
International Professional Practices Framework

Supplemental Guidance

GTAG®

Global Technology Audit Guide

# Assessing Cybersecurity Risk

## Roles of the Three Lines of Defense

The Institute of Internal Auditors | Global

# Table of Contents

## Executive Summary

Organizations of all types are becoming more vulnerable to cyber threats due to their increasing reliance on computers, networks, programs and applications, social media, and data. Security breaches can negatively impact organizations and their customers, both financially and in terms of reputation. Global connectivity and accessibility to information by users outside the organization increase risk beyond what has been historically addressed by IT general and application controls. Organizations' reliance on information systems and the development of new technologies render traditional evaluations of IT general and application controls insufficient to provide assurance over cybersecurity.

Cybersecurity refers to the technologies, processes, and practices designed to protect an organization's information assets — computers, networks, programs, and data — from unauthorized access. With the frequency and severity of cyberattacks on the rise, there is a significant need for improved cybersecurity risk management.

The internal audit activity plays a crucial role in assessing an organization's cybersecurity risks by considering:

- Who has access to the organization's most valuable information?
- Which assets are the likeliest targets for 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 timely if a cybersecurity incident occurred?

This practice guide discusses the internal audit activity's role in cybersecurity, including:

- The role of the chief audit executive (CAE) related to assurance, governance, risk, and cyber threats.
- Assessing inherent risks and threats.
- The first, second, and third lines of defense roles and responsibilities related to risk management, controls, and governance.
- Where gaps in assurance may occur.
- The reporting responsibilities of the internal audit activity.

In addition, the guide explores emerging risks and common threats faced by all three lines of defense and presents a straightforward approach to assessing cybersecurity risks and controls.

## Introduction and Business Significance

Internal auditors need an updated approach for providing assurance over cybersecurity risks. Although IT general control evaluations are useful, they are insufficient for providing cybersecurity assurance because they are neither timely nor complete. Foundational auditing objectives, such as completeness, accuracy, and authorization, are still relevant. However, many emerging factors are driving a need for an updated internal audit approach that provides valued conclusions on cybersecurity assertions.

The proliferation of technology today enables more user access to an organization's information than ever before. Third parties are increasingly provided access to organizational information through the supply chain, customers, and service providers. A greater variety of data has become readily available as organizations often store large volumes of sensitive and confidential information in virtualized infrastructure accessible through cloud computing.

Another factor that affects the internal audit approach is the increasing number of devices that can be connected and always engaged in data exchange (a phenomenon known as the "internet of things"). As organizations globalize and the organization's web of employees, customers, and third-party providers expands, expectations for constant access to the organization's information also increases. Younger generations of "digital natives"[1] expect real-time access to data from everywhere.

Unanticipated threats to security may be introduced by hostile global relationships, organized hackers, insiders, and substandard software and services. Cybersecurity protocols may increase in complexity as mandates and regulatory standards around disclosure of cybersecurity incidents or breaches continue to grow. The importance of detecting and communicating a risk event in a mandated amount of time outweighs the preventive value of traditional, cyclical IT general controls.

In response to such emerging risks, CAEs are challenged to ensure management has implemented both preventive and detective controls. CAEs must also create a clear internal audit approach to assess cybersecurity risk and management's response capabilities, with a focus on shortening response time. The CAE should leverage the expertise of those in the first and second lines of defense to remain current on cybersecurity risk.

[1] The term "digital native" was coined and used in the 2001 article "Digital Natives, Digital Immigrants," by educational consultant and author Marc Prensky, in reference to the generation of people that grew up using the digital language of computers, video games, social media, and the like.

## Key Risks and Threats Related to Cybersecurity

Cybersecurity is relevant to the systems that support an organization's objectives related to the effectiveness and efficiency of operations, reliability of internal and external reporting, and compliance with applicable laws and regulations. An organization typically designs and implements cybersecurity controls across the entity to protect the integrity, confidentiality, and availability of information.

Cyberattacks are perpetuated for varied reasons including, but not limited to: financial fraud, information theft or misuse, activist causes, to render computer systems inoperable, and to disrupt critical infrastructure and vital services of a government or organization. Five common sources of cyber threats are listed in Table 1.

**Table 1: Five Common Sources of Cyber Threats**

- Nation-states
- Cybercriminals
- Hacktivists
- Insiders and service providers
- Developers of substandard products and services

To understand the cyber threats relevant to an organization, it is important to determine what information would be valuable to outsiders or cause significant disruption if unavailable or corrupt. Also, it is important to identify what information may cause financial or competitive loss or reputational damage to the organization if it were acquired by others or made public. Examples of information to consider include: customer and employee data, intellectual property, supply chain, product quality and safety, contract terms and pricing, strategic planning, and financial data.

The industry in which the organization operates establishes an important context when identifying cyber threats. For example, retailers may focus on protecting customer data and ensuring that customer services are not disrupted. Intellectual property may be a key concern for organizations centered on research and development. Manufacturers may concentrate on the reliability and efficiency of production and supply chain systems, as well as the quality and safety of products. Professional services firms may be most concerned with sensitive commercial information contained in contracts and financial costing models.

## Three Lines of Defense: Roles and Responsibilities

A best practice approach to improve the effectiveness and efficiency of risk and control functions within organizations is provided in The IIA Position Paper "Three Lines of Defense in Effective Risk Management and Control," issued in January 2013. An essential step in

evaluating the internal audit activity's role in cybersecurity is to ensure the three lines of defense are properly segregated and operating effectively. Additionally, an escalation protocol should be established to define roles and responsibilities involved in identifying and escalating risks that exceed the organization's risk appetite; that is, the level of risk that an organization is willing to accept.

As the first line of defense, management owns and manages the data, processes, risks, and controls. For cybersecurity, this function often resides with system administrators and others charged with safeguarding the assets of the organization. Common first line of defense activities are identified in Table 2, on page 7.

The second line of defense comprises risk, control, and compliance oversight functions responsible for ensuring that first line processes and controls exist and are effectively operating. These functions may include groups responsible for ensuring effective risk management and monitoring risks and threats in the cybersecurity space. Common functions performed by the second line of defense are listed in Table 3, on page 9.

As the third line of defense, the internal audit activity provides senior management and the board with independent and objective assurance on governance, risk management, and controls. This includes assessing the overall effectiveness of the activities performed by the first and second lines of defense in managing and mitigating cybersecurity risks and threats. Common activities performed by the third line of defense are outlined in Table 4, on page 12.

## Owners and Key Activities of the First Line of Defense

The first line of defense consists of the operational managers that own and manage risks and controls and implement corrective actions to address process and control deficiencies. Organizations may establish several positions with cybersecurity in mind.

A chief technology officer (CTO) is typically responsible for providing knowledge and direction regarding the technologies available to drive the organization's mission and often has responsibility for protecting the organization's intellectual property. The CTO's responsibilities may also include ensuring the organization is prepared for the next phases of technological development that will enable competitive advantage, strategic change, and innovation.

The organization may also employ a chief security officer (CSO), a chief information security officer (CISO), or someone else charged with the responsibility for IT security. The CSO or

CISO, as a cornerstone in identifying and understanding cyber threats, generates and deploys the cybersecurity strategy and enforces security policy and procedures. They often take the lead role in developing oversight programs to validate that the organization's assets and stakeholder data are properly protected.

A chief information officer (CIO) may be employed with responsibility for driving competitive advantage and strategic change throughout the organization. The CIO can also be responsible for developing the information cybersecurity program, implementing an entitywide cybersecurity training program, and developing cybersecurity policy.

The CTO, CSO, CISO, and CIO collaborate with the chief executive officer and other members of senior management in the fight against cybercrime and related cyberattacks. If entities within the organization have assumed responsibility for their own technology, these entities also take responsibility to design and implement appropriate controls to secure their technology and data in coordination with other risk assessment activity within the organization.

**Table 2: Common First Line of Defense Activities**

- Administer security procedures, training, and testing
- Maintain secure device configurations, up-to-date software, and security patches
- Deploy intrusion detection systems and conduct penetration testing
- Securely configure the network to adequately manage and protect network traffic flow
- Inventory information assets, technology devices, and related software
- Deploy data protection and loss prevention programs with related monitoring
- Restrict least-privilege access roles
- Encrypt data where feasible
- Implement vulnerability management with internal and external scans
- Recruit and retain certified IT, IT risk, and information security talent

When organizations do not have the scale to support the positions described above, a common approach is to assemble a council of business and IT managers who have a stake in responding to cybersecurity risk. The aforementioned responsibilities may be covered through one or more individuals in the first line of defense with the appropriate authority to address the corresponding risk.

## Common Cyber Threat Controls

Because cyber threats are designed to take down systems or capture data, the threats often occur wherever critical data is stored: data centers, internal networks, externally hosted environments, and even business continuity platforms. No matter where an attack occurs, the end result may include violation of laws and regulations, fines, reputational damage, and loss of revenue.

Sensitive or confidential data can be classified and stored internally, externally, or both. Internally, most organizations rely upon technology such as secure configurations, firewalls, and access controls as their first line of defense. However, in a dedicated attack where the firewall is overloaded, the attackers may gain access and unauthorized transactions may be processed.

To reduce the risk of such attacks reaching the firewall, the first line of defense takes preventive action at the perimeter of the network. This is a challenging process that involves restricting access and blocking unauthorized traffic. Detective controls, such as monitoring, should also be established to watch for known vulnerabilities based on intelligence gained about software products, organizations, and malicious websites.

Many organizations establish a whitelist of good traffic and a blacklist of blocked traffic. However, active monitoring and frequent updating is critical due to the dynamic nature of network traffic. If the attacker manages to gain access to the system, the next line of attack is likely to obtain administrative privileges and cover their tracks.

When data is stored external to the organization, it is vital for the organization to ensure vendors are properly managing relevant risks. A critical first step for the first line of defense is to establish strong contracts that require: service organization control (SOC) reports, right to audit clauses, service level agreements (SLAs), and/or cybersecurity examination engagements. Additionally, expectations should be set around reporting requirements to specify protections related to information security.

After due diligence has been performed and the contract has been negotiated and executed, management should consider overseeing and governing the vendor by monitoring and reporting on key metrics to ensure conformance with SLAs. If the vendor does not meet contractual requirements, management could invoke the right to audit clause, ask for timely resolution of concerns, enforce penalties, and consider plans to transition to an alternative vendor if necessary.

Management must also be alert to attack schemes involving social engineering, including phishing emails and malicious phone calls. By impersonating a legitimate organization or person with a need for information or action, attackers convince authorized individuals to share

sensitive data, provide their system credentials, click links that route to fraudulent websites, or perform actions that install malware on the victim's computer. Malware is becoming more sophisticated and increasingly targeted to a specific purpose or network. Once malware is installed, it can replicate across the organization's network, disrupt system performance and availability, steal data, and advance fraudulent efforts by the attackers.

Malware is advanced by exploiting the lack of awareness. Therefore, reminding individuals frequently to be on the lookout for any suspicious or unusual emails, unprecedented requests, phone calls, or system activity is important. Training will also help individuals recognize fictitious communications and to report such incidents quickly for research, escalation, and resolution. Lessons learned and intelligence gained from peers in the industry can also be leveraged for training, awareness, and adoption of additional preventive measures.

## Owners and Key Activities of the Second Line of Defense

The second line of defense, often comprised of IT risk management and IT compliance functions, plays a key role in an organization's security posture and program design.

The second line is responsible for:

- Assessing the risks and exposures related to cybersecurity and determining whether they are in alignment with the organization's risk appetite.
- Monitoring current and emerging risks and changes to laws and regulations.
- Collaborating with the first-line functions to ensure appropriate control design.

Cybersecurity risks are notably more dynamic than most traditional risks and necessitate a timely response. As the risks and the organization's exposure to them change, the second line is critical in driving governance and oversight to adequately prepare and secure the organization in response to the evolving threat landscape. A security breach

**Table 3: Common Second Line of Defense Activities**

- Design cybersecurity policies, training, and testing
- Conduct cyber risk assessments
- Gather cyber threat intelligence
- Classify data and design least-privilege access roles
- Monitor incidents, key risk indicators, and remediation
- Recruit and retain certified IT risk talent
- Assess relationships with third parties, suppliers, and service providers
- Plan/test business continuity, and participate in disaster recovery exercises and tests

may lead to changes in an organization's risk appetite and government legislation and regulations.

According to The IIA Practice Guide "Internal Audit and the Second Line of Defense," providing oversight and designing policies, standards, and limits are key tenets of the second line. For example, clear expectations and guidelines, based on vulnerability risk tiers that include acceptable noncompliance rates, should be established to guide patching critical infrastructure before escalating concerns to senior management.

The second line should work closely with the first and third lines of defense to create effective awareness among the board or governing bodies and to ensure reporting on cybersecurity risks and controls is adequate and up to date. As the second line of defense performs and reports on their risk assessments, they should continue to keep cybersecurity a priority. Also, depending on the industry and type of organization, a dedicated cybersecurity risk assessment may be warranted.

The role of the second line should be clear. For example, the role that IT compliance plays in an active, urgent security incident must be understood prior to the event. Key risk indicators, with agreed-upon thresholds, serve as useful tools in monitoring, governance, and reporting.

Organizations leverage key vendors and suppliers in critical processes. The second line of defense may need to assess the relationships with these third-party service providers for cybersecurity risk, especially because the vendors may have access to sensitive, classified data via direct network connections or other methods of data transfer. Technical and contractual control provisions require review, and it is essential that vendors provide periodic assurance with adequate reporting on the agreed-upon cybersecurity controls.

The second line of defense is responsible for ensuring management provides engaged vendor governance related to cybersecurity risk. Such governance would typically include obtaining and reviewing control reports, monitoring control activities, and appropriately escalating risks to governing bodies within the organization, such as a vendor risk committee, when vendors do not comply with expectations or SLAs.

## Pitfalls of the First and Second Lines of Defense

Pitfalls often occur when monitoring and oversight are not an ongoing part of a cybersecurity protocol. New threats and vulnerabilities continue to be introduced every day. Lack of robust and regular cybersecurity training, education, and monitoring could enable attacks and threats to an organization and compromise vital systems and data.

To mitigate this risk, many organizations have formed a cybersecurity committee, often led by the CSO, CISO, and/or chief privacy officer, that meets periodically with stakeholders of the

infrastructure, network, and security teams, as well as relevant members of IT risk and compliance management. One primary objective of the committee is to understand the organization's key assets, risk assessments, likelihood of threats, potential impact, and controls in place to adequately protect these assets against cybersecurity attacks. The committee also discusses emerging threats and relevant metrics, including the results of recent penetration tests, which test the effectiveness of security defenses through mimicking the actions of real-life attackers.[2]

Other pitfalls include the lack of:

- Clearly identified lines of defense functioning in close collaboration to ensure significant risks are identified and managed efficiently and effectively.
- Executive involvement and support to ensure cybersecurity strategy receives adequate attention and focus.
- Timely response and post-incident root cause analysis.
- Defined protocols and responsibilities for responding to escalating incidents.
- Necessary skill sets.
- Industry information and knowledge to proactively address emerging risks.
- Investing or budgeting enough time, money, and resources to cybersecurity initiatives, including routine maintenance and patching.

## Role of the Internal Audit Activity as the Third Line of Defense

While governance is primarily the responsibility of an organization's board and senior management, assessing governance is one of the internal audit activity's primary roles. IIA Standard 2110.A2[3] requires the internal audit activity to assess whether the organization's information technology governance supports the organization's strategies and objectives.

As the third line of defense, the internal audit activity plays an important role in coordinating with the second line of defense, particularly the cybersecurity function. The internal audit activity can be consulted regarding:

- The relationship between cybersecurity and organizational risk.
- Prioritizing responses and control activities.
- Auditing for cybersecurity risk mitigation across all relevant facets of the organization; for example, privileged access, network design, vendor management, monitoring, and more.

[2] ISACA, "ISACA Glossary of Terms," 69. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (accessed June 20, 2016). All rights reserved. Used by permission.

[3] *The International Professional Practices Framework (IPPF) (*Altamonte Springs: The Institute of Internal Auditors, Inc., 2013), 30.

- Assurance in remediation activities.
- Raising risk awareness and coordinating with cybersecurity risk management, particularly in organizations lacking mature first and second lines of defense functions.
- Validating that cybersecurity provisions are included in the organization's business continuity plans and disaster recovery testing efforts.

As part of evaluating the effectiveness of the risk management process required in IIA Standard 2120: Risk Management, the role of the internal audit activity is to independently assess cybersecurity risks and controls to ensure alignment with the organization's risk. This involves reviewing the adequacy of the second line's work related to frameworks, standards, risk assessments, and governance.

**Table 4: Common Third Line of Defense Activities**

- Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity
- Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration
- Track diligence of remediation
- Conduct cyber risk assessments of service organizations, third parties, and suppliers (note: first and second lines of defense share this ongoing responsibility)

Additionally, the internal audit activity evaluates the effectiveness of the controls in the first line of defense. It is important to note that IT general controls are the foundation but do not offer a complete solution for mitigating cybersecurity risks. The complexity of cybersecurity requires added layers of controls, such as monitoring for risk, detecting exploits as they happen, and prompting corrective action.

Because assurance based on traditional, separate evaluations is not sufficient to keep up with the pace of cybersecurity risk, an innovative assurance strategy is required. Increasingly, continuous auditing techniques are needed to evaluate changes to security configurations, emerging risk outliers and trends, response times, and remediation activities.

To increase the value of the internal audit activity, the CAE may seek a vision for innovative continuous assurance through ongoing evaluations, which provide timely and forward-looking communication of emerging risk. Global Technology Audit Guide® (GTAG®), "Coordinating Continuous Auditing and Continuous Monitoring to Provide Continuous Assurance," gives

further clarification on building a strategy for conducting ongoing evaluations in coordination with compliance functions in the second line of defense.

According to the Practice Guide "Reliance by Internal Audit on Other Assurance Providers," the internal audit activity can rely on the second line of defense if the internal auditor reperforms or otherwise verifies the work and comes to the same conclusion. For example, instead of reperforming a penetration test completed by IT risk management, an internal auditor can review the testing details (including the scope) and decide whether to rely on the results. When possible, the internal auditor should observe and interview the technical staff that performed the work, leveraging the results and lessons learned to include in future cybersecurity internal audit procedures.

With the first and second lines of defense, the internal audit activity should discuss and clearly establish expectations of third-party service providers. Depending on the scope of services, third-party service providers can arrange continuous monitoring of cybersecurity risk, particularly as cloud computing is driving increased demand of hosted infrastructure. Using continuous monitoring technology, service providers have developed cybersecurity competencies to provide management with an economical way to readily measure cyber risk and shorten response time. However, these types of services are not typically the primary source of assurance, and user organizations rarely request that their service providers perform continuous monitoring.

Here are 10 questions a CAE should consider when evaluating the organization's governance related to cybersecurity.

1. Are senior management and the governing body (audit committee, board of directors, etc.) aware of key risks related to cybersecurity. Do cybersecurity initiatives receive adequate support and priority?
2. Has management performed a risk assessment to identify assets susceptible to cyber threats or security breaches, and has the potential impact (financial and non-financial) been assessed?
3. Are first and second lines of defense collaborating with their peers in the industry (e.g., conferences, networking forums, and webcasts) to keep current with new/emerging risks, common weaknesses, and cybersecurity breaches associated with cybersecurity?
4. Are cybersecurity policies and procedures in place, and do employees and contractors receive cybersecurity awareness training on a periodic basis?
5. Are IT processes designed and operating to detect cyber threats? Does management have sufficient monitoring controls in place?
6. Are feedback mechanisms operating to give senior management and the board insight into the status of the organization's cybersecurity programs?

7. Does management have an effective hotline or emergency procedure in place in the event of a cyberattack or threat? Have these been communicated to employees, contractors, and service providers?
8. Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the CAE need to consider additional resources with cybersecurity expertise?
9. Does the organization maintain a list of third-party service providers that have system access, including those that store data externally (e.g., IT providers, cloud storage providers, payment processors)? Has an independent cybersecurity examination engagement been conducted to assess the effectiveness of the service organization's controls as a part of their cybersecurity risk management program?
10. Has internal audit adequately identified common cyber threats facing the organization (e.g., nation-states, cybercriminals, hacktivists, networked systems, cloud providers, suppliers, social media systems, malware), and incorporated these into the internal audit risk assessment and planning processes?

**Table 5: Red Flags Signal Potential Governance Gaps**

- Disparate, fragmented governance structure
- Incomplete strategy
- Delays of cybersecurity effort
- Budget cuts and attrition
- Unclear resolve to enforce accountability

These 10 questions highlight the need for strong governance not just at the top but throughout the organization. When answers are consistently favorable across the organization, then good governance is likely in place.

Using the questions, the CAE can begin identifying red flags related to cybersecurity. The CAE may evaluate whether the second line of defense is acting strategically and whether the first line of defense is positioned to identify and respond to risks and take corrective action promptly. The overarching measure is the governance structure. Table 5 lists red flags that signal potential governance gaps.

It is the CAE's role to interpret preliminary responses from these initial questions and begin the process of identifying areas under threat based on a disciplined risk-based approach. The CAE's professional judgment will play a large role in obtaining a thorough understanding of the interrelationships of threats to cybersecurity.

It is important to note senior management's governance structure may impact the manner in which these red flags are perceived. Therefore, the CAE's professional judgment and risk-based audit approach can facilitate effective communication of these red flags to assess if management has controls in place to mitigate threats.

Common red flags may signal symptoms of weak governance: A lack of strategy for the cybersecurity program and related initiatives and/or multiyear delays on cybersecurity efforts. Significant budget cuts to security functions may also warrant attention. If the information security function is passive and not willing or able to drive accountability with management on necessary cyber controls, there may be a need to increase executive awareness and support for the function.

## Internal Audit Scope and Collaboration

Scoping for cybersecurity risk is an interdependent exercise that requires internal audit to jointly plan with compliance functions in the second line of defense. Audit planning is most effective when integrated with compliance functions who have the insight to prioritize business impact and with whom they can collaborate during and after the internal audit.

The CAE should define what is covered by the internal audit plan and also note areas where assurance may not currently be provided. In alignment with IIA Standard 2050: Coordination, proper coverage of cybersecurity risk will require collaboration with the first and second line of defense to ensure the internal audit activity identifies the information that is most important to the organization. Giving priority to the most important information, the internal audit activity should work with relevant data owners (including enterprise data management), evaluate the provisioning process, and determine who has been granted access to the data in context with its importance.

The internal audit activity should then work with operational management to identify the systems and technologies that enable access paths to view critical information (e.g., employee data, personally identifiable information, customer credit card numbers, vendor purchase history). Working with operational management will also help ensure the relevant elements for cybersecurity vulnerabilities are monitored on an ongoing basis. Internal audit should consider sizing the scope of the cybersecurity audit based on who has access to critical information and assess the technology related to their access path.

The following questions will facilitate the process of identifying critical information:

- What information is deemed critical and why?
- What is the value of the data (to fraudsters, competitors, etc.)?
- Where is the information accessed, processed, and stored?
- How is information transmitted?

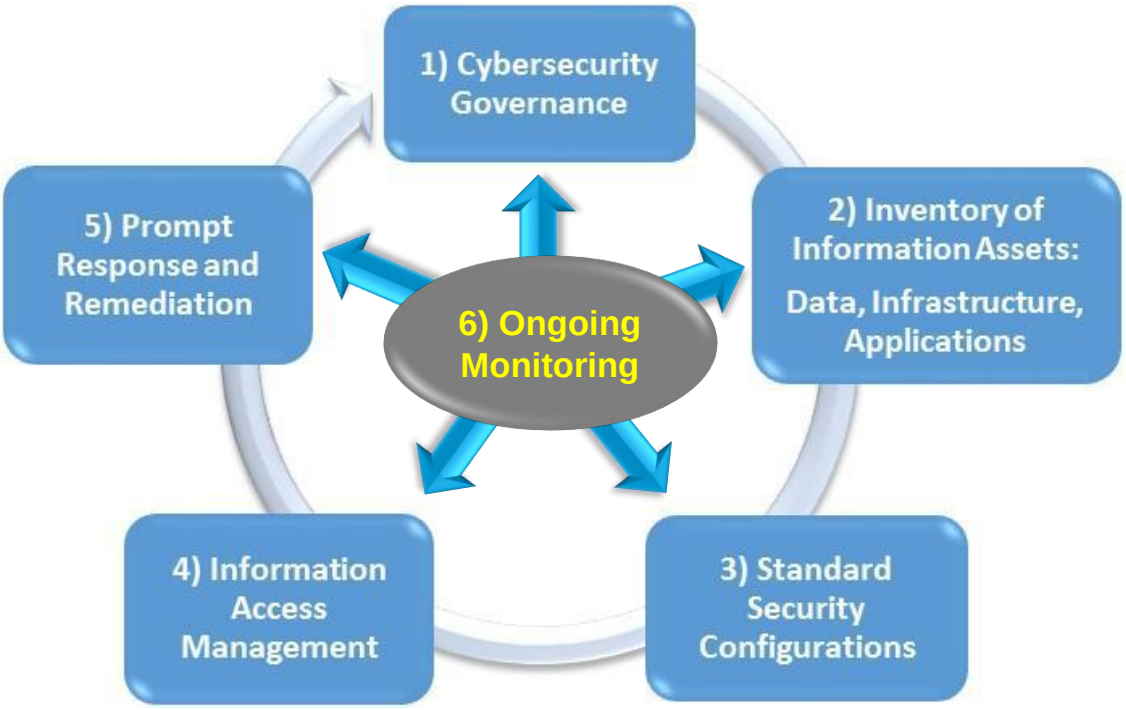
- What is the extent of rigor followed to grant and revoke access?
- Have access levels been determined by role and what roles have administrative access?
- How is access assigned, approved, monitored, and removed?
- How well protected is the information to unauthorized access?
- What type of testing is performed (penetration, access, tracked changes, etc.)?
- How is cybersecurity risk monitored for those who have functional access to critical information?

If not already documented in a business continuity or disaster recovery plan, management should consider performing a business impact analysis to classify, prioritize, and document the population of critical systems, data, and resources. The CAE can utilize the business impact analysis results to determine if the internal audit plan sufficiently covers systems that contain critical information. The CAE can then disclose to the board the areas where assurance may or may not be currently provided and the plans to provide coverage.

# An Approach for Assessing Cybersecurity Risks and Controls

The six interdependent components of the framework illustrated below can be used to assess the design and operating effectiveness of management's cybersecurity controls and governance. Since deficiencies in any of the components will impact the overall effectiveness of cybersecurity, assessing how each is designed and operating with the others gives the CAE a basis for determining how well prepared the organization is to address cybersecurity risks. When components are not designed or operating well together, the organization is ill prepared to address cyber threats and emerging risks.

## Cybersecurity Risk Assessment Framework




### Component 1: Cybersecurity Governance

The internal audit activity should understand the organization's cybersecurity governance. IIA Standard 2100: Nature of Work, requires the internal audit activity to evaluate and contribute to the improvement of governance, risk management, and control processes. Governance may include clarifying roles and responsibilities, establishing accountability, adopting a multiyear

strategy, and prioritizing action plans to include strategic collaboration with multiple stakeholders.

Strong cybersecurity governance depends on:

- Collaborating and collecting cybersecurity risk intelligence and expertise based on threats that could affect the organization.
- Setting risk appetite and tolerance.
- Planning for business continuity and disaster recovery in the event of an interruption.
- Responding promptly to security breaches.
- Establishing a culture of awareness of cybersecurity risks and threats.

Effective governance is evidenced in clearly defined policies, relevant tools, sufficient staffing, and insightful training.

Multiple stakeholders with varied perspectives strengthen the quality of governance. A cybersecurity governance committee usually includes senior management and representation from the first, second, and third lines of defense; technology and process owners; and potentially key external stakeholders, such as suppliers, customers, service providers, and peer groups.

Incident response teams regularly report to management and the board the types of breaches encountered to provide additional insight into previously unknown gaps. Management can then track the identified issues through remediation.

### Component 2: Inventory of Information Assets

The IT department should keep a current inventory of all information assets and prioritize those that are most essential to advancing the organization's objectives and sustaining operations. To meet strategic organizational goals and initiatives, these assets require more than traditional IT general controls and periodic evaluations. Preventive and detective controls designed to protect the most valuable assets need to be continuously monitored to ensure ongoing effectiveness.

When evaluating the organization's information assets, the following should be considered:

- Data
  - Types (e.g., transactional, IT configuration, unstructured)
  - Classification (enables standardization and prioritization)
  - Environments (e.g., data warehouses, key data bases)

- Infrastructure repository of technology assets
  - Servers
  - Network devices
  - Storage
  - End-user devices (e.g., laptops, mobile devices)
- Applications
- External relationships
  - Third-party hosted environments
  - Sharing of data files with external organizations (e.g., vendors, regulatory bodies, governments)

The capability to identify which software and devices are interacting on the network is fundamental to being able to defend against cyber threats. The organization cannot defend against network attacks on unknown devices and software. Organizations that allow employees to bring their own devices experience a larger volume and variety of devices and software accessing data via the corporate network. Controlling employee-owned devices and connectivity to the network should be a key focus of management. Increasingly, more employees are being required to have greater accessibility to organizational information around the clock. The ability to detect, authenticate, and inventory unknown devices would allow the organization to track, monitor, and measure changes in those devices to ensure the overall cybersecurity strategy is effective.

### Component 3: Standard Security Configurations

Centralized, automated configuration management software can be used to establish and maintain baselines for devices, operating systems, and application software. Using management software is more effective than managing systems manually or in a nonstandard fashion. Information security and the internal audit activity should review baselines to ensure an accurate assessment of environments based on risk can be achieved (e.g., externally facing web environments may require additional protection). Processes to apply necessary patches, as well as software and hardware updates, are also needed to ensure secure configurations remain current as new threat information becomes available in the industry.

### Component 4: Information Access Management

Management should consider implementing preventive controls such as having a process to approve and grant access to users based on job roles. Additionally, a process to detect when employees move within the organization would help to ensure that user access is adjusted and relevant to the new role. The internal audit activity may perform a review of user access to key data and systems to validate that access levels are justified for the current roles.

Privileged administrative access is especially important. Users with the capability to access and release information are most susceptible to cybersecurity risk. By inadvertently disclosing their password or loading malware as a result of phishing attempts, users can circumvent layers of systematic controls designed to prevent unauthorized access. People with access reside inside and outside the organization, so attention should be given to employees, consultants, and vendors with access to key data, whether that data is hosted internally or externally. Validating the preventive control activities for granting and revoking access and evaluating the susceptibility and behaviors of users with privileged access is a leading measure of the effectiveness of the organization's cybersecurity program.

### Component 5: Prompt Response and Remediation

The capability of the organization to promptly communicate and remediate risks indicates the program's effectiveness and level of maturity. Mature programs are able to continuously shorten the time to management response. One role of the second line of defense is to:

- Communicate risks that matter.
- Enact remediation.
- Track identified issues to resolution.
- Trend and report on resolution across the entity.

### Component 6: Ongoing Monitoring

As a final component of this framework, continuous auditing of each of the five components described above when conducted will help to determine how risk is managed and how well corrective action is operating. An effective assessment approach requires more than routine, checklist adherence surveys. The second line of defense is expected to implement a monitoring strategy designed to generate behavioral change that includes:

- Access-level evaluation and scanning that involves monitoring people with access to sensitive information to measure related cybersecurity risk. For a subset of users that perform critical processes, it is helpful to develop a systematic way to find vulnerabilities among relevant IT assets, security configurations, problematic websites, incidents of malware, and data exfiltration.
- Vulnerability assessment: Regularly scanning systems is critical to identify vulnerabilities within the environment. Once vulnerabilities are identified, categorized (e.g., critical, major, moderate) and addressed (e.g., address all critical vulnerabilities on high-risk systems within 30 days), remediation activities should be invoked for identified vulnerabilities.
- Externally facing systems often pose the highest risks to organizations and should receive priority; however, remediation activities are best not limited to only externally facing environments. First and second line resources can work across the

organization to define and agree on SLAs, and internal audit can help by assessing whether management is complying with the defined SLAs.

- Third-party risk assessments and monitoring: Programs can assist in assessing third-party vendors' risks and the level of security risk posed to the organization based on the services provided. For example, if the vendor hosts sensitive organizational data, management should consider having defined oversight programs such as:
    - Active monitoring of SLAs.
    - Information security configuration changes.
    - Results from independent cybersecurity examination engagements.
    - Service organization controls (SOC) reports.
    - Vulnerability assessments and penetration tests.
    - Escalation procedures with vendor management.
    - Baseline assessments performed to inspect key security controls.
    - Ongoing evaluations that analyze the technical architecture and controls in place to protect the organization's data.
    - Monitoring third-party resources that access the organization's network and systems to ensure these resources are not conducting inappropriate activity or exposing the organization to unnecessary risk with this access.
- Penetration testing: The second line of defense may conduct penetration testing for known vulnerabilities to assess preventive technical controls, as well as management's ability to detect and respond to attacks. Penetration tests should include unannounced components to provide a more reliable and objective assessment of the organization's capabilities and readiness to respond to real-world cyberattack situations. However, the scope of the tests should be reasonable, not disruptive to operations, and be approved by relevant leadership in advance. For example, conducting a test of a denial-of-service attack scenario, which is an interruption of the network with malicious intent, should be coordinated with leadership so as not to disrupt normal operations.
- Malware: Because vulnerabilities may be discovered after a device or software product was shipped to a customer, a process should be considered to regularly scan devices and products, identify vulnerabilities, and patch systems in order of priority (e.g., critical assets with critical patches first). Some systems and patches may fall below an established risk threshold, and therefore would be monitored and reported, but with no further action taken.
- Incident monitoring and response: This combination of processes allows an organization to detect, respond to, remediate, recover, and report to management in the event of a breach. Logging and monitoring technologies, as well as a highly trained response team, are essential to ensure these controls are successful in meeting objectives.

Emerging industry cybersecurity risks as well as incidents experienced by the organization or by peer organizations necessitate adjustments over time to the ongoing monitoring strategy.

Appendix D lists each component of this framework and the management activities, including continuous monitoring, that the internal audit activity may want to consider in providing continuous auditing and assurance.

## Role of CAE in Reporting Assurance to the Board and Other Governing Bodies

As the risk landscape evolves and use of cloud services, mobile devices, and social media increase, cyber threats increase. Routinely, CAEs should discuss the organization's risk appetite with senior management and the board. CAEs should also meet regularly with the organization's risk management leaders or committee to prioritize cybersecurity risks and threats to ensure resources are allocated to the most significant ones. Thus, it is essential for management to identify and develop a strategy to address the information systems and data assets most crucial to the organization and for the CAE to validate this with senior management and the board.

The board and senior management look to the CAE for assurance on risk management and controls, including the overall effectiveness of the activities performed by the first and second lines of defense in managing and mitigating cybersecurity risks and threats. The board needs to understand the information systems and data assets that are most crucial to their organization and gain assurance from the CIO, CISO, CSO, CTO, and CAE that controls are in place to prevent, detect, and mitigate cyber risks within the acceptable level of tolerance.

The CAE should ensure board members are well-informed on common and industry-specific cyber threats and the impact that cybersecurity incidents may have on the organization. The board and senior management may benefit from participating in awareness training and education sessions to gain an understanding of the organization's cyber threat profile. Continuously increasing awareness will better position the board with the knowledge needed to validate an appropriate governance structure is in place to protect and monitor the systems and data that are vital to the organization. Technical cybersecurity topics that are translated into meaningful information enables the board to exercise oversight responsibilities and monitor the cyber landscape and associated risks over time.

Effective communication between all three lines of defense and the board is essential. Establishing periodic communication helps to ensure the board is provided with relevant information to effectively carry out an internal control oversight role. The board will also be looking to the CAE to provide assurance that management has a strategy and plan in place to notify the board, enforcement authorities, customers, and the public in the event of a major

breach. Escalation and communication protocols should be established and reviewed by the board to ensure timely and appropriate notification takes place if a breach occurs.

The strategy and communication plan should be documented with clearly defined roles and responsibilities in the event of a disruptive cybersecurity exploit. The plan needs to be tested and drafts of potential communication letters/press releases reviewed by legal counsel in advance. A comprehensive, well-planned response and remediation strategy will help with minimizing the impact to the organization and maintaining the trust and confidence of customers and other stakeholders in the event a breach occurs.

# Appendix A. Key IIA Standards

The following selections from The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) are relevant to cybersecurity.

### Standard 1210 – Proficiency

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

> **1210.A3 –** Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

### Standard 2050 – Coordination

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

### Standard 2110 – Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization;
- Ensuring effective organizational performance management and accountability;
- Communicating risk and control information to appropriate areas of the organization; and
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

> **2110.A2 –** The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

### Standard 2120 – Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

# Appendix B. Related IIA Guidance

**Practice Guide,** "Business Continuity Management – Crisis Management"

**Practice Guide,** "Auditing Privacy Risks, 2nd Edition"

**GTAG,** "Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition"

**GTAG,** "Management of IT Auditing, 2nd Edition"

**GTAG,** "Information Technology Outsourcing, 2nd Edition"

**GTAG,** "Identity and Access Management"

**GTAG,** "Developing the IT Audit Plan"

**GTAG,** "Information Security Governance"

**GTAG,** "Auditing IT Governance"

**Position Paper,** "The Three Lines of Defense in Effective Risk Management and Control"

# Appendix C. Definition of Key Concepts

**Cybersecurity:** The protection of information assets by addressing threats to information processed, stored, and transported by inter-networked information systems.[4]

**Cyber threat:** Persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.[5]

**Hacktivists:** A small population of politically active hackers that pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their subgoals are propaganda and causing damage to achieve notoriety for their cause.[6]

**Information security:** Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability).[7]

**Malware:** Malicious software designed to infiltrate, damage, or obtain information from a computer system without the owner's consent.[8]

**Patch:** Fixes to software programming errors and vulnerabilities.[9]

**Phishing:** This is a type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.[10]

**Security posture:** The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.[11]

---

[4] ISACA, "ISACA Glossary of Terms," 29. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (accessed June 20, 2016). All rights reserved. Used by permission.
[5] Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Cyber Threat Source Descriptions." https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions (accessed June 20, 2016).
[6] Ibid. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#hack (accessed June 20, 2016).
[7] ISACA, "ISACA Glossary of Terms," 49. 2015. http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf (accessed June 20, 2016). All rights reserved. Used by permission.
[8] Ibid., 59.
[9] Ibid., 69.
[10] Ibid., 70.
[11] Richard Kissel, Editor, "Glossary of Key Information Security Terms, NSISTIR 7298, Revision 2," 179. 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (accessed July 5, 2016).

# Appendix D. Internal Audit Considerations for Cybersecurity Risk

The following components, organized by activities described in this guide, function together to address cybersecurity risk. Also included are considerations to monitor operating effectiveness:

## Component 1: Cybersecurity Governance

- Clear, strategic purpose with accountable stakeholders and defined roles and responsibilities.
- Reporting line to enable suitable authority and objectivity.
- Expertise to deploy security tools and enforce policy.
- Elements of practice including:
    - Defining and communicating the risk appetite.
    - Setting cybersecurity policy.
    - Conducting risk assessments and monitoring, based on a consistent rationale and methodology.
    - Training and staffing to deploy security monitoring strategy to sustain as organizational needs change.
    - Requiring independent cybersecurity examination engagements of third-parties who produce or provide particular goods or services.
- Ongoing communication, metrics, reporting, and action tracking.
- Incident management.
- Planning business continuity related to cyberattack scenarios.
- Senior management and board visibility and involvement.

## Component 2: Inventory of Information Assets

- **Inventory of data**: Management has identified and classified the types and location of critical and sensitive data, whether internal or external to the organization.
- **Inventory of authorized and unauthorized devices:** Authorized hardware devices access the network (inventory, track, and correct) and unauthorized devices found are removed.
    - Monitor the number of unauthorized devices on the organization's network and the average time taken to remove the unauthorized devices from the network.
    - Track the percentage of systems on the organization's network that are not using user authentication to gain access to the organization's network.
    - Maintain an up-to-date listing of network devices, servers, and end-user devices.
- **Inventory of authorized and unauthorized software:** Ensure only authorized software is installed/executed on the network (inventory, track, and correct) and that

unauthorized software is prevented from being installed. If unauthorized software is detected, it should be removed timely.

- Number of unauthorized software instances on the network and the average time taken to remove the unauthorized software from the network.
- Percentage of organization's systems not running whitelisting/blacklisting software.
- Number of software applications blocked by the organization's software whitelisting/blacklisting software.
- Percentage of hardened systems.

### Component 3: Standard Security Configurations

- **Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers:** Establish, implement, and actively manage (track, report on, correct) security configurations.
  - Percentage of organization's systems not configured according to the approved configuration standard.
  - Percentage of organization's systems with security configuration not enforced by technical configuration management applications.
  - Percentage of organization's systems not up to date with the latest available operating system software security patches.
  - Percentage of organization's systems that are not up to date with the latest available business software application security patches.
- **Secure configurations for network devices such as firewalls, routers, and switches**: Establish, implement, and actively manage (track, report on, correct) security configurations.
  - Volume and frequency of configuration changes to the network system.
  - Average time to alert organization's administrator of unauthorized configuration changes and the average time to block/quarantine changes on the network.

### Component 4: Information Access Management

- **Controlled use of administrative privileges**: Monitor the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- **Account monitoring and control:** Manage the lifecycle of system and application accounts (creation, use, dormancy, and deletion).
- **Controlled access based on the need to know:** Track, control, prevent, and correct secure access to critical assets (e.g., information, resources, systems).
- **Population of users:** User access processes must consider all people with access to critical data, including internal and external users. Most organizations have employees,

consultants, and vendors accessing data internally and externally. Include third parties where file transfers are sent.

### Component 5: Prompt Response and Remediation

- Continuous improvement of the cybersecurity program from raising recommendations and taking timely action to completion.
- Assess vulnerabilities, analyze threat intelligence, and identify gaps.
- Measure performance and compare to industry benchmarks and peer organizations.
- Identify specific knowledge, skills, and abilities needed to support program.
- The following lists some examples of metrics:
  - Quantity and percentage of sustained remediation based on location/department/employees.
  - Number of IT vulnerabilities and policy exceptions based on location/department/employees.
  - Platform compliance scores based on location/department.

### Component 6: Ongoing Monitoring

- **Malware defenses:** Control the installation, spread, and execution of malicious code; rapidly update defense, gather data, and take corrective action.
- **Limitation and control of network ports, protocols, and services:** Track, control, and correct the operational use of ports, protocols, and services on network devices.
- **Application software security:** Prevent, detect, and correct security weaknesses of all in-house developed and acquired software.
- **Wireless access control:** Track, control, and correct the use of wireless LANs, access points, and wireless client systems.
- **Boundary defense:** Detect, prevent, and correct the flow of information transferring networks of different trust levels.
- **Penetration tests, phishing tests, and red team exercises:** Test the overall strength of an organization's defenses (technology, processes, and people).
- **Maintenance, monitoring, and analysis of change events:** Collect, manage, and analyze change events and incidents that could help detect, understand, or recover from an attack. Include analysis from intrusion detection systems (IDS) and privileged user activity logs.
- **Data protection/data loss prevention:** Prevent/mitigate effects of data exfiltration; ensure privacy/integrity. Deploy tools to assist where appropriate.

## Authors/Contributors

Bradley C. Ames, CRMA, CISA

Forrest R. Foster, CISA

Caroline Glynn, CIA, CISA

Mike Lynn, CRMA

Dean Nakama

Tim Penrose, CIA, CISA

Sajay Rai, CISM

## About The IIA

The Institute of Internal Auditors (The IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 185,000 members from more than 170 countries and territories. The association's global headquarters are in Altamonte Springs, Fla. For more information, visit www.globaliia.org or www.theiia.org.

## About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (non-mandatory) guidance for conducting internal audit activities. While supporting the *International Standards for the Professional Practice of Internal Auditing* (*Standards*), Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

### Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. As part of the IPPF Guidance, conformance with Practice Guides is recommended (non-mandatory). Practice Guides are endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance or www.theiia.org/guidance.

## Disclaimer



## Copyright



September 16