contracting, and remote workforces are shifting operational control. Data continues to expand along with requirements to protect it. And, attackers can range from hackers to nation states, all continuously innovating and subverting common controls, some beyond the reach of a country's law enforcement.

Headline-making breaches, combined with growing government focus on cyber threats, have increased concern among corporate audit committees and boards of directors. Under U.S. Securities and Exchange Commission (SEC) guidance, public companies are expected to address potentially material cybersecurity risks and cyber incidents in the Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A).[2] Amid ever-growing concerns about cyberattacks affecting the nation's critical infrastructure, President Obama's Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, has highlighted the role of businesses in improving the nation's cybersecurity framework and the need to adapt to rapidly changing regulatory agency expectations and oversight.[3]

Three lines of defence

Business units and the information technology (IT) function integrate cyber risk management into day-to-day decision making and operations. This comprises an organization's first line of defence. The second line includes information and technology risk management leaders who establish governance and oversight, monitor security operations, and take action as needed, often under the direction of the chief information security officer (CISO).

Increasingly, many companies are recognizing the need for a third line of cyber defence—independent review of security measures and performance by the internal audit function. Internal audit should play an integral role in assessing and identifying opportunities to strengthen enterprise security. At the same time, internal audit has a duty to inform the audit committee and board of directors that the controls for which they are responsible are in place and functioning correctly, a growing concern across boardrooms as directors face potential legal and financial liabilities.

The why and how of cyber risk assessment and defence

Exploring an organization's cyber risks begins with three key questions:

Who might attack? Are the perpetrators criminals, competitors, third-party vendors, disgruntled insiders, agenda-driven hackers, or someone else?

What are they after, and what business risks need to be mitigated? Do they want money or intellectual property? Is their goal to disrupt the business or ruin its reputation? Could health and safety risks be created?

What tactics might they use? Will they go phishing, test system vulnerabilities, use stolen credentials, or enter networks through a compromised third party?

Deloitte has identified a three-pronged approach to help clients address the threats identified through examining these questions:

Secure. Most organizations have established controls such as perimeter defences, identity management, and data protection to guard against known and emerging threats.

Risk-focused programs prioritize controls in areas that align with top business risks.

Vigilant. Threat intelligence, security monitoring, and behavioural and risk analyses are used to detect malicious or unauthorized activity such as application configuration changes or unusual data movement, and to help the organization respond to the shifting threat landscape.

Resilient. Incident response protocols, forensics, and business continuity and disaster recovery plans are put into action to recover as quickly as possible and reduce impact.

Exploring the who, what, and how questions posed above in the context of a secure, vigilant, and resilient organization provides the foundation for a broad internal audit cybersecurity assessment framework that will be an integral component of the organization's cyber defence initiatives.

Cybersecurity assessment framework—a comprehensive approach

Many internal audit functions have performed procedures around evaluating components of the organization's cybersecurity readiness. These targeted audits, such as attack and penetration procedures, are valuable but do not provide assurance across the spectrum of cybersecurity risks. For internal audit to provide a comprehensive view of cybersecurity, and avoid providing a false sense of security by only performing targeted audits, a broad approach should be employed. Figure 2 portrays a cybersecurity assessment framework built on our recommended Secure.Vigilant.Resilient.™ concept. As shown, multiple security domains support each of the three themes. In assessing cybersecurity readiness, internal audit can benefit from understanding the capabilities within each of the 12 domains, how they are addressed today, and gaps that may exist within the organization.

Figure 2. Representative cybersecurity framework

Notably, roles and responsibilities within the framework are not limited to the IT organization, but span the entire enterprise. For example, data management and protection, elements of vigilance shown in Figure 2, are put in the hands of managers and employees across the business to define what their data is. This responsibility exists up and down the organization, with even CEOs tasked to assess the risk exposures in their memos and other communications.

Other important considerations can include the limited scope of existing IT audits and the lack of internal audit review of certain capabilities. Colour highlights in the framework indicate that Sarbanes-Oxley testing, penetration and vulnerability testing, and business continuity and disaster recovery testing each address certain elements of the Secure.Vigilant.Resilient.™ framework. However, numerous other risks may be missed in the IT function's general computer controls testing, for example, the non-highlighted vigilance functions of threat modelling and security event monitoring, and the resilience functions of recovery, testing, and exercising. An internal audit cyber risk assessment could identify these gaps, leading to wargaming scenarios and exercising to spotlight critical questions. Who should a threat recipient alert to the danger? How does the organization respond? If a ransom is demanded, should the organization pay it?

Several factors are noteworthy as internal audit professionals consider and conduct a cybersecurity assessment.

First, it is vital to involve people with the necessary experience and skills. Internal audit has the know-how to conduct assessments. However, understanding whether the IT department or the CISO is doing a robust job of threat modelling can require subject matter specialists who know effective questions to ask. A tech-oriented audit professional versed in the cyber world can be an indispensable resource.

It's also important to evaluate the full cybersecurity framework, rather than cherry-pick items. This evaluation involves understanding the current state against framework characteristics, where the organization is going, and the minimum expected cybersecurity practices across the industry or business sector.

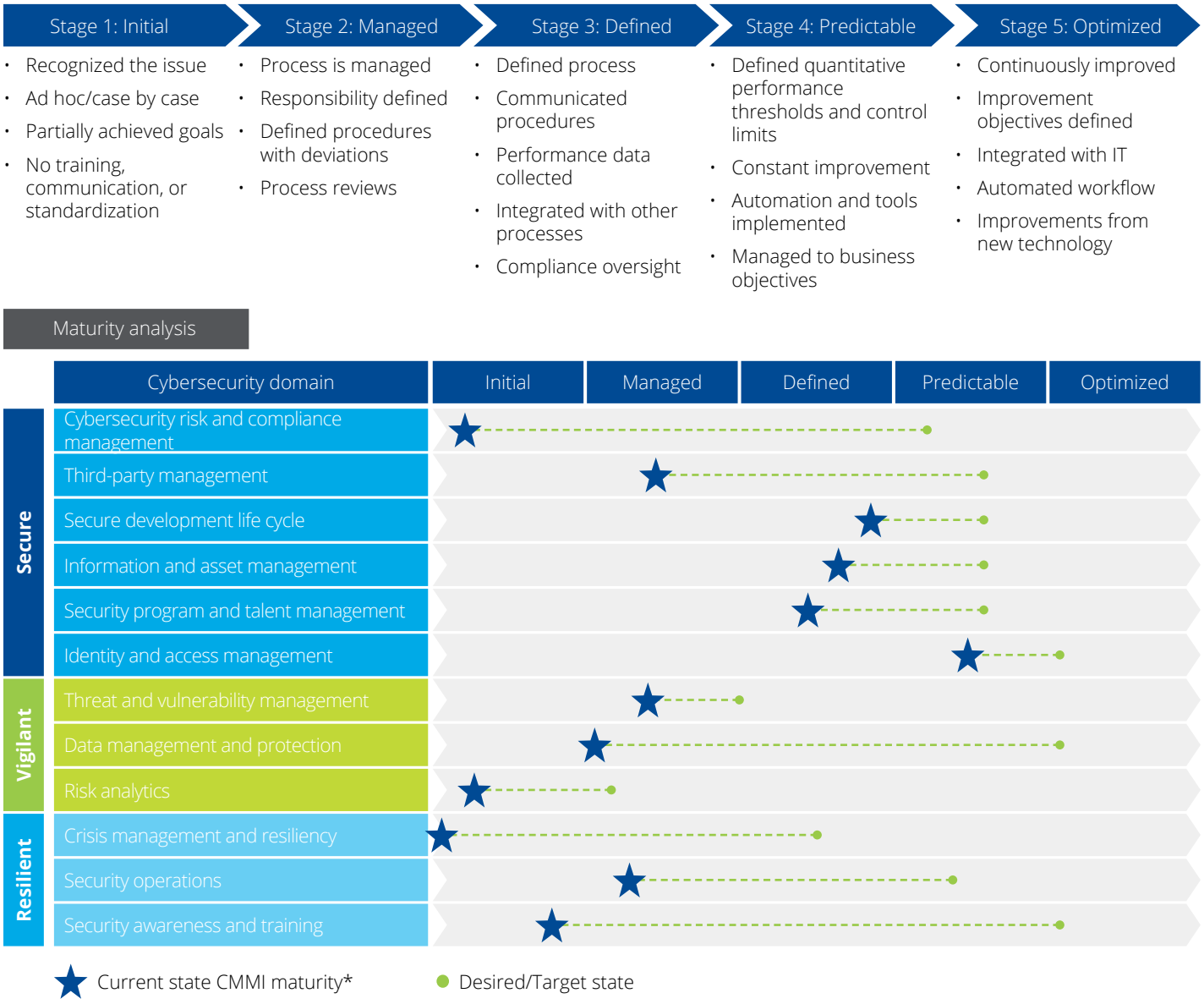
Finally, the initial assessment should be a broad evaluation. It is not intended to be an exhaustive analysis requiring extensive testing. Instead, the initial assessment should drive additional risk-based cybersecurity deep-dive reviews.

Cyber risk assessment—an important starting point

Maintaining and enhancing security capabilities can help mitigate cyber threats and move the organization toward its desired level of cybersecurity maturity. By performing a comprehensive cyber risk assessment, internal audit can present objective perspectives and findings to the audit committee and board members, and use those findings to develop a broad internal audit plan that addresses the areas of cyber risk for the organization over a single or multi-year audit period. Performing risk assessments may be one strategy for organizations, or some may elect to use the maturity analysis approach. The maturity analysis approach can provide additional value to management and those tasked with corporate governance by providing a quick visual reference that gives clear cues about areas they should explore further. With the proper subject matter expertise and involvement, a cyber risk assessment can also be structured to generate a list of cybersecurity gaps and provide the organization with a roadmap for short- and long-term remediation activities.

Figure 3 presents an analysis built around the secure, vigilant, and resilient themes and is mapped to the themes' 12 cybersecurity domains. The five maturity stages—Initial, Managed, Defined, Predictable and Optimized—reflect the progress the organization has made in maintaining and enhancing security capabilities to help mitigate cyber threats and achieve its desired maturity level. The green dotted lines lead to the level of maturity an organization is targeting, potentially identified in a remediation roadmap. As changes are implemented, the results should map to the location of the green dots. The board should agree to the desired maturity level upon completion of the work, at which point internal audit would test it once again and come back to the board to confirm the targeted level has been achieved.

Figure 3. Sample risk assessment maturity analysis



*The industry-recognized Capability Maturity Model Integration (CMMI) can be used as the model for the assessment. Each domain consists of specific capabilities that are assessed and averaged to calculate an overall domain maturity.

A separate assessment scorecard should support the maturity evaluation, highlighting in detail the cyber risks surrounding people, process, and technology. Findings must be documented and recommendations made for closing identified gaps.

Foundations of an internal audit plan for cybersecurity

As noted earlier, the cyber risk assessment underpins both the maturity analysis provided to the audit committee and board and the development of a risk-based, multi-year internal audit plan for cybersecurity. The multi-year plan can be developed through the results of the assessment, with some audits occurring at a higher frequency than others based upon urgency and consideration of other testing and assessment activities underway in the organization.

The internal audit plan for cybersecurity is not set in stone. Adjustments can be made based on the emergence of new risks, changes in the relative intensity and importance of existing threats, and other organizational developments.

Internal audit's role in strengthening cybersecurity

Cyber risks continue to grow in frequency, variety, and the potential harm they can cause to companies, their trading partners, and their customers. Most businesses take these risks seriously, but more can be done, both to combat the dangers and to keep company leaders apprised of cybersecurity preparedness. Internal audit has a critical role in helping organizations in the ongoing battle of managing cyber threats, both by providing an independent assessment of existing and needed controls and helping the audit committee and board understand and address the diverse risks of the digital world.

Contacts

Contact us to further discuss internal audit's role in cybersecurity and how Deloitte Risk Advisory is helping organizations meet the expectations of boards and audit committees today.

Kareem Sadek
Partner, Risk Advisory
ksadek@deloitte.ca

Farzin Ismail
Senior Manager, Risk Advisory
fismail@deloitte.ca

Marco Spagnoli
Senior Manager, Risk Advisory
mspagnoli@deloitte.ca

Endnotes

[1] "Cybercrime Will Cost Businesses Over $2 Trillion by 2019," Juniper Research, May 12, 2015, http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[2] "CF Disclosure Guidance: Topic No. 2," U.S. Securities and Exchange Commission, October 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) – 21 Critical Infrastructure Security and Resilience," U.S. Department of Homeland Security, March 2013, http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

[4] The framework in Figure 2 aligns with industry standards, including National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Committee of Sponsoring Organizations (COSO), and Information Technology Infrastructure Library (ITIL).

deloitte.ca

Designed and produced by the Deloitte Design Studio, Canada. 17-5103T