Whitepaper Guidance for Healthcare Internal Auditors and Compliance Professionals

Cyber Assurance: How Internal Audit, Compliance and Information Technology Can Fight the Good Fight *Together*

ahia
Assoc. of Healthcare Internal Auditors

Deloitte.

INTRODUCTION

Hospitals, insurers, life sciences, and other healthcare organizations have been adopting new technologies at a breakneck pace. In fact, adoption has outdistanced many organizations' ability to identify, manage, and oversee the risks associated with those technologies.

Board members of healthcare organizations need a clear understanding of the organization's overall exposure to cyber risks but sometimes the picture is unclear. As a result, boards and their audit and compliance committees are calling upon internal audit and/or compliance to provide assurance regarding the organization's management of cyber risks. While these governing bodies benefit from cyber security education provided by the chief information officer (CIO), chief technology officer (CTO), and chief information security officer (CISO), education efforts can fall short of the boards' needs for clarity and understanding for three reasons:

- Information Technology and Security department reports and presentations are often complex, difficult to connect to business objectives, and focused primarily on technical risks that may put the board in unfamiliar territory. Boards aren't currently required to include cybersecurity technical specialists; existing members may be more comfortable with financial or operational internal controls and regulations.
- IT and security functions cannot provide the independent, objective assurance that board members desire when it comes to cybersecurity.
- Due to news reports of breaches and emerging legislation from regulatory, governmental and auditing entities, many board members have a heightened awareness of cyber risks.

Technology adoption follows the same trajectory in healthcare as it does in many organizations: adoption comes first and if the technology adds value for patients, providers, customers, and other stakeholders, it is institutionalized. Only after technology is institutionalized—and poses significant threats—do most management teams seriously address a technology's risks.

Creating a risk management program prematurely is arguably wasteful, but organizations that delay too long may find themselves playing catch-up to address technology adoption risks.

This delay and struggle to catchup cycle is evident in the adoption of mainframe computers, personal computers and the Internet, mobile devices, cloud computing, and our current age of total digitalization. These technologies are so pervasive and varied that we simply use the term "cyber" to describe the environment and related risks.

Cyber risks may present challenges for healthcare internal audit and compliance functions in evolving their cyber assurance program and capabilities. Discussions with board members and senior executives indicate an increasing desire for assurances related to cyber risks and cybersecurity beyond Information Technology reporting; in the near future, cyber auditing may be business as usual much like Sarbanes-Oxley (SOX) audits. No other organizational functions have the independence, objectivity, organization-wide perspective, and skill sets needed to

deliver that assurance. While specific cyber risk assessment and auditing skills may be in short supply, they can be acquired through training, rotational programs, and co-sourcing. External assistance can help internal audit and compliance develop a comprehensive view of cyber assurance needs.

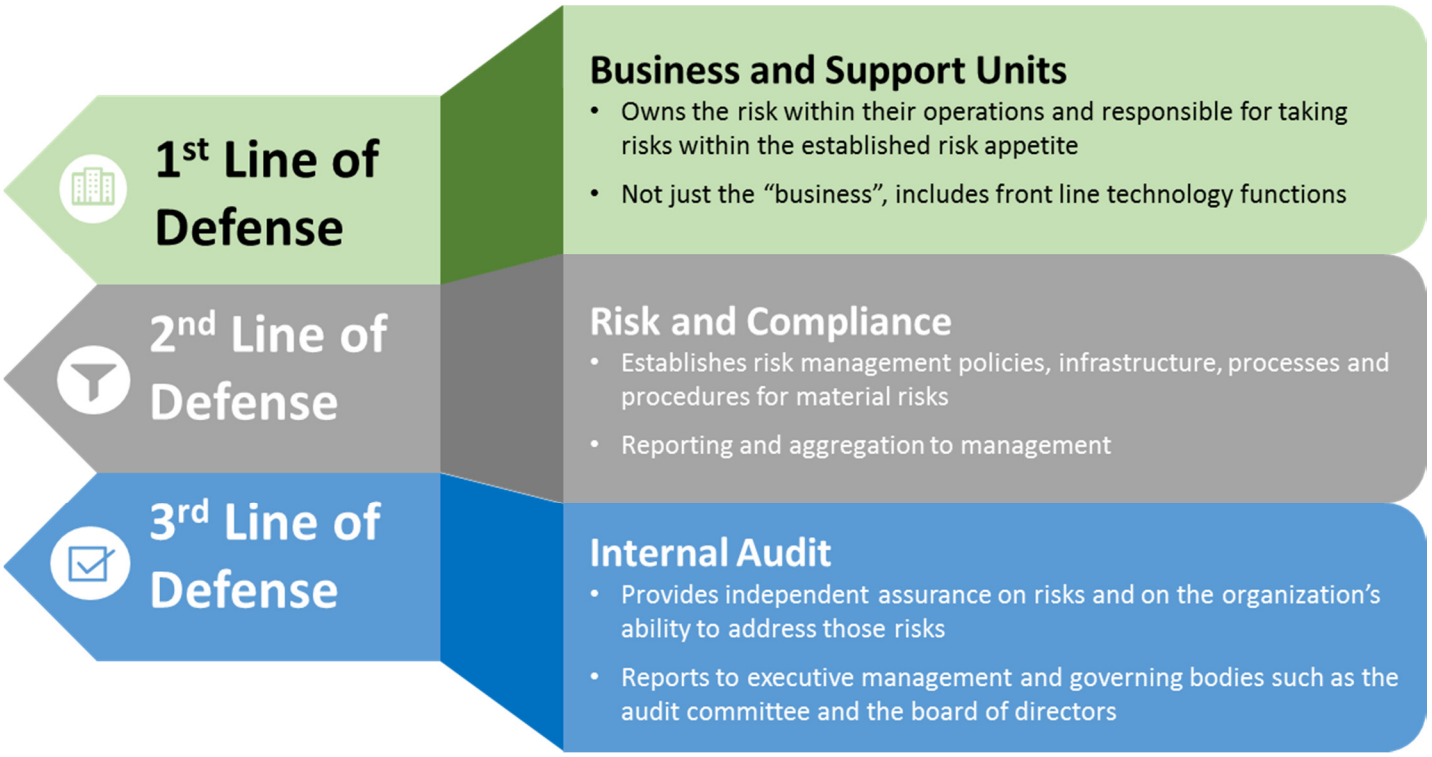
The key question for both the internal audit and compliance functions that have yet to engage in cyber assurance is how to go about it. Although cyber assurance may seem daunting, it is a fairly straightforward process if undertaken systematically.

WHERE TO BEGIN

Begin with the rationale. Board members and management need independent assurance on the effectiveness of cybersecurity risk management and controls. Assurance is not just a "one and done," effort; rather it should be a consistent measurement of the cybersecurity program based on an assurance cycle. Moreover, after an assurance program has been established, internal audit and/or compliance can also provide consultative support to management around cybersecurity.

Perhaps the best rationale for a cyber assurance program is enablement of internal audit as the third line of defense in risk management and governance (the first line is operations, and the second line is internal control monitoring, compliance, and risk management). Management and, ultimately, the board are responsible for understanding and addressing the full range of risks posed to the organization. Internal audit's role as an independent assurance provider is essential to sound risk management and governance.

LINES OF DEFENSE



After the rationale is accepted, the cyber assurance plan should be defined. A solid cyber assurance plan should be:

- Structured as an ongoing risk-based program
- Built around a cyber assurance framework
- Executed on an assurance cycle

An Information Security risk-based program recognizes that different assets and risks require different levels of risk management. To gauge resource allocations, the organization must first understand which digital assets are most valuable, the vulnerability of those assets, and the likely impact if those assets were compromised or stolen. Valuable assets include patient records and customer data, contracts and plans, analytics related to fees and services, ongoing or completed research and other intellectual property, and personal information on organizational leaders and staff. In addition, biomedical devices used for patient treatment and monitoring and other applications specific to the organization must be appropriately secure.

One key goal is to identify the "crown jewels"—the digital assets with the highest value, which require the highest levels of protection. Next, the analysis identifies other digital assets and the levels of protection they warrant based on their value and vulnerability. This risk-based approach then tailors cyber assurance activities to the value and vulnerability of digital assets.

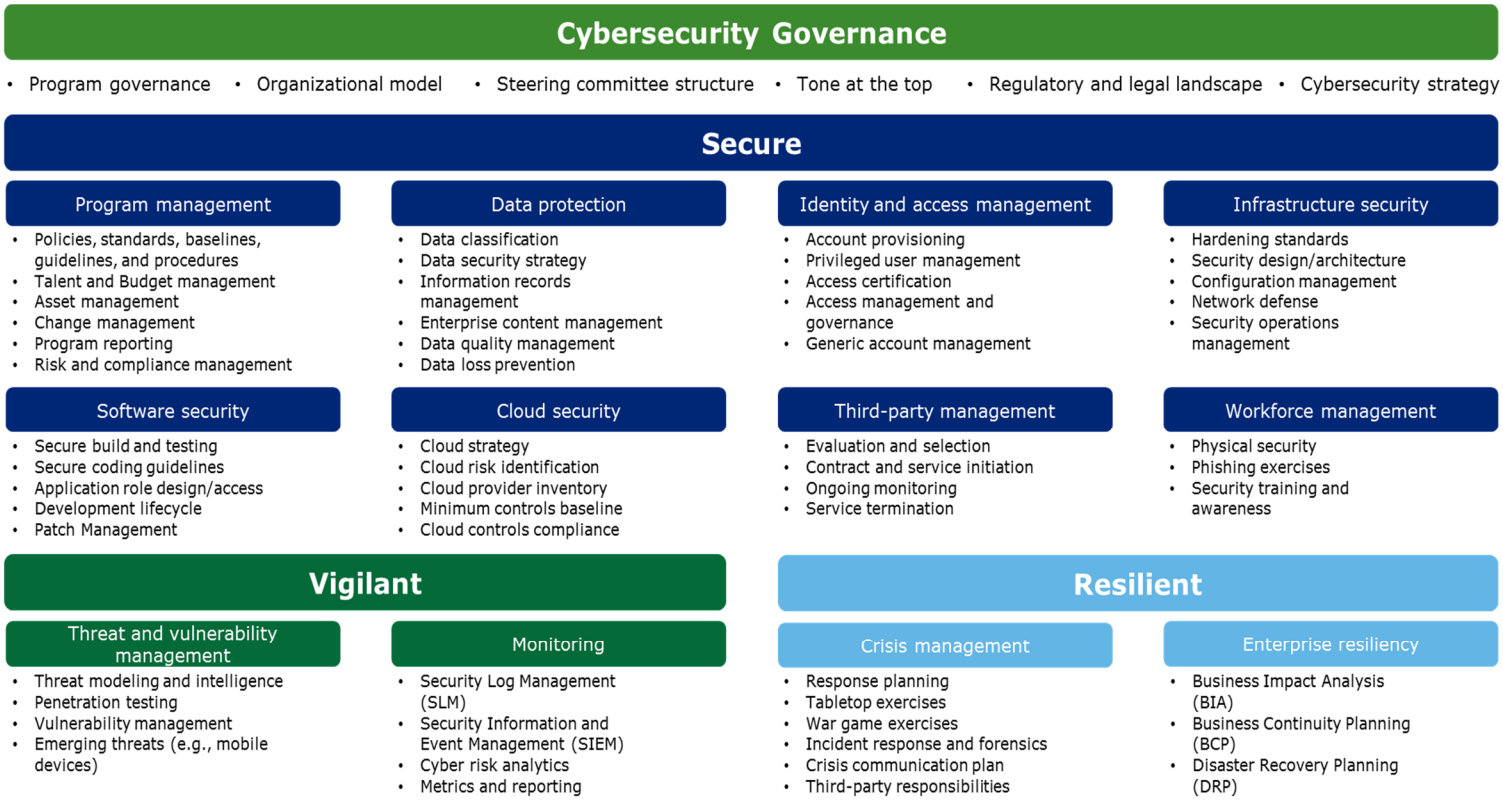
A ***cyber assurance framework*** is perhaps the most important component; it is the yardstick that measures the program and promotes understanding of the cyber risks the organization faces.

Although no standardized framework currently exists that addresses all of the cyber assurance issues that an audit committee faces, organizations have presented frameworks that focus on aspects of cyber risk. These organizations include the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Committee of Sponsoring Organizations of the Treadway Commission (COSO), ISACA, and the Center for Internet Security (CIS). These organizations' frameworks have specific areas of focus, such as information security or technology risk, and elements of those frameworks have been adopted by primary stakeholders with responsibility for cyber risk.

An organization can also create its own cyber assurance framework based on applicable elements of existing frameworks. A comprehensive framework specific to healthcare should include alignment with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

Comprehensive cyber assurance frameworks are developed to assist internal audit and/or compliance and can be customized to an organization's specific requirements and environment. An organization's framework should be rationalized and focused on cyber assurance needs, the specific coverage areas desired by internal audit and/or compliance, and aligned with relevant industry standards such as NIST, ISO, COSO, HIPAA, HITECH and other leading practices.

Example: Cyber Assurance Framework



A comprehensive cyber assurance framework helps organizations maintain a secure, vigilant, and resilient environment and identifies specific domains and characteristics that contribute toward that end.

This framework enables the team to consider a wide range of risks across various domains and sets the stage for a comprehensive risk assessment, a necessary early step in virtually any risk management, governance, and assurance effort. The framework also promotes broad discussion, review, and reporting of cyber risks and cyber risk management mechanisms.

An ***assurance cycle*** ensures that cyber risks receive targeted levels of audit attention. The assurance cycle should relate to the value of digital assets and potential threats, rather than to a rigid periodic cycle. Scheduled cyber audits of specific domains will help ensure appropriate areas are reviewed, but the cycle should be dynamic rather than static. For example, critical domains might be reviewed annually or biannually while less critical ones could be reviewed once or twice in a three-year period. Domains subject to newly emerging threats should receive focused attention as well.

The assurance cycle should link to regulatory mandates while recognizing that cyber threats usually outpace regulatory review and reporting requirements.

GETTING WITH THE PROGRAM

A program approach includes a comprehensive risk assessment that leads to a multi-year plan of risk-based assurance cycles. With the plan in place, program execution can begin.

Program execution calls for the right people with the right skills, which can present a challenge. Recent research[1] found that 45 percent of surveyed chief audit executives (CAEs) in life sciences and healthcare (LSHC) organizations view specialized IT skills—that is, cyber domain-specific skills—as the second largest skill gap their internal audit and compliance groups face in the next three to five years (after data analytics skills, at 49 percent). Only 20 percent of surveyed LSHC CAEs noted that their groups currently have those skills in-house. Skill gaps can be addressed through outsourcing, co-sourcing, and training, and they must be addressed if internal audit and compliance are to provide the assurance boards are now seeking.

Execution also calls for the right tools, tests, and questions. Useful questions for internal audit to ask include:

- Where might we be allocating too many resources to protect low-value digital assets?

[1] *Evolution or irrelevance? Internal Audit at a crossroads Deloitte's Global Chief Audit Executive Survey*, 2016, Deloitte Touche Tohmatsu Limited < www.deloitte.com/globalCAEsurvey >

- Where might we be allocating too few resources?
- How might the organization rationalize, harmonize, and optimize cyber controls and compliance efforts?
- How can we reduce the cost and increase the quality of cyber risk management?

Program execution flows through to reporting, which should be accurate, timely, relevant, and useful to stakeholders. Avoid IT jargon. Speak the language of business and risk management. Use visualization tools, such as heat maps and bubble charts, to bring out key points and relationships for stakeholders.

The simplified chart below maps back to the domains in the Cyber Assurance Framework and shows how the organization's risk management can be characterized as adequate (green/unshaded), of concern (yellow/lightly shaded), or of serious concern (red/darkly shaded). An actual report would provide indicators at finer levels of domain detail so stakeholders could hone in on specific concerns.

Sample Cyber Risk Reporting Tool

Visualization tools enable internal audit to communicate more effectively. These tools also enable internal audit to expand on areas "of concern" and let users who want more detail to drill down.

While internal audit can, and should, initiate the effort to provide or upgrade cyber assurance, this should not be a unilateral effort. A sustainable cyber assurance program calls for senior executive support, adequate resourcing, and strong organizational commitment.

ESTABLISH A STEERING COMMITTEE

To initiate a higher level of cyber assurance and obtain ongoing guidance, the organization should form a cybersecurity steering committee. This committee should include senior representatives of compliance, internal audit, information security, information management, legal, data owners and business management. Reporting to the board's audit and/or compliance committee, this committee:

- Assists the audit and/or compliance committee in establishing strategy, expectations, and accountability for cybersecurity and cyber incident preparedness
- Evaluates available internal and external resources and recommends funding to initiate and maintain an effective cybersecurity and cyber assurance program
- Recommends enhancements to existing and future cybersecurity initiatives, and engages in discussion and approval of the cyber assurance framework and other program components.

This committee facilitates senior-level engagement, demonstrates organizational commitment to cybersecurity and cyber assurance, and enables the planning and resourcing needed to launch and maintain the cyber assurance program. If the committee already exists, internal audit should assess its member coverage. The existing committee may solely focus on Information Technology and fail to incorporate the broader organizational stakeholders whom are also impacted and play a role in cyber security.

Respond Now to Rising Risks

As media reports of breaches regularly remind us, no organization is immune to cyber risks, threats, and incidents. Board members and senior executives in healthcare understand that those managing cybersecurity cannot provide objective, independent assurance on cyber risks or on the organization's ability to address those risks. These stakeholders are looking to internal audit to provide that assurance. This is the time for internal audit and compliance to work together to plan, resource, and initiate a cyber assurance internal audit program. Taking action now can reduce pressure when cyber assurance requirements are promulgated over the near to medium term. Benefits include enhanced security for digital assets, improved compliance with related regulations, and greater organizational impact and influence for internal audit and compliance.

ABOUT THE AUTHORS

Debra A. Muscio

SVP, Chief Audit, Ethics and Compliance Officer
Community Medical Centers
Fresno and Clovis, CA

Ms. Muscio is driven to help the internal audit and compliance profession raise the bar on security compliance awareness, risk assessments, remediation, monitoring and auditing by aligning teams that communicate and collaborate to achieve their goals. With over 30 years of experience in the Internal Audit and Compliance profession, she has championed the alignment of Security Compliance and Audit with independent reporting to the audit and compliance committee of the board. She has served on various boards and committees in the Healthcare Audit and Compliance Profession and continues to educate and mentor leaders at all levels to enhance knowledge and awareness.

Glenn M. Wilson

Internal Audit Senior Manager, Deloitte & Touche LLP
Cyber Assurance Services

Like you, Mr. Wilson is driven to raise the bar on security by helping organizations lower their risk. With over two decades of technical, real-life, in-the-trenches information security experience, his view on security can be radically different. Glenn helps many of the world's largest organizations reduce their risk by helping them manage cyber more effectively. He has governed as chief information officer (CIO), served over a dozen boards, educated audiences, and has the keen ability to translate complex technical issues into plain English for executives and other decision makers.

Contacts

Deloitte
Glenn M. Wilson
Deloitte & Touche LLP
555 West Fifth St. Suite 2700, Los Angeles, CA 90071-3462
Tel/Direct: +1 213-688-6976 | Fax: +1 213-673-5879 | Mobile: +1 949-612-5589
glennwilson@deloitte.com | www.deloitte.com
LinkedIn: http://www.linkedin.com/in/gmw13
Twitter: https://twitter.com/DeloitteGlenn

Community Medical Center
Debra Muscio
789 N. Medical Center Drive East, Clovis, CA 93611-6878
Office +1 559-324-4830
dmuscio@communitymedical.org

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org.

AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. They are intended to supplement and support the mandatory requirements of formal professional standards. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities and design audit approaches. A ***white paper*** *is an authoritative report or guidance that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services. Interested?*

Contact ***a member of the AHIA White Paper Subcommittee:***

Alan Henton, AHIA White Paper
Subcommittee Chair
alan.p.henton@vanderbilt.edu

Mark Eddy
mark.eddy@hcahealthcare.com

Linda McKee
lsmckee@sentara.com

Mark Ruppert
mruppert@socal.rr.com

Debi Weatherford
debi.weatherford@piedmont.org

Todd Havens, AHIA Board Liaison
todd.havens@vanderbilt.edu