Deloitte.

Cyber risk and the new age chief audit executive

Elevating the CAE's influence in an evolving cyber risk landscape

Today's internal audit (IA) teams and chief audit executives (CAEs), in particular, have a lot on their minds. Rapid advances in technology have bred a new generation of cybercriminals bent on disrupting operations or stealing data and assets, with potentially costly impact on corporate reputations and bottom lines. Worldwide cybercrime costs are estimated to hit $10.5 trillion annually by 2025.[1]

With enforcement unable to keep pace with attacks,[2] many organizations are bolstering their defenses. And those defenses go far beyond the chief information and security offices. CAEs are rapidly transforming their traditional audit and assurance role by further educating themselves and building more tech-savvy teams to join the cybersecurity fight.[3]

A now-or-never moment in the evolution of the CAE

As stakes have risen, so have expectations of IA. Boards and CEOs are increasingly recognizing their gaps in understanding where cyber risk lies, including chronic underestimation of former employees with login rights, third-party vendors with access to corporate IT systems, and total cyber breaches across the organization.[4] Business executives and boards are turning to the CAE to provide an independent and objective assessment of their organization's cyber risk management practices and capabilities.

Table 1: Internal audit must respond well to boards' questions around cyber. To be strategic and innovative, IT internal audit should prioritize relevant cyber risks to elevate IA's value and impact to the organization.

Many boards are asking...	Internal audit should...
What kind of attacks are happening, and have we established an appropriate cyber risk escalation framework?	**Determine whether the following exist:** • Operationalized roles and responsibilities. • Key risk and performance indicators. • Incident management framework including escalation criteria aligned with the cybersecurity program.
How do our cybersecurity program and capabilities align to industry standards and peer organizations?	**Validate whether the organization has:** • Conducted an external benchmarking review of its cybersecurity program. • Periodically verified its compliance with policies, industry standards, and regulations. • Formally certified critical and applicable areas of its business.
What has management done to protect the organization against third-party cyber risks?	**Evaluate whether the following exist:** • Cybersecurity risks are part of the due diligence process for critical third-party arrangements. • Third parties are engaged through a consistent process and receive specific training on cybersecurity. • Processes are in place to ensure timely notification of cybersecurity incidents from third parties.
Can we rapidly contain damages and mobilize diverse response resources should a cyber incident occur?	**Confirm whether:** • Cybersecurity incident response plans and procedures are documented and rehearsed via wargaming simulations. • Cyber incident response policies and procedures are integrated with existing business continuity management and disaster recovery plans.
How do we evaluate the effectiveness of our organization's cybersecurity program?	**Collaborate with stakeholders to:** • Conduct regular internal and external assessments of vulnerabilities to identify cybersecurity control gaps. • Evaluate cyber risk management effectiveness as part of quarterly reviews.

IA should augment teams with complementary, nontraditional skill sets:

96% of respondents said IA needs to broaden its skill set, especially in IT, cyber and data areas.

Global Audit Committee Survey | September 2020

As the stars align on technology, threats, and solutions, CAEs are taking a more prominent seat at the C-suite table. To reinvent themselves (and their teams) by focusing on rising cyberthreats like ransomware, phishing attacks, and data breaches, CAEs need to seize a once-in-a-generation opportunity to make a splash as trusted advisers to senior leaders, audit committees, and boards of directors.[5]

Those who aren't willing to capture their moment could leave their organization with increased risk exposure.

Next-gen role of internal audit in addressing cyber risks

Often, the greatest threats organizations face are the ones they don't see coming. IT functions may be the backbone of threat management, cyber defenses, and asset protection, but CAEs and IA functions are looking to contribute in different ways.

CAEs are covering their "A's" by providing insights about cyber risks and refocusing to **assure** on business resiliency, **advise** on cyber readiness, **anticipate** perilous cyber events, and **accelerate** adaptation of the IA function to meet current and future cyber risk advisory demands. With increased and expanding legal liabilities along with potential vulnerabilities, IA is helping their companies more effectively manage cyberthreats.

Assure. Providing validation of effectiveness of the cyber program to address the company's greatest cyber risks.

Advise. Collaborating with the business, CISO, and IT on strategic priorities while providing real-time feedback on cyber readiness, risks, and controls.

Anticipate. Understanding digital transformation, which assets need to be protected, and what could go wrong.

Accelerate. Improving IA through organizational learning, management action, and technology-enabled cyber audit techniques.

Assure: Providing confidence in the company's cyber capabilities

Board members and senior leaders want assurance about the security of their crown jewels and a better understanding of the degree to which cyber events might disrupt the business. Not surprisingly, they are looking to CAEs—with unique insight into how operations affect the bottom line—to provide this assurance.

In response to this ask, IA is taking several approaches. One approach leverages recognized frameworks such as NIST or ISO to establish a baseline understanding of program maturity.[6] This highlights the level of compliance with leading security policies and practices through interviews and reviews of supporting documentation. These assessments are typically followed by deeper-dive controls testing of higher-risk domains such as network security, vulnerability management, and third-party security.

For organizations with more mature programs, IA may opt for a more advanced approach to adding value—simulated breach attacks, attack and penetration testing or red team operations[7]—to test program effectiveness. During these exercises, skilled security professionals act out real-world cyberthreats such as attempting to access a business-critical server, targeted phishing attempts, or physical breaches of sensitive areas. In these attack scenarios, IA attempts to disrupt cyber defenses and identify gaps in preventive, detective, and response capabilities. These tests uncover real evidence that assures (or refutes) the sufficiency of technology, human, and physical defenses in the event of a real attack.

No matter the approach, by asking the right questions and validating the effectiveness (or ineffectiveness) of cyber capabilities and controls, CAEs are becoming essential allies when building or strengthening robust cyber programs.

Forward-looking CAEs are also taking other steps to provide cyber assurance:

- Leading security certifications and third-party assurance efforts (e.g., Cybersecurity Maturity Model Certification (CMMC) and ISO 27001.
- Peer benchmarking to identify areas of the business that are secure—or exposed—and measuring against industry peers.
- Shifting from historical reporting to forward-looking, impactful, and compelling reports with graphics and visualizations that get to the punchline quickly and succinctly. To build trust, some teams are also highlighting success stories and problems overcome in their audit reports.

Advise: Collaborating with the business and IT around risk to strategic priorities

Many CAEs are on the front lines providing credible, real-time risk-related advice and leading practices to management on strategic priorities such as product launches, new technology plays, and other digital transformation that could impact their company's cyber risk posture. To pull this off, CAEs are:

- **Bringing the talent.**
  Internal audit—often staffed with accountants with limited knowledge of IT infrastructure or cybersecurity—is also challenged by the need to recruit, develop, and retain talent. For specialized cyber audit skills, CAEs are relying on creative delivery models, such as guest auditors, special retention and rotation programs, and co-sourced arrangements with reputable firms.
- **Pivoting to face emerging risks.**
  In our 2020 survey of 60 board members, [8]audit committee chairs, and members, more than one-third suggested that IA is less impactful than it could be. A focus on cyber risks as they emerge is increasing IA's winning brand. Following the massive shift to a remote workforce, many IA teams rallied to quickly assess security around virtual private networks and multi-factor authentication—a true value-add. Auditing at the speed of risk keeps IA resilient" (and relevant) in an era where risk priorities are changing at the speed of light.
- **Innovating to meet fresh challenges head-on.**
  As new areas of cyber risk materialize, the CAE needs to be able to shift to address them, making decisions based on imperfect information in real time using on-the-spot judgment. When rapidity and flexibility are called for, CAEs should look to work on output in a fast-paced, iterative way, prioritizing speed over elegance facilitated by technology and agile methodologies. Innovative CAEs think big, holistically, and strategically.[9]
- **Cultivating stronger relationships.**
  Leading CAEs meet regularly with IT, business, and security stakeholders to discuss teaming and how to bring the auditor's lens to address cyber risks. For example, one large tech company's IA team participates in wargaming, ransomware preparedness, and incident response to rehearse, refine, and test cyber response strategies. This collaboration helps IA teams build trust while demonstrating they have "skin in the game" when it comes to combating cybercrime.

IA should move the needle toward more advisory work:

- 70% of respondents said IA should spend more time on advisory activities
- 92% of respondents said IA should provide insights & help prepare for emerging risks

Global Audit Committee Survey | September 2020

What is showing up on internal audit plans?

Cyber identity & access management

Key risks:

- Inappropriate access rights increase the risk of data breaches, financial losses, and regulatory fines
- Risks related to implementation of IAM solution

IA focus:

- Review access management policies and controls
- Deliver advice and recommendations related to IAM system implementations and transformations

Cyber network & endpoint protection

Key risks:

- Network security device deployment and configuration risks
- Operational risk due to reliance on IT infrastructure

IA focus:

- Review IT security requirements and road map
- Perform an assessment of endpoint security, compliance monitoring, and key configurations

Extended enterprise IT & cyber risk

Key risks:

- Potential reputational damage and regulatory action due to increased reliance on third parties
- Financial impact due to failure of a third-party or subcontractor

IA focus:

- Identify business-critical activities, products, and services
- Review third-party risk management programs with focus on IT security
- Develop or revalidate contingency plans for the higher-risk third parties

Anticipate: Understanding digital transformation to deliver forward-looking cyber insights

Every organization's pace of digital transformation (M&A, new ERP, move to the cloud, etc.) is unique and potentially introduces new cyber risks. As organizations modernize applications, data, and infrastructure, static annual audit plans are no longer adequate. CAEs should shift to continuous, dynamic risk assessments flexible enough to incorporate new risk domains and sources of unstructured data that help IA anticipate and respond to where the greatest risks lie—such as cyber risks. A CAE in the media industry indicated that half of her current audit schedule is focused on IT and cyber audits because that is "where the risks lie." Assessments should aim to leverage CISO's key risk indicators (KRIs) in a dynamic, regularly updated process linked to key data points and presented through dynamic visualizations to understand cyber risk trends. Field results gathered over time from KRI-driven assessments can generate more accurate predictors—and potential areas for IA to focus as the cyber landscape changes leading to real-time assurance.[10]

Of course, not all risks are created equal (and all cannot be avoided); therefore, it's crucial for IA to continuously align with cyber subject-matter experts to get outside-in perspectives as well as maintain ongoing dialog with their IT and security stakeholders on which cyber audits rise to the top of the list. As one manufacturer shifts its business model to become more of a tech company, cloud computing has proliferated. At the same time, shadow IT (without explicit approval from IT) for managing, storing, and processing critical data has significantly increased. To assess this combined risk, IA is performing a cloud assessment and also leveraging an automated discovery tool to assist with the identification, response, and management of shadow IT. Keeping in lockstep with management to provide insights as the business evolves is enhancing iInternal audit's credibility and value.

Accelerate: Making improvements from within

When examining its current and future roles, particularly in addressing cyberthreats, IA can help their organizations accelerate change by focusing on organizational learning, management action, and improvement and change. IA functions should take a fresh approach to the nature of cyber work they perform and focus on improvement in how they communicate with and educate the organizations they serve:

- IA can help facilitate safe and effective environments to accelerate organizational learning around cyber risk. This can help organizations embrace IA as a learning tool, instead of employing standardized assessments that can provoke negative reactions by management or affected teams. Since approximately 95% of cybersecurity breaches are caused by human error,[11] it is paramount that CAEs help the business think outside the box by recommending innovative e-learning techniques, such as augmented reality, virtual reality, and gamification, to drive greater engagement, adoption and changed behavior.
- IA teams can help management accelerate action and remediation. In general, IA concludes its reporting and then leaves any potential issues for management to fix. Alternatively, IA could provide additional value by helping to assemble the relevant teams and personnel from the organization to uncover root causes of these concerns and share perspectives on potential solutions—while maintaining IA's independence and objectivity. This can help capture the value IA has delivered throughout the audit life cycle from identifying issues to implementation of those solutions.
- IA should challenge itself to improve on how it engages with internal clients, such as insightful reporting language and its approach to stakeholder management. IA can accelerate its own improvement—and potential transformation—by embracing a more agile and more continuous improvement mindset leveraging innovative audit techniques and technologies. According to SonicWall, "the second quarter of 2021 saw the highest volume of ransomware attacks ever." With over 100 different strains, SonicWall stated that the ransomware volume jumped from 115.8 million to 188.9 million attacks from Q1 to Q2.[12] In response to ransomware, CAEs are working with advisers to model the latest potential threats against their organization using playbooks based on actual attacks, active investigations, and cutting-edge research—unleashing real and safe attacks in production environments to evaluate control and remediation effectiveness in a low-effort, high-value, automated security assessment.[13]

Conclusion: The dawning of a new age

CAEs are often viewed as too critical based on their comfort of 20/20 hindsight, weighing in only after the action. But in a time of pervasive cyberthreats, CAEs are stepping up and looking forward (and around the corner), filling a vital role that often exceeds their traditional station. Forward-looking CAEs have moved beyond merely earning their seat at the C-suite table; they continue to adapt to meet heightened expectations of their expanding cyber role. IA, more broadly, should evolve in parallel. Together, they can modernize how they assess, engage, and collaborate with the greater organization on cyber risk. This can be achieved in a three-pronged approach:

- **Shift to risk-based cyber audits**—Maximize the risk assessment process to identify emerging cyber risks and threats.
- **Build and maintain effective relationships**—New ways of collaborating with stakeholders doesn't mean IA cannot assert itself independently to assess cyber.
- **Develop an enhanced talent model/skill set**—Leverage alternative resourcing models to upskill certified IT auditors and target cyber specialists as part of recruitment efforts.

CAEs have the necessary tools and, perhaps more importantly, the right perspective to help organizations stay ahead of current and future threats. With the stakes this high, the expanding role of the CAE couldn't come soon enough. Ones that transform and dive headfirst into the cyber pool may be rewarded with greater peace of mind during the next threat; for those who do not, they may find themselves stepping into the board's pressure cooker to answer, "Where was internal audit?"

Contacts

Sarah Fedele
Principal
Deloitte & Touche LLP
sarahfedele@deloitte.com

Pete Low
Managing Director
Deloitte & Touche LLP
plow@deloitte.com

Vipul Patel
Senior Manager
Deloitte & Touche LLP
vbpatel@deloitte.com

Endnotes

1. Steve Morgan, "Cybercrime to cost the world $10.5 trillion annually by 2025," *Cybercrime Magazine*, November 13, 2020.
2. Cloudian, *2021 Ransomware Victims Report*, July 15, 2021; Matt Stieb, "What's driving the surge in ransomware attacks?", *Intelligencer,* September 7, 2021; Robert Anderson, Jr., "How government and industry are failing in battle against ransomware attacks," The Hill, October 21, 2021.
3. Gartner, *2022 Audit Plan Hot Spots*, September 22, 2021; Help Net Security, "The long-term impacts of the pandemic on internal audit teams," September 16, 2021.
4. Deloitte, Internal Audit Risk and Opportunities for 2022, 2021.
5. Richard Chambers, "New survey sheds light on shifting internal audit priorities," AuditBoard, July 28, 2021.
6. Databrackets, "Comparing NIST, ISO 27001, SOC 2, and other security standards and frameworks," September 9, 2020.
7. Crowdstrike, "Red team vs blue team cybersecurity simulation defined," January 6, 2022.
8. Adam Regelbrugge et al., Responding to the innovation imperative: A guide to accelerating innovation in Internal Audit, 2020.
9. Ibid
10. Laura Skov, "A risk assessment path to real-time assurance," *Deloitte Risk & Compliance Journal for the Wall Street Journal,* January 13, 2020.
11. "X-Force Threat Intelligence Index 2022," IBM Security, February 2022.
12. SonicWall, *2022 SonicWall Cyber Threat Report,* 2022.
13. Deloitte, *Leveraging Breach and Attack Simulation (BAS) to prioritize security remediation and reduce risk,* 2020.

Deloitte.