

# Auditors Have a Role in Cyberresilience

Cyberthreats are an issue for any organization or individual anywhere in the world due to the increasing dependence on computer systems, infrastructure, the Internet, social media and technological innovation. The global cybersecurity ecosystem has dramatically evolved, and keeping it safe has become a complex issue, largely because cybercriminals' persistent attacks evolve faster than security solutions are being developed.

Implementing a successful control environment and cyberresilience in an organization is no longer the responsibility of IT departments only. Boards of directors (BoDs) are, ultimately, liable and responsible for the survival of their organizations and, in today's interconnected world, cyberresilience is a major responsibility of the BoD and the entire organization's staff, executives and individuals included. The changes and improvements that come with new technology and innovation and their adoption by organizations have become more complex than the evolution of audit/control, thereby hindering its ability to provide assurance over cybersecurity. Hence, the increasing complexity of cybersecurity and techniques is worrying organizations significantly because they have not changed much in their control approaches.

Security is not a product but a process, and cybersecurity threat control is not only the responsibility of IT professionals but the responsibility of every individual in the organization, especially the three control defense layers (operational management, risk and security management, and internal audit). It is vital that audit takes a leading role in determining whether a regular and disciplined approach exists to evaluate and strengthen the effectiveness of cyberrisk management.

Internal audit plays a crucial role in assessing an organization's cybersecurity risk by considering:<sup>1</sup>

- Who has access to the organization's most valuable information?

- Which assets are the likeliest targets of cyberattacks?
- Which systems would cause the most significant disruption if compromised?
- Which data, if obtained by unauthorized parties, would cause financial or competitive loss, legal ramifications or reputational damage to the organization?
- Is management prepared to react immediately if a cybersecurity incident occurred?

In addition, The Institute of Internal Auditors (IIA) supplementary Global Technology Audit Guide (GTAG) explores emerging risk and common threats



## **Shemlse Gebremedhin Kassa, CISA, COBIT 5 Foundation, CEH, CMC, MSCS**

Is a business and information technology professional consultant. He has a multidisciplinary academic and practicum background in business and IT with more than 15 years of experience in management, IT, accounting, budgeting, auditing and security consultancy in the banking and financial industries. He currently serves as chief executive officer and cybersecurity consultant to MASSK Group. Kassa is highly motivated and engaged in cybersecurity and audit program/research, and he strives to update current technology developments to keep up with the dynamically changing world and ever-increasing need for technology management. He has published articles in local and international journals on business and technology.

faced by all three lines of defense and presents a straightforward approach to assessing cybersecurity risk and controls.<sup>2</sup>

Since the early 1970s, IT controls addressing IT-related risk posed to accounting information systems have been considered one discipline. Over the years, however, organizations have expanded these practices to address areas beyond the IT controls necessary for accounting systems. In 1996, ISACA® developed the COBIT®<sup>3</sup> framework, at which point the concept of IT auditing took a giant leap. As a result, many organizations now offer services that focus on IT controls that address the risk to cybersecurity and the availability and confidentiality of an organization's information and systems.

“THE SECURITY POVERTY LINE IS THE POINT BELOW WHICH AN ORGANIZATION CANNOT EFFECTIVELY PROTECT ITSELF AGAINST LOSSES TO CYBERATTACKERS.”

### Risk Related to Cybersecurity

A cybersecurity assessment can also necessitate a risk-based IT audit plan, which can help determine audit frequency and level of risk. The increase in cybersecurity attacks creates an urgent need for strategies and the advancement of cybersecurity risk management. In an ideal world, cybersecurity plans are well designed, routinely tested and perfectly executed; everyone knows their roles and follows the policies and practices designed to protect the organization from cybersecurity attacks. However, the reality is that in many cases, the attention and commitment needed to manage cyber risk from planning to action is inconsistent and not always promising. For example, the 2017 African Cybersecurity Survey revealed that more

than 95 percent of African organizations in private and public sectors are either operating at or below the security poverty line.<sup>4</sup> The security poverty line is the point below which an organization cannot effectively protect itself against losses to cyberattackers. Its core characteristics include:

- Lack of skill
- Lack of resources
- Lack of tools
- Lack of basic necessities
- Lack of ability to resolve catastrophic cybersecurity issues without the help of external parties

Most of these organizations spend a maximum of US\$1,500 annually on cybersecurity technologies and services.<sup>5</sup>

Cyber risk is a business risk, not just an IT risk and, for this reason, organizations performing a risk assessment of the threat landscape should begin by looking at the tone at the top. Typically, the risk assessment is owned by the enterprise-level functions; however, it can and should be a joint effort between the audit function and the business functions to ensure that there is synergy between the two. Risk assessments are intended to help identify and address the gaps that may widen in the event of a cyberattack due to a lack of key controls.<sup>6</sup>

Factors that affect the audit approach are innovation and new technologies such as the Internet of Things (IoT), the advancement of mobile technology, cloud computing, grid technology and social media. These technologies are at risk for major breaches of information, and they generate rapid transformation in the IT risk landscape. Established security measures such as antivirus and antimalware software and firewalls are now insufficient to protect against IT risk. Instead, organizations should focus on defense-in-depth strategies and start working on cyber resilience strategies to reduce the potential impact of a breach.

## Cybersecurity Program Goal and Audit Objectives

The advancement of information systems and technology offers a vital benefit for enterprises. However, technology evolution also brings ever-increasing challenges due to the existence of hackers, malware, viruses and cybercrimes. Therefore, frequent and strong follow-up is required via regular information systems security audits. Nevertheless, the scarcity of professionals and the lack of well-suited frameworks in this domain are frequently cited as main barriers to success.<sup>7</sup> Audits have various shapes and have diverse focuses with respect to cybersecurity testing; these aspects of the cybersecurity audit program should require frequent testing. The audit objectives should be aligned with cybersecurity goals to achieve the best business outcomes. One of the primary goals of any cybersecurity program should be to limit the attractiveness of the enterprise as a target for attackers. The more time it takes an attacker to penetrate a system, the less desirable that target becomes.<sup>8</sup> Hence, audit's goal is to provide advice to prevent or detect the attacker's attempt by hiding vulnerable areas of an enterprise's system before they can be exploited by attackers on a continuing basis.

Staying safe is no longer about simply preventing a hack. It is about staying ahead of hackers who are already inside the organization. The best way to do this is by having three lines of defense in the operational managers, IT risk management and compliance, and internal audit roles, each of which contributes to the overall assurance of the cybersecurity program.

## The Auditor's Critical Role in Cyberresilience

The role of auditors in any enterprise is designed to add value by providing independent objective assurance on the efficacy and efficiency of the organization's operation to the responsible stakeholders. Cybersecurity audit assessment also follows a similar approach to other assessments performed by auditors, but it requires a deep understanding of technology (i.e., integrated systems, applications, technologies), supporting

“CYBERRESILIENCE IS NOT A ONE-TIME EFFORT BUT A CONTINUOUS AND PROGRESSIVE PROCESS OF TASKS THAT REQUIRE REASONABLE INVESTMENT, RESOURCES AND PROFESSIONAL SKILLS.”

technologies (i.e., routers, firewalls, servers, workstations) and the environments involved.

As the third line of defense, internal auditors play an important role in coordinating with the second line of defense, particularly the cybersecurity function. Internal audit activity can be consulted regarding:<sup>9</sup>

- The relationship between cybersecurity and organizational risk
- Prioritizing responses and control activities
- Auditing for cybersecurity risk mitigation across all relevant facets of the organization

Cyberresilience is not a one-time effort but a continuous and progressive process of tasks that require reasonable investment, resources and professional skills. To achieve an optimum level of cyberresilience, an organization should address four important task layers. The internal audit practices on cybersecurity emanate from these four methods of attaining cyberresilience. It is recommended that, in any organization, internal auditors perform an audit assessment and consulting activities for each of the four categories of cyberresilience, but all organizations should incorporate qualified IT auditors within the internal audit team. The four areas are the responsibility (**figure 1**) of each of the three lines of defense players and may be performed in one or more categories, but the focus here is to present the responsibility of the third line of defense players (internal audit) only. Those task layers are:

- **Identify, protect, shield, defend and prevent—**  
The preliminary action of cyberresilience is effectively identifying associated risk. Recommended solutions at this stage are

Figure 1—The Role of Auditors in Cyberresilience



implementing an information security management system (ISMS) using best practice standards and frameworks such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/IEC 27001 *Information security management*<sup>10</sup> and COBIT® 5 for *Information Security*,<sup>11</sup> and performing regular penetration testing.

“MOST OF THE TIME, GOVERNANCE AND MANAGEMENT OF CYBERSECURITY ARE NOT CONSIDERED MAIN ACTIVITIES, BUT THEY ARE CRUCIAL FOR CYBERRESILIENCE FROM INCEPTION TO DEATH.”

On this level, internal auditors should first understand and identify how much risk

cyberattacks pose and advise on what should be done by responsible stakeholders to defend and prevent the possible loss of assets. Some of the auditor's major tasks here include:

- Review cybersecurity policies and procedures and suggest enhancements.
- Carry out access management processes audit.
- Review cyberresilience activity using a recognized comprehensive framework.
- Evaluate the adequacy of the network segmentation and database integrity strategy.
- Evaluate cyberinsurance requirements and coverage.
- Perform a penetration test.
- **Monitor, hunt, detect**—Establish the required monitoring areas (i.e., security operating center [SOC]) with best practices such as security information and event management (SIEM), which provides real-time analysis of security alerts generated.

This phase looks at how to audit cybersecurity monitoring and detection practices that the enterprise has implemented to find malware, viruses, malfunctions and hacking attempts. It is also important to evaluate the functionality of end points, the functionality of networks, ways to hunt malpractice in the system, ways to use process monitoring to trace activities, etc. Some of the auditor's main activities here are:

- Review and ascertain whether privileged access activity is monitored.
- Perform monitoring and detection in collaboration with the chief information security officer (CISO).
- Ensure third-party activity on penetration tests.
- Review vulnerability assessment results, frequency and corrective measures taken.
- Check the effectiveness of cyberawareness programs.
- Hunt information flows between physical and logical systems.

- **Respond, recover, sustain**—Survive incidents and enable a return to normal operation after a cyberattack. Recommended steps here include implementing a business continuity management system (BCMS) using ISO 22301 *Societal security—Business continuity management systems—Requirements*<sup>12</sup> or other related frameworks to develop and implement an incident response management program.

Auditors are engaged in advising, reviewing and sometimes participating in assessing damage and its impact. Auditors should continue advising management and business units to help sustain operations and restore and recover from cybersecurity incidents.

Some specific auditor activities include:

- Business impacts are evaluated and incorporated into the strategy.
- Evaluate and test whether regular backups of all critical systems take place.
- Review testing of incident response plans.
- Review data storage culture on and offsite and its functionality.
- Participate in the IT department's regular recovery testing procedures.
- Participate in disaster recovery and continuity exercises or testing.
- Assess the redundancy of the operating system, storage, power, core database server and cabling, and generally evaluate whether the concurrency rule is applied for core activities.

- **Governance and management**—Security is not only technical but also operational, so cybersecurity risk, compliance and education must be addressed.

Most of the time, governance and management of cybersecurity are not considered main activities, but they are crucial for cyberresilience from inception to death. Therefore, cyberresilience is an expensive process that requires strong attention, involvement and direction of management and governance.

“AUDITORS CAN BE MAIN PLAYERS IN CHANGING THE ATTITUDE AND WORKING CULTURE OF THE ORGANIZATIONS IN THE CYBERSECURITY AND CYBERRESILIENCE PROCESS.”

In this phase, auditors are engaged in some critical tasks, including:

- Continuously evaluating cybersecurity practices, policies and plans
- Reviewing business continuity and disaster recovery plans
- Reviewing the alignment of IT policies and procedures with business
- Reviewing user awareness and training programs
- Communicating risk and audit results to the board and executive management in a timely manner
- Providing assurance on readiness and response efforts
- Creating a collaborative work environment with IT and other parties
- Promoting communication and coordination about cyber risk
- Communicating the need for cyberresilience to the entire enterprise
- Participating in IT projects to ensure security before purchase or service
- Evaluating vendor, interconnected third-party and supplier management processes



## Conclusion

Cyberresilience is a key process that all organizations must manage well. To that end, auditors can be main players in changing the attitude and working culture of the organizations in the cybersecurity and cyberresilience process. Experiences in cybersecurity show that organizations with little budget can still maintain reasonable security levels when they understand the critical areas that need to be protected the most.

Certain cybersecurity domain assessments should be partially covered by existing internal IT audits and other audit lines of an organization; however, many capabilities have historically not been reviewed by internal audit only and need to be outsourced to external auditors and subject matter experts or consultants as appropriate. As internal audit departments begin to develop capabilities surrounding cyberresilience in the coming years, many of the challenges they can expect to face will be similar to challenges addressed when absorbing IT audit functions.

## Endnotes

- 1 The Institute of Internal Auditors, *Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk: Roles of the Three Lines of Defense*, <https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-Risk-Roles-of-the-Three-Lines-of-Defense.aspx>
- 2 Ibid.

- 3 ISACA®, *COBIT® 2019*, USA, 2018, [www.isaca.org/COBIT](http://www.isaca.org/COBIT)
- 4 Serianu, *Africa Cyber Security Report 2017*, Kenya, 2017, [www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf](http://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf)
- 5 Ibid.
- 6 Khan, M.; "Managing Data Protection and Cybersecurity Audit's Role," *ISACA® Journal*, vol. 1, 2016, <https://www.isaca.org/archives>
- 7 Kassa, S. G.; "Framework for Protecting Your Valuable IT Assets," *Practically Speaking* blog, 26 September 2016, <https://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=333>
- 8 ISACA, *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, USA, 2017, <https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Auditing-Cyber-Security.aspx>
- 9 Op cit Institute of Internal Auditors
- 10 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), *ISO/IEC 27001 Information security management*, Switzerland, 2013, <https://www.iso.org/isoiec-27001-information-security.html>
- 11 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, [www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx](http://www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx)
- 12 International Organization for Standardization, *ISO 22301:2012 Societal security—Business continuity management systems—Requirements*, Switzerland, 2012, <https://www.iso.org/standard/50038.html>