THE FUTURE OF CYBERSECURITY IN INTERNAL AUDIT

A joint research report by
the Internal Audit Foundation
and Crowe

By John Jamison,
Lucas Morris, and
Christopher Wilkinson

Table of Contents

Contributors

John D. Jamison, CISSP, CISA, CFE
Crowe

Lucas J. Morris, CISSP
Crowe

Christopher R. Wilkinson, CISSP
Principal
Crowe

Introduction and Executive Summary

Over the course of just a few years, cybersecurity has grown into one of the most significant risk management challenges facing virtually every type of organization. Is the internal audit function keeping pace with this rapidly changing area of risk? This report examines this question and, based on a survey of internal audit and cybersecurity professionals, offers some observations on how internal audit departments are adapting in order to address cybersecurity risks.

A decade ago, the internal audit function evolved and adapted to the increasingly important role that information technology (IT) was playing in all aspects of business operations. Today, internal audit faces the need to adapt once again to address the critical risks associated with cybersecurity.

Recognizing this need, the Internal Audit Foundation and Crowe, in collaboration with The Institute of Internal Auditors' (IIA's) Audit Executive Center, conducted a limited survey of IIA members in order to understand how internal audit has begun to adapt to this new risk landscape.

This report offers a summary of key findings from that research and provides insights into some current internal audit and cybersecurity policies and practices. In addition, the report's authors draw on industry experience and observation based on their working relationships with internal audit functions across a broad range of industries.

The survey respondents represented organizations of various sizes in a variety of industries. Their positions and job titles covered the full range of relevant responsibilities including chief audit executives (CAEs), audit directors, senior managers, managers, and internal audit staff. Their responses provide insights into the future role of internal audit in dealing with cybersecurity issues and illuminate several important areas of concern. These insights fall generally within three broad categories:

- **Evolving relationships.** Cybersecurity concerns are driving organizations to redefine the boundaries across the three lines of defense, and static relationships will not be equipped to address the emerging risks. This means that internal audit's relationships with other key players, such as IT departments, information security (InfoSec) professionals, and risk management groups, must continue to evolve.
- **Internal audit's increasing role.** To maintain effectiveness and credibility, internal audit professionals must have a clear grasp of the larger issues and interdependencies involved. This grasp includes understanding how much emphasis should be given to the prevention, detection, and response elements of a cybersecurity program as well as the sufficiency of the controls and testing. Internal audit must assert itself in independently assessing the rapidly evolving and escalating risk environment. Because the costs of any failure in the first or second lines of defense are so high, internal audit must be extra vigilant.
- **Access to cybersecurity expertise.** As internal audit's role evolves, it will require access to personnel resources with technical expertise that is currently in high demand. However, such resources can be difficult and expensive to attract and retain. How can internal audit ensure its readiness to meet this challenge and position itself as knowledgeable, competent, and ready to address the issues? In many cases, internal audit will need to revisit its relationships with IT and InfoSec professionals in order to fill in the gaps.

The goal of this report is to examine current industry perceptions regarding those areas of concern. It also aims to synthesize contemporary industry perspectives into actions that could help audit shops prepare to address cyber risk by building relationships, identifying and adapting their role, and developing or acquiring the knowledge needed to get the job done.

Cybersecurity began as an isolated, sometimes mysterious, technical area within companies. Nevertheless, it has quickly grown into a global governance, risk, and control issue involving nation states, organized crime, individual hackers, government agents, business users, and other organizations.

The stakes are high, with significant risks and potential rewards for all involved. Internal audit teams are encouraged to consider the findings in this report in order to be prepared to respond proactively to this rapidly evolving area of risk.

Relationship Management in Cybersecurity

Maintaining effective relationships with other groups and departments within the organization is always a critical concern for the internal audit function. It is important for internal audit to understand the universe of relationships within an organization in order to better protect it.

Although internal audit also must develop and maintain sound relationships with various external groups — such as regulatory agencies, industry standard-setting and professional organizations, and relevant law enforcement authorities — the focus of this report is on internal audit's relationships with other groups within the organization. Cooperative, positive relationships with those being audited can greatly expedite the audit process and improve the quality of the audit results.

At the same time, however, internal audit must be careful not to allow such relationships to compromise its necessary independence. While independence is essential, a confrontational or adversarial approach can hinder internal audit's effectiveness. It is a matter of striking the right balance, and the methods for determining and achieving that balance will vary widely from one organization to another.

In the case of cybersecurity, the ability to strike the right balance can be further complicated by the need for specialized expertise and technical knowledge, which often are available only within the IT or InfoSec departments themselves. The internal audit function can benefit when audit professionals make a special effort to understand the backgrounds, mentalities, and motivations of the technical personnel who are being audited and who also must provide some of the technical expertise that internal audit needs to perform its function.

To gauge how effectively internal audit communicates with personnel in the cybersecurity realm, survey participants were asked specifically about the collaboration they experience within their own organizations in relation to four specific departments: IT, information security, risk management, and other compliance functions. The survey asked participants
to rate the level of collaboration they experienced on the following scale:

0: We do not perform audits of this area or have no relationship at this time.

1: There is little communication and few pre-agreed upon responsibilities for assessments.

2: Communication with audit is formalized but limited to assessment requests.

3: Communication is frequent and goes beyond audit requests and assessments.

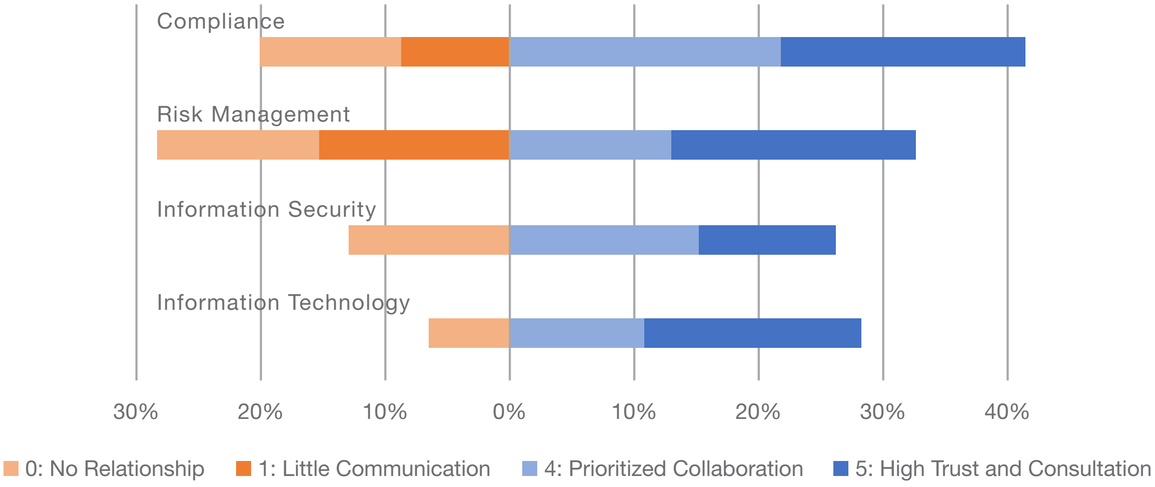
4: Communication by the department is prioritized, frequent, and includes sharing of ideas and resources.

5: There is a high degree of trust between audit and the department, including being consulted as a priority, albeit independent, partner throughout the year.

The results revealed that internal audit is more likely to at least have formalized audits and communication with the IT and InfoSec departments, which is good. The results also suggested such audits and communication are less likely to be in place with the compliance and risk management functions, although these results could be skewed by smaller organizations that may lack formalized departments in these areas.

Participants' responses based on this rating scale produced the following results:

Exhibit 1: Very Weak and Very Strong Relationships With Internal Audit



Source: Crowe analysis

Survey respondents were more likely to report strong relationships with compliance and risk management. These results, as illustrated in Exhibit 1, suggested that internal audit is more likely to have either a very strong relationship with both the compliance and risk management functions, or a very weak relationship with these groups. For compliance, the combined responses for ratings zero, one, four, and five was 62 percent. For risk management, the combined responses for these very strong and very weak relationships were 61 percent.

On the other hand, the percentage of companies stating that they maintain a relationship characterized by the sharing of resources and high trust levels was lowest with the IT and InfoSec teams, despite the fact that they reported a higher level of communication with these departments. This situation reinforces the perception that barriers exist between the internal audit function and the IT and InfoSec departments.

Information Technology

Because technology is a key component in any organization's ability to achieve its goals and objectives, the relationship between audit and IT is one of the most critical to the success of technology assessments. Unfortunately, in many organizations, the traditional relationship between the audit and IT teams has not been fully collaborative.

In some cases, this situation might stem from IT team members' understandable pride in the tools, systems, and processes they have built. Preventing this natural pride from growing into defensiveness can require some relationship-building skills on the part of the auditors. In other instances, IT auditors who lack sufficient cybersecurity-specific skills can damage the relationship with the IT department due to a lack of credibility.

The responses to the Foundation's survey indicated that the majority of internal audit departments (93 percent) had working relationships with IT, which is a positive sign. However, just over 28 percent of internal audit departments had what would be considered collaborative relationships with the IT departments.

A sound relationship between audit and IT is important for cybersecurity as well. Such a relationship can provide an excellent foundation for tackling cyber risks, which will require even greater coordination and collaboration among these groups. By working together, the internal audit and IT teams can bring greater clarity and understanding of the organizational risks and business objectives through joint assessments that might have traditionally been performed exclusively by internal audit.

Information Security

In addition to the IT function, the information security team will often have significant responsibilities that will need to be assessed throughout the organization. Although sometimes the InfoSec and IT organizations are combined, they also can operate separately. In fact, a growing number of regulatory agencies are starting to require the separation of these two functions, which, in turn, requires a different approach for each audit.

Further distinction should be made between the information security function in general and the cybersecurity team. Cybersecurity is generally understood to be a subset of the broader information security function, which is responsible for numerous areas that are not necessarily driven by technology issues. In an ideal world with unlimited resources, the responsibilities of these two functions would be clearly distinct and carefully delineated.

In reality, however, considerable crossover frequently exists, with general InfoSec team members often responsible for specific cybersecurity duties and concerns. Additionally, many organizations outsource a portion of their cybersecurity program to third-party vendors, including managed security service providers (MSSPs) and penetration testing providers. It is critical that internal audit reviews the services these third parties provide, which means audit must first understand the objectives, scope, and results of these services to ascertain if they are meeting expectations, mitigating relevant risks, and providing value to the organization.

Penetration testing in support of regulatory requirements provides one example of how this understanding is pertinent. The Payment Card Industry Data Security Standard (PCI DSS) requires that organizations perform penetration testing on a regular basis, but this testing is focused on the cardholder environment. If this is the only penetration testing that an organization is performing, it is likely that the majority of the corporate infrastructure is not being assessed.

The responses to the Foundation's survey indicated that the majority of internal audit departments (87 percent) had a working relationship with InfoSec, which is a positive sign. However, just over 26 percent of internal audit departments had what would be considered a collaborative relationship with the InfoSec department. These results are very similar to those with the IT department, which is expected, as duties are often shared between the two functions.

In many instances, the InfoSec team might have a stronger, more positive relationship with the audit team than other groups do because, in part, it focuses less on running infrastructure or maintaining access and capacity and more on monitoring and detecting risk. As a result, the InfoSec team might have a more intuitive understanding of internal audit's function and value. As the audit team seeks to build its capabilities, it is possible the InfoSec team could help audit gain an even greater perspective of the risks faced by the IT infrastructure.

Internal audit, InfoSec, and cybersecurity also can take active steps to help strengthen their relationships. Examples include co-sponsoring joint research projects or co-hosting security-related training sessions or luncheon topics. In addition to bolstering much-needed technical expertise and improving overall awareness of cybersecurity concerns, such activities also help develop a closer professional relationship among the individuals most directly involved in cybersecurity risk management.

One complicating factor in such relationships is the necessary independence that internal auditors must maintain. For example, IT auditors typically must use external security frameworks such as banking regulations as a baseline to perform their audits. When a significant or material finding pops up, it is the auditor who must bring bad news to the chief information security officer (CISO) and the rest of the InfoSec team. It can be difficult to maintain a collaborative approach in such circumstances, no matter how much the IT auditor and CISO wish to maintain a positive relationship.

Information Risk Management

At its heart, information security is the process of understanding, managing, and mitigating risks. Ultimately, this focus on risk can help the risk management team within an organization develop critical relationships with both information security and internal audit. Furthermore, it will be critical that the risk management team tracks personnel, procedural, and technical controls to help mitigate and control cybersecurity risk. As with all other areas of the organization, audit must be prepared both to review the risk management and identification procedures and to make sure that cybersecurity feeds into the organization's enterprise risk management framework.

It is worth noting that, broadly speaking, industry observation indicates that the most effective organizations take a risk-based, rather than a controls-based, approach to cybersecurity. The internal audit team is heavily involved and works closely with various participants in the risk management process, including operational risk, business risk, and the chief risk officer.

The responses to the Foundation's survey indicated that 72 percent of internal audit departments had a working relationship with risk management, which was the lowest of all departments surveyed. The results showed that more than a quarter of internal audit departments were not working with risk management on cybersecurity, reinforcing the mindset that cybersecurity is an IT issue. It is incumbent on internal audit to work intentionally to create awareness that cybersecurity is an enterprise governance, risk, and control issue.

Compliance and Other Teams

From helping with the development and deployment of policies to performing critical roles during the incident response process, an effective cybersecurity program must rely on the support of the legal, compliance, and other teams. In some organizations, disaster recovery, business continuity planning, incident response, legal, and compliance teams are all key players in a cohesive cybersecurity effort.

Recognizing the number of significant players involved, the internal audit team must be prepared to work with these teams to assess their organization's understanding of risk and the roles they play in cybersecurity. The Foundation's survey showed that the relationship with compliance had the highest percentage of respondents (42 percent) reporting the relationship was considered collaborative. This result seems to indicate that organizations view cybersecurity compliance as a goal or a destination, which can be a shortsighted approach in managing overall exposure.

It is important to reinforce that internal audit collaboration with these various teams cannot come at the expense of objectivity. As internal audit works to attract, retain, and train individuals with the skills and expertise necessary in cybersecurity, it must work closely with other teams to develop and understand the appropriate processes and standards. Furthermore, when collaborating with other teams, internal audit must also balance the opportunities for learning and development with the need for independence.

In the end, all teams are still working toward a common goal: the ultimate success of the organization.

Goals of a Cyber Audit Program

As high-profile breaches continue to demand a focus on cybersecurity, internal audit departments are challenged to upgrade their capability to assess the procedural, personal, and technical controls related to their organizations' data and information security practices. In stepping up to this challenge, it can be helpful to recognize and address the ongoing evolution of the well-established three lines of defense model and to clearly delineate both the broad goals of a cyber audit program and the specific activities that must be carried out — and audited — in pursuit of those goals.

The Lines of Defense

The IT, InfoSec, and internal audit groups are involved in helping to defend the organization from cybersecurity risk. Although the traditional three lines of defense risk management model provides roles for each of these functions, in many organizations the boundaries between these departments — as well as many others — are blurring.

It is incumbent on audit professionals to resist — or at the least question — any blurring of these lines. Nevertheless, as a practical matter, they must acknowledge the ongoing blurring of the traditional lines of defense and be willing to reassess how the model can be applied more effectively.

The first line of defense in this model is composed of business process owners and management. In the case of cybersecurity, this includes the lines of business and employees around the organization, but also focuses on IT, which is responsible for the data infrastructure, systems, and processes where the risk resides.

The second line of defense — the actual implementation and execution of risk management processes — is the responsibility of the InfoSec function. The InfoSec team either installs and monitors controls to detect malicious activity or employs third-party vendors to perform this function. When an attack is detected, the InfoSec team is also responsible for responding effectively.

In many organizations, however, particularly those without a dedicated InfoSec department, the responsibility for information security monitoring and response often falls to the IT team — and the boundaries between the first two lines of defense begin to blur.

As the third line of defense, internal audit is responsible for verifying that the cybersecurity effort is, in fact, a risk-based approach that properly identifies and prioritizes the risks, gathers the right information, and prescribes appropriate responses. In reality, internal audit frequently lacks the resources and background to evaluate the existing program. Instead, many internal audit organizations look to cybersecurity professionals and outside vendors to assess their cybersecurity program. This assessment includes ethical hacking, specialized evaluations, risk assessments, and assessing InfoSec governance. Many of these assessments can be performed by the second line as well.

While such blurring of the three lines is not necessarily desirable, it is in many cases unavoidable. That said, it is incumbent on internal audit to develop cyber audit plans more judiciously in order to minimize redundancy and duplication of effort and to minimize the possibility of gaps or oversights.

The relationships among all the groups involved are critical. Better collaboration — particularly between the second and third lines of defense — can reduce duplication while still clearly delineating who takes responsibility for each of the critical functions. In other words, the various players are independent but integrated.

Looking Beyond Compliance

One area in which organizations often struggle is determining how to integrate their cybersecurity audit program within the organization's overall risk management framework. For example, when the Federal Financial Institutions Examination Council (FFIEC) published its Cybersecurity Assessment Tool (CAT) in 2014, many banks initially questioned how they would understand and prioritize the more than 400 individual controls and practices named in the document.

The FFIEC tool outlined a comprehensive process for identifying an institution's inherent risk within five broad domains. It also provided methodologies for evaluating both the current and desired cybersecurity maturity levels that management would deem acceptable for the institution.

Those organizations that approached the FFIEC assessment as primarily a compliance function — using it as a checklist of practices that would help them pass regulatory scrutiny — often had difficulty reaching their desired maturity levels across the five domains. A more nuanced approach was necessary, in which the board and senior management team determine the acceptable level of risk for the organization in each specific area of concern.

Similar experiences occur in organizations that apply any of the other national or global cybersecurity frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Cybersecurity Standards (specifically 27000 to 27008), the European Telecommunications Standards Institute (ETSI) Cybersecurity Standards for the European Union, or Japan's Cybersecurity Basic Act.

While checklist compliance with the relevant framework is the point of some cybersecurity tools, those organizations that are ahead of the curve do not regard compliance as the goal. Rather, they seek to develop appropriate levels of cybersecurity across the various risk components, recognizing that a completely risk-free environment will never be achievable.

Prevention, Detection, and Response

A fundamental tenet of cybersecurity practice in the past few years has been the realization that, although many attacks can be thwarted, preventing all possible attacks is simply not feasible. When assessing the likelihood of attack, the popular saying among cybersecurity professionals is, “It’s not a matter of if, it’s a matter of when.”

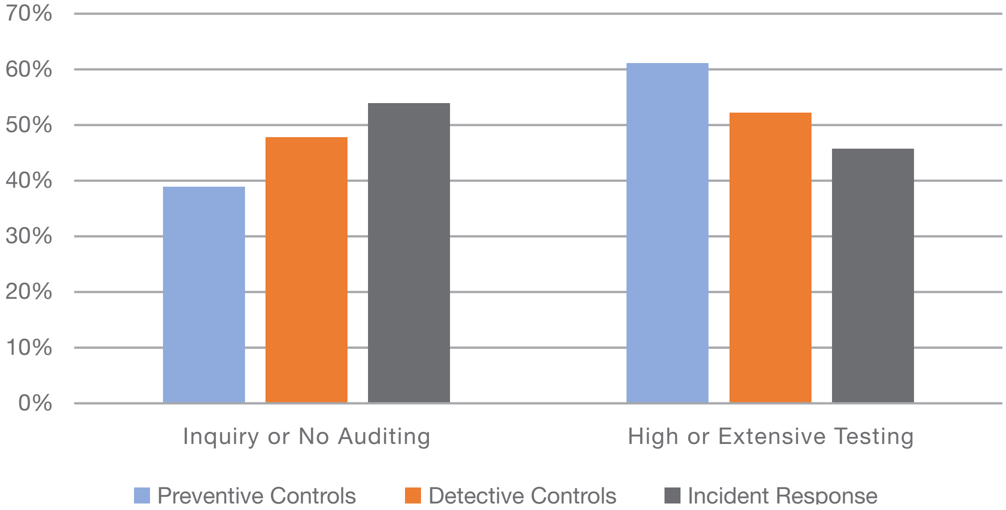
This realization has led to the development and widespread acceptance of a three-phased defense strategy composed of prevention, detection, and response. Although IT and InfoSec do their best to prevent the vast majority of attacks, it is critical that systems are in place to detect those that they cannot prevent. By looking for indicators of compromise on the network, gaps in the preventive controls can be strengthened, allowing the organization to enhance its overall coverage.

Further, knowing that not every attack will be prevented or immediately detected, the organization should also have in place incident response plans to limit the damages caused by the loss or compromise of critical data and to hasten a return to normal operations.

Although internal audit’s role in this three-pronged strategy has traditionally focused on the realm of prevention, best-in-class performers will work to broaden their scope to audit cybersecurity capabilities related to detection and response as well. Throughout all three of these stages, audit must be prepared to assess the effectiveness of the controls in place.

The Foundation's survey explored this issue and asked participants how extensively their organizations were auditing cybersecurity capabilities in these three areas. For each area, the survey asked them to characterize the level of audit testing they performed on a four-level scale — from "no auditing" to "extensive testing." Their responses are shown in Exhibit 2.

Exhibit 2: Cybersecurity Controls Audit Depth



Source: Crowe analysis

The survey responses indicated that preventive controls are not only the most frequently covered, but they also are tested at the highest rates. As cybersecurity evolves, the ability to detect and respond will be just as crucial as the controls associated with preventing attacks. Furthermore, the results showed that most organizations do at least a basic auditing of their cybersecurity, but there is room to grow.

Specialized Cyber Assessments

Although the approach for cybersecurity audits is similar to other assessments performed by internal audit, cyber assessments require a deep understanding of the applications, systems, and technologies involved. These specialized assessments focus on both the supporting technologies — such as network routers and firewalls, servers and workstations, and application development environments — and the applications themselves.

As noted earlier, the responsibility for conducting and evaluating the results of such assessments varies from one organization to another, so both the InfoSec function and internal audit must collaborate on who conducts such assessments and how often they should take place, taking into account the organization's agreed-upon risk tolerance levels.

Internal audit should be performing a broad range of specialized assessments in relation to cybersecurity concerns. Two specific types of assessments in particular are often misunderstood:

- **Vulnerability assessments.** A vulnerability assessment typically involves using an automated tool to scan an IT infrastructure and report the results. The tool's job is to identify all systems and the associated applications and services they are running. Based on this information, the tool attempts to identify issues such as missing patches, default passwords, and known exploits.
- **Penetration testing.** Penetration tests, often referred to as "pentests," mimic a real-world attacker attempting to access systems and data by identifying vulnerabilities and combining (or "chaining") them to get unauthorized access to information or gain administrative control. Unlike vulnerability assessments, penetration tests can take into account the human factor, along with mitigating controls and the issue's impact on the overall confidentiality, integrity, and availability of the supporting environment.

Ultimately, each organization, based on its risk assessment as well as its IT infrastructure, must determine what particular assessment or combination of assessments best fits its information security strategy. Typically, a combination of both types of assessments is necessary for a robust vulnerability management program. Although InfoSec or IT teams will typically drive this program, it is critical that the internal audit team reviews it to validate the scope, assessment, and results.

In the same way, every organization must determine for itself whether it is cost-effective — or even possible — to develop the technical capacity to conduct these assessments in-house. The resources and necessary capabilities can be expensive, but in large organizations, where the scope of the cybersecurity operation merits ongoing testing, having the capacity in-house can be desirable.

In many other cases, however, outside vendors can perform these assessments more cost-effectively. The CAE needs to make an informed, considered decision in this area to determine when it makes sense to develop in-house capabilities. If this function is contracted out, it is still important that internal audit assess the efficacy of the arrangement, including review of the vendor selection and qualification processes.

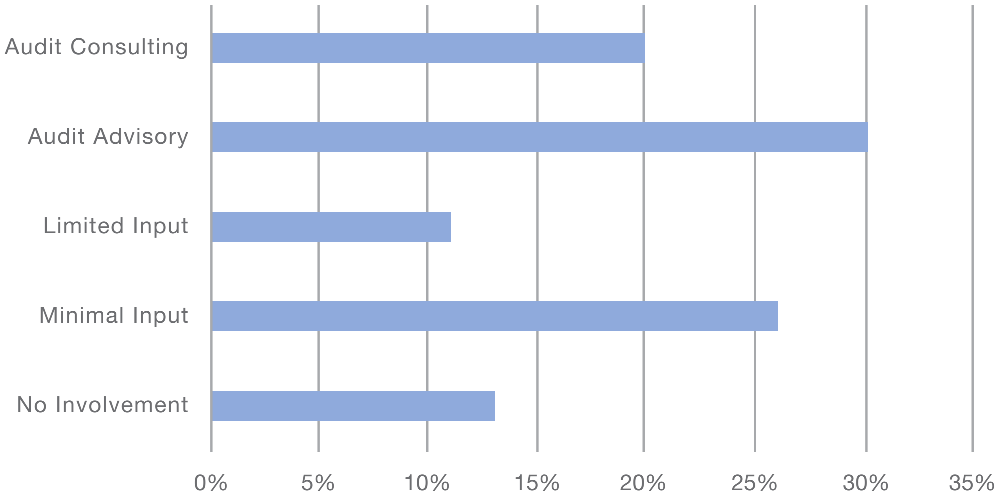
Internal Audit's Role in Cybersecurity

IT's dramatically larger role in today's data-driven economy is, without question, one of the most important business trends of recent decades. Like all other professions, internal audit's challenge is to stay current with events while concurrently expanding its role in safeguarding the security and availability of critical business information.

The Foundation's survey results reflect this continuing adaptation, but they also suggest that considerable room still exists for internal audit to play a larger and more proactive role in IT and InfoSec strategies generally and in cybersecurity concerns specifically. For example, only 20 percent of the survey participants reported that their organizations consulted with the audit team in the design and planning of major IT projects and continued to involve internal audit actively throughout the projects' duration.

In the majority of organizations surveyed, internal audit's input into IT projects was limited to an advisory role or less. In 50 percent of the organizations, internal audit had no, minimal, or limited involvement until projects were completed (Exhibit 3).

Exhibit 3: Audit Involvement in Change Management



Source: Crowe analysis

Similarly, approximately half (52 percent) of the survey participants reported that the internal audit function was a member of their organizations' project or IT governance committees. This result suggests that internal audit leaders must continue to assert and demonstrate the value their departments can provide in terms of helping to manage risk associated with IT initiatives more effectively.

In terms of cybersecurity issues specifically, the survey responses indicate that opportunity exists for greater visibility to cybersecurity concerns at the board level. Only 39 percent of the respondents said their organizations went beyond standard audit reports in reporting cybersecurity risk and trends to the board or audit committee. As the attention paid to cybersecurity concerns continues to grow, internal audit should expect to take a more proactive role in helping to validate the business's assessment and management of this rapidly growing area of risk.

Cybersecurity Frameworks

One of the fundamental first steps internal audit must take in developing a cybersecurity audit plan is to thoroughly understand the cybersecurity framework the organization uses. The selection of a framework is a management decision, often determined by IT and InfoSec executives. The framework sets out the standards that internal audit will audit against. As such, the framework is a pivotal factor that drives the development of the audit plan.

All such frameworks are designed to provide a way for organizations to begin the management of their cybersecurity systems and help establish a common language and terminology for all parties involved. For those reasons, the chosen standard also provides a practical methodology for the audit team to use as it plans its assessment of the same program compliance.

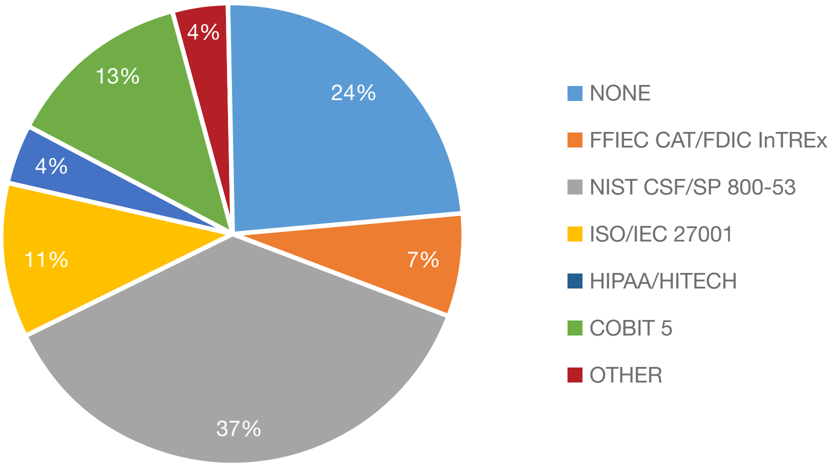
A number of specialized frameworks have been specifically tailored to address certain industries and control environments. When determining which framework to use, the audit team must take into account specific industry standards, regulator guidance, and any legal requirements imposed by authorities in the organization's jurisdiction, in addition to considering the advantages and disadvantages of each framework. Some of the most widely used frameworks that could be applicable to various organizations include:

- **NIST CSF and NIST SP 800-53.** The NIST CSF was published in 2014, following a presidential executive order. The CSF consists of the framework core, which is a set of about 100 cybersecurity activities (controls) across five functions; the framework tiers, which help define an organization's cybersecurity risk management "maturity"; and the framework profiles, which show the current and target states of the organization. The NIST Special Publication 800-53 provides a catalog of security controls designed for federal information systems. These more than 170 controls are spread across three security control baselines, which are starting points for selection of implementation of controls. Both NIST frameworks take a risk-based approach to recommending controls to implement in order to provide flexibility to organizations of different sizes, complexity, and objectives.
- **ISO/IEC 27001.** The ISO and the IEC published the 27001 security standard in 2013 as an update to the 27001:2005 standard. This framework is unique in that organizations can become 27001-certified, and the framework is used internationally. Similar to the NIST frameworks, this framework does not require all 114 controls be in place, but it serves as a basis for certification and provides a set of risk-based recommended controls for an organization to implement as well as a process for managing risk.
- **CIS Top 20.** The Center for Internet Security (CIS) published the Critical Security Controls for Effective Cyber Defense, which is a set of 20 best-practice guidelines. These guidelines are further broken down into about 150 controls. The CIS Top 20 guidelines are largely tactical and actionable technical defense controls that don't emphasize overall cyber risk management and governance.
- **HIPAA and HITECH.** The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) are two standards that focus on protecting electronic personal health information (ePHI) in the healthcare industry and in other industries that handle employee or customer health records. These standards are legal requirements, industries must be in compliance with them, and violations can lead to fines.

- **COBIT 5.** ISACA developed the original version of Control Objectives for Information and Related Technologies (COBIT) in 1996. COBIT 5 is the latest iteration of this framework, which places emphasis on managing cybersecurity risk through compliance with effective IT governance and management and on linking IT and cybersecurity objectives to business strategic goals.
- **FFIEC CAT and FDIC InTREx.** The FFIEC released its assessment tool, the CAT, in 2014 as a framework against which financial institutions can measure themselves. Institutions can use this tool to assess their cybersecurity preparedness, which is determined by an institution's calculated inherent risk profile and cybersecurity across five domains, while taking into account risk tolerance and business objectives. Unlike other frameworks, the CAT is more rigid in requiring a number of the almost 500 maturity controls to be met before achieving specific maturity levels. The Federal Deposit Insurance Corporation (FDIC) has incorporated a portion of the CAT controls into regulatory examination guidance for banks, with the introduction of the Information Technology Risk Examination (InTREx) program in 2016.
- **PCI DSS.** The PCI DSS is a continually updated set of information security standards mandated by the Payment Card Industry Security Standards Council. Unlike other standards and frameworks, the scope of the PCI DSS only includes cardholder data, such as information contained on credit cards. The controls in these standards are often very detailed and specific, and organizations that are found to be in violation of these standards can be fined or might receive increased fees from payment card brands, such as Visa and Discover.

Survey results indicated that nearly one-fourth of organizations were not leveraging a framework to define their approach to cybersecurity. Of those companies that were using a framework, NIST was the most commonly adopted framework, by 37 percent of respondents. NIST was followed, not closely, by COBIT 5 and ISO/IEC 27001 at 13 percent and 11 percent, respectively (Exhibit 4).

Exhibit 4: Primary Framework Used to Define Cybersecurity Approach



Source: Crowe analysis

Coming Changes in Internal Audit

While many internal audit organizations outsource large portions of their general IT audit processes, the trend toward migrating these capabilities in-house is clear. As internal audit departments begin to develop internal capabilities surrounding cybersecurity in the coming years, many of the challenges they can expect to face will be similar to challenges addressed when absorbing IT audit functions.

As with any IT audit functions, the initial moves into cybersecurity audit capabilities are likely to occur in areas that do not require extensive technical training — areas such as policies and procedures, system backups, and compliance with the designated frameworks mentioned earlier. Change and patch management and audits of workstations are similarly cybersecurity related, and in the short term might require a minimal amount of training in order for organizations to begin to incorporate them into their internal audit rotations.

Beyond these broad trends, several other immediate opportunities are already presenting themselves in many organizations. One such opportunity involves internal audit departments taking a much deeper dive into application controls.

In many instances, audits of application controls are driven primarily by some sort of compliance requirement. For more in-depth application controls examinations, auditors focus considerable attention on areas such as input controls, data processing functions, output controls, and access management. As cybersecurity comes more into focus for these areas, personnel with more advanced technical skills, particularly with respect to homegrown, customized, or other nonstandard applications, will play an important role in identifying additional technical controls that might be necessary.

Another area of expected change relates to business continuity planning, specifically disaster recovery planning. While a good portion of IT auditors' activities in these areas are driven by standardized work programs and industry-accepted frameworks, these areas will likely evolve into collaborative, risk-driven efforts. Most disaster recovery plans are written from an operational perspective, with a focus on restoring production or other business-critical processes. In future audits with a stronger cybersecurity focus, internal audit will likely be able to introduce security questions and to point out how restoring operating capacity in a new environment could introduce previously unrecognized security issues.

For now, many internal audit departments should concentrate on upgrading their teams' existing skills in reviewing policies and procedures, confirming documentation for business continuity and disaster recovery, and performing similar compliance-oriented tasks. The interim objective would be to upgrade these capabilities through training and professional development in order to address cybersecurity issues specifically. This objective would be achievable prior to attempting to recruit and retain personnel with more technically oriented skills, as discussed in the next section.

Future Skill Requirements

In order to perform the specialized assessments that will be required as part of the growing emphasis on cybersecurity, internal audit ultimately will need to expand its skill base. However, attracting talent with the necessary technical skills can be challenging. As such, it often could be necessary for internal audit to access these skills by engaging outside resources. It will be particularly important to develop or have access to specialized expertise in three general areas:

- **System administration.** System administration includes technical understanding of servers, applications, database platforms, and other functions that could be vulnerable to cybersecurity threats. Internal audit should have access to individuals with expertise in this area because it will be increasingly difficult to audit such systems without being able to understand their configurations.
- **Network design and configuration.** Internal audit should also have access to individuals with expertise in the design of various networks, including data and voice, across the organization. Many critical protection and detection components are configured as part of a network, including firewalls and access control lists (ACLs), intrusion detection systems (IDSs), and network access control (NAC) solutions.
- **Software development.** Internal audit departments do not have to be populated by people who can write code, but it is important to have access to people who understand software development platforms and development languages.

In the Foundation's survey, those participants who identified as CAEs or directors were asked to rate the overall technical skill levels of their internal audit teams in certain specific competencies within the three broad categories just described. The competencies addressed were:

- Microsoft Windows™ and Microsoft Active Directory™ software
- UNIX and Linux
- Network design and implementation (such as Cisco and Palo Alto networks)
- Database administration (such as Microsoft SQL Server™, Oracle, and MySQL databases)
- Security information and event management (SIEM)
- Telephony and Voice over Internet Protocol (VoIP)
- Software development
- IT governance and risk
- Penetration testing

The audit executives were asked to rate their teams on the following scale:

- Novice — Understands basic networking, system, and cybersecurity concepts (accounts, etc.)
- Intermediate — Retains a more in-depth knowledge of networking, systems administration, network monitoring, and penetration testing and understands at a high level how these systems work and the process of how to administer them
- Advanced — Has extensive knowledge of IT and InfoSec systems, including hands-on experience in either cybersecurity or IT

Exhibit 5: Skill Level of Internal Audit Teams

Skills	Novice	Intermediate	Advanced
Microsoft Windows and Active Directory Software	30%	52%	17%
UNIX and Linux	74%	22%	4%
Network Design and Implementation	74%	22%	4%
Database Administration	48%	43%	9%
SIEM	30%	57%	13%
Telephony/VoIP	65%	30%	4%
Software Development	48%	43%	9%
IT Governance and Risk	13%	61%	26%
Penetration Testing	57%	35%	9%

Source: Crowe analysis

🟩 High Skill 🟥 Low Skill

The results (Exhibit 5) showed that respondents were more likely to have confidence in their audit team's abilities for solutions such as Microsoft Windows and Active Directory software, SIEM products, and IT governance and risk, but in other areas tended to lack that level of confidence. This perception was most apparent within the network design and UNIX/Linux skill sets, as almost 75 percent of respondents felt their audit team had only novice-level skills.

The skills gap was also evident in two other critical areas, with 57 percent and 65 percent of respondents citing only novice skills for penetration testing and telephony/VoIP, respectively. Finally, although the percentages varied across competencies, very few organizations felt they had advanced skill sets in any area. These responses highlighted a critical gap for those organizations attempting to develop work programs and controls for critical technologies.

The audit executives also were asked about their future hiring plans as they relate to these competencies. A majority of respondents (52 percent) said they expect to hire individuals with specific expertise in IT governance and risk within the next three years but that they will avoid some of the more technical areas such as UNIX/Linux, VoIP, software development, and networking, most likely opting to rely on third parties in these areas.

The apparent disparities between existing skill levels and future hiring plans suggest many internal audit executives have not yet evaluated their current capabilities in light of the expected expansion of cybersecurity audit responsibilities. Moreover, the requisite technical skills are continually growing and changing. Future requirements are likely to encompass artificial intelligence, blockchain technologies, quantum computers, and other specialized disciplines that have yet to be recognized, named, or defined. With some internal auditors already operating from a reactive stance, these future areas of concern will further complicate matters.

Finding and Retaining Talent

In view of the new skill sets required, the logical question becomes: How can internal audit either find or develop the skilled technical talent it will need? Equally important, what can be done to retain skilled individuals once they are on board? At a higher level, the audit department must also explore ways that it can get audit professionals further involved in the technical nature of the work, including providing insight on the design of technologies without impairing their necessary independence.

Two underlying factors complicate the answers to these questions. One is the continuing high demand for the specialized skills involved. The second is the different set of career motivations that drive many cyber professionals, including their desire to work on challenging, diverse projects that involve new technologies and concepts.

What's more, the highly competitive nature of the cybersecurity job market allows the most talented prospects to be quite selective in choosing their next opportunity. The most desirable talent is driven not just by pay and benefits, but also by the opportunity to stay on the leading edge of their profession and to be exposed to a fast-changing array of technical and professional challenges. Such employees might feel constrained by the duties that are required of them in an internal audit department, and they would be more attracted by the environment they find in a research, security, IT, or startup organization.

While the demand for cybersecurity professionals has tapered off slightly in recent years, it remains at a very high level. This demand makes it difficult to offer competitive salary and benefits packages within the constraints of the internal audit department's budget, especially for small organizations or teams.

In organizations of sufficient size to warrant a dedicated InfoSec department, many of the highest performers will naturally be attracted to this function. Internal audit can find it difficult to compete with the intellectual challenge these positions promise — which is yet one more reason why the internal audit department should make a special effort to avoid presenting itself as a department that focuses on routine, checklist compliance.

Two other tactics can prove useful in developing the needed talent for effective cybersecurity audit capabilities. First, the internal audit team can look within its own talent base, particularly to those working in a more traditional IT audit capacity. Numerous examples exist of high-performing IT audit personnel who are eager to make the transition to cybersecurity specialization. These candidates not only know the organization, but they have the added advantage of having already developed an understanding of risk and audit competencies that can be readily applied to cybersecurity. In many cases, the technical training required to migrate from system technology to cybersecurity technology is easily managed. Additionally, as smaller audit teams start to employ internal IT audit capabilities, either via training or hiring, there are cybersecurity fundamentals that can be incorporated into areas such as change management, access controls, IT operations, and disaster recovery, thus reducing the need for outsourced resources.

The second tactic for addressing the talent needs associated with cybersecurity audit relates back to the topic of relationship management addressed earlier. While internal audit's independence and objectivity must be maintained, establishing a more collaborative working relationship with the IT and InfoSec functions can provide auditors with indirect access to technical competencies that could otherwise be difficult or inefficient to develop and maintain.

Conclusion

As internal audit departments continue to adapt to their growing responsibilities in validating the effectiveness of cybersecurity risk management, the responses recorded as part of the Foundation's research project can provide a valuable snapshot of the current state of the profession — as well as a potential road map for the future.

As the survey participants indicated in their responses, a number of opportunities for improvement exist in terms of improving the level of collaboration and support among the various groups and interests involved, including IT, InfoSec, and the broad risk management function. At the same time, the evolving responsibilities of internal audit in addressing cybersecurity issues mean that audit professionals must develop their own clear understanding of the principles of data security and the cyber frameworks that apply within their own organizations.

Finally, recognizing the growing need for technical expertise and experience that is specifically relevant to cybersecurity, audit executives will need to continue developing creative ways of attracting and retaining talent with the requisite skills while also strengthening relationships with other elements within the organization that can provide valuable guidance and support.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2018 Crowe LLP.

RISK-18000-002A

Crowe

INTERNAL AUDIT FOUNDATION™