Cybersecurity Audit Survival Kit

AUDITBOARD

Table of Contents

Cybersecurity Audit? InfoSec Professionals and Internal Auditors, Start Here

Cybersecurity threats have made safeguarding organizational assets more critical than ever. For many organizations, **cybersecurity audits serve as essential checkpoints to evaluate the robustness of their defenses and identify vulnerabilities**.

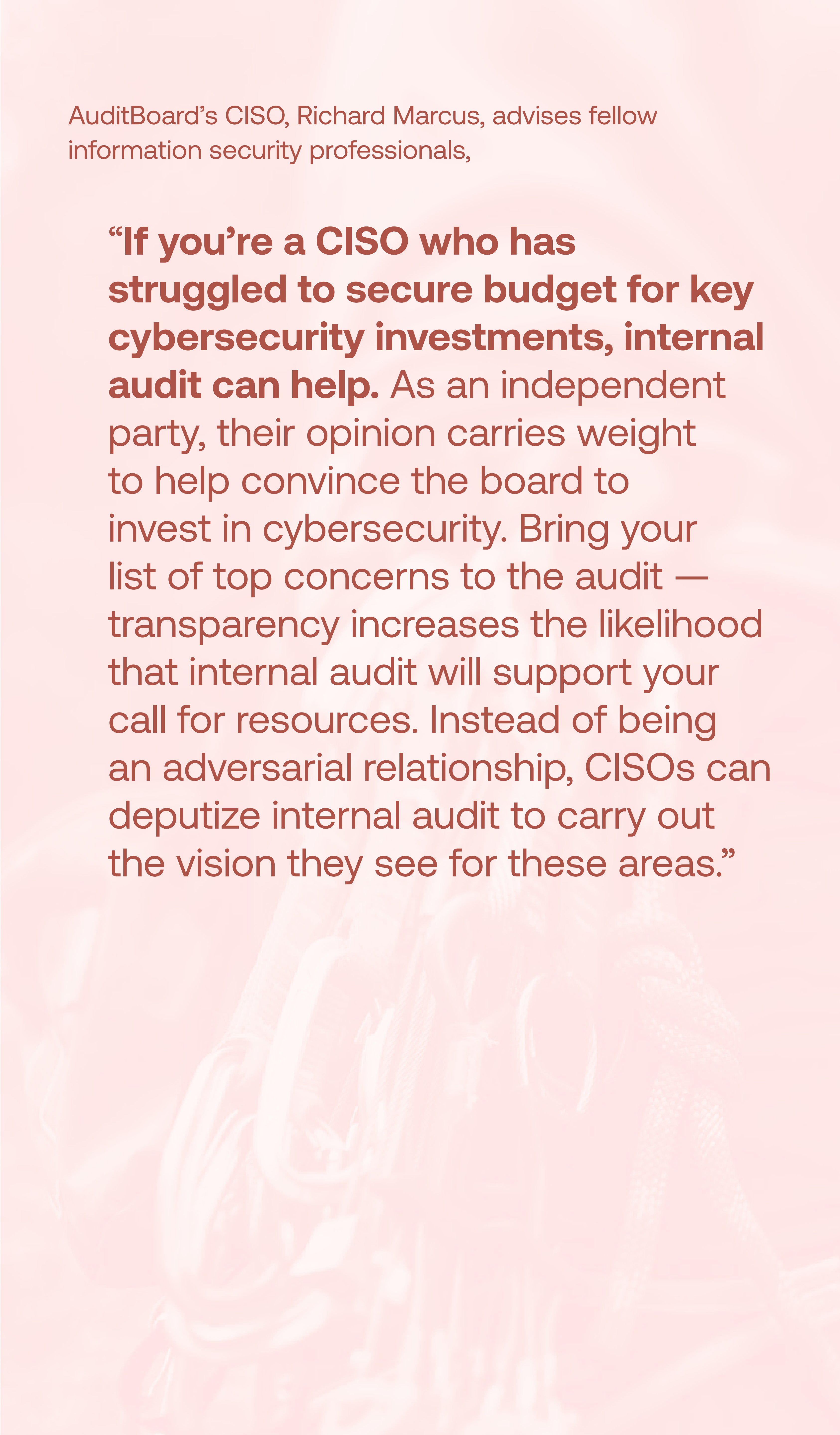
However, these audits are often fraught with challenges. Misaligned objectives, insufficient resources, and a lack of understanding between internal auditors and information security teams create inefficiencies and frustration on both sides. Now, The Institute of Internal Auditors (The IIA) has published **new guidance designed to help CAEs and CISOs work together to improve the experience and outcomes for everyone involved**.

The IIA addresses the challenges faced by both audit and InfoSec by introducing the Cybersecurity Topical Requirement, part of its Global Internal Audit Standards released in January 2024. This requirement represents a significant evolution in cybersecurity audits by providing specific, actionable guidance to internal auditors on auditing cyber risks. For information security professionals, the requirement increases transparency by providing insight into the control expectations that internal audit will be assessing.

A cornerstone of the guidance is its emphasis on collaboration. The requirement seeks to foster a shared language related to cybersecurity risk and control and common objectives between audit and InfoSec teams — increasing coordination while ensuring audits are rigorous, consistent, and aligned with organizational priorities. When internal audit and InfoSec work together effectively, there will be less tension, more trust, and stronger resilience against cyber threats.

This guide breaks down the IIA's Cybersecurity Topical Requirement implications for both internal audit and InfoSec professionals. To help jump-start collaboration during the audit process under the new requirement, we've broken down key actions for both teams leading up to, during, and after a cybersecurity audit and included a cybersecurity audit readiness checklist to support audit and InfoSec in working together.

We encourage you to share this guide and the Cybersecurity Topical Requirement with your audit and InfoSec colleagues to spark discussions about its impact and champion its integration into your processes. By working together, internal audit and InfoSec can present a united front in the fight to secure the organization against bad actors.



AuditBoard's CISO, Richard Marcus, advises fellow information security professionals,

> **"If you're a CISO who has struggled to secure budget for key cybersecurity investments, internal audit can help.** As an independent party, their opinion carries weight to help convince the board to invest in cybersecurity. Bring your list of top concerns to the audit — transparency increases the likelihood that internal audit will support your call for resources. Instead of being an adversarial relationship, CISOs can deputize internal audit to carry out the vision they see for these areas."

Quick Overview of The IIA's Cybersecurity Topical Requirement

For InfoSec professionals who may not be familiar, The IIA is a globally-recognized authority in internal audit standards. Its guidance helps internal audit functions maintain consistency, quality, and alignment with best practices worldwide. In January 2024, The IIA released its updated Global Internal Audit Standards, marking a significant evolution in its framework. Among these innovations was the introduction of "Topical Requirements," which address specific subject areas that pose unique risks and challenges.

Historically, internal auditors have approached cybersecurity with varying levels of rigor, often depending on the organization's size, sector, and the auditor's familiarity with cyber risks. Recognizing cybersecurity's critical and universal nature, The IIA introduced its Cybersecurity Topical Requirement as the first subject under its new Topical Requirements framework. This requirement complements the broader Global Internal Audit Standards, providing targeted guidance for high-risk areas.

The Cybersecurity Topical Requirement ensures that internal auditors approach cybersecurity audits with a consistent methodology. It emphasizes the need for auditors to develop a thorough understanding of the cybersecurity landscape, encompassing potential threats, vulnerabilities, and the implications of cyber incidents for organizational operations. By **establishing a baseline for cybersecurity audits**, The IIA provides a roadmap that organizations of all sizes can adopt, promoting consistency and reducing the variability that has historically characterized cybersecurity audits.

Unlike traditional audit approaches that often treat cybersecurity as an isolated risk, this requirement mandates that **cybersecurity risks be integrated into audit plans continuously**. This shift recognizes that cyber threats are dynamic, requiring an ongoing and adaptive audit approach.

Collaboration is a foundational part of the guidance. Internal auditors are encouraged to work closely with InfoSec teams to understand the organization's cybersecurity posture comprehensively. Collaboration is essential for evaluating cyber controls effectively and fostering a shared commitment to organizational resilience.

Cybersecurity Topical Requirement – At a Glance

Designed to ensure consistency in cybersecurity auditing. The guidance is mandatory for assurance services and recommended for advisory services. The goal of the guide is to align efforts and encourage collaboration between audit and InfoSec teams.

Governance: Formal strategy, policies, defined roles, and stakeholder engagement.

Risk Management: Cyber risk assessment, accountability, incident response, and awareness training.

Controls: Internal and vendor security, talent development, continuous monitoring, IT lifecycle security, and network/ endpoint protection.

Specifics of the Cybersecurity Topical Requirement

The Cybersecurity Topical Requirement is designed to standardize and enhance internal auditors' approaches to cybersecurity audits and give InfoSec teams insight into the control expectations that the auditors will be assessing. The guidance starts by listing requirements in three domains: Governance, Risk Management, and Controls.

The guidance includes two documents: the Topical Requirement and a Topical Requirement User Guide.

- **The Topical Requirement** summarizes the three domain areas as "a minimum baseline for assessing cybersecurity in an organization." Under each area, the document lists the applicable requirements internal auditors must assess.
- **The User Guide** supplements the summary with detailed considerations for applying the requirements within each domain. The detailed instructions provide a step-by-step guide to conducting a cybersecurity audit. Next, the User Guide includes mapping to the NIST Cybersecurity Framework 2.0, COBIT 2019, and NIST 800-53. The final section of the User Guide is a sample audit program that can be used as a resource for designing specific audit test steps.

Key aspects of the guidance include:

1. **Comprehensive Understanding of Cyber Risks:** Internal auditors must gain a thorough understanding of the cybersecurity landscape, including the potential threats, vulnerabilities, and impacts unique to their organization. This marks a departure from traditional approaches that treat cybersecurity as a niche domain.
2. **Integration With Audit Plans:** Cybersecurity risks must be woven into audit plans throughout the year rather than being isolated to annual reviews. This ensures that audits remain relevant in the face of rapidly evolving threats.
3. **Collaboration With InfoSec Teams:** Auditors are encouraged to work closely with InfoSec counterparts to align on objectives, share knowledge, and achieve a comprehensive assessment of cybersecurity controls.
4. **Minimum Standards for Cybersecurity Audits:** The guidance sets clear expectations for the scope and depth of cybersecurity audits, ensuring consistency across organizations of all sizes.

While the guidance is written from an auditor's perspective, **its content is valuable to anyone protecting an organization from cyber threats**. The appendices, in particular, are a solid roadmap for evaluating an organization's control environment, regardless of your role. By providing these standards, The IIA has created a resource for improving audit quality and fostering better relationships between auditors and InfoSec professionals, bolstering cyber resilience.

Governance Requirements for Cybersecurity

Internal auditors must assess **how effectively an organization's governance processes address cybersecurity risks** during their audits. For governance, this involves ensuring that cybersecurity policies and procedures are established, regularly updated, and aligned with widely recognized frameworks such as NIST or COBIT.

Organization leaders must define and assign clear roles and responsibilities for cybersecurity to qualified individuals. Auditors should also verify that updates regarding cybersecurity strategies, risks, and controls are communicated regularly to the board. Additionally, it is important to confirm that key stakeholders, including leadership and strategic vendors, are actively engaged "to discuss and act on existing vulnerabilities and emerging threats in the cybersecurity environment." Furthermore, essential resources such as funding, training, and technology should be communicated to support these initiatives.

Risk Management in Cybersecurity

Auditors evaluate whether **an organization's risk management processes effectively address cybersecurity risks**. The risk management evaluation includes verifying that a structured approach is in place to identify, analyze, and mitigate IT and cybersecurity risks, with input from cross-functional teams and external stakeholders as necessary.

Risk management policies must be established, regularly updated, and aligned with recognized frameworks. Clear accountability should be designated to monitor and respond to emerging risks. The processes should facilitate the escalation of critical risks that reach "an unacceptable level according to the organization's established risk management guidelines," ensure compliance with legal and contractual obligations, and manage risks associated with third parties. Additionally, auditors will assess data protection measures, such as encryption practices and data retention policies, and communicate any cybersecurity operational risks to management and employees.

Control Processes for Cybersecurity

Internal auditors must assess **the organization's cybersecurity controls to determine whether they are properly designed and implemented**. This involves prioritizing controls based on risk, effectively allocating resources, and providing necessary staff training. Policies should encompass all facets of cybersecurity operations, including system development lifecycle integration, hardware management, and production support.

The requirement calls for IT general controls like "configuration, end-user device administration, encryption, patching, user-access management, and monitoring availability and performance." Controls must cover areas such as network security, email, file sharing, and the physical security of high-risk information centers. Additionally, auditors must ensure that the organization has effective incident response and recovery procedures in place and that cybersecurity is integrated with service delivery processes, such as change management and help desk operations.

How the Requirement Impacts Your Job

Introducing the Cybersecurity Topical Requirement has far-reaching implications for internal auditors and InfoSec professionals, both in their individual roles and in their working relationships.

For InfoSec professionals, the requirement provides greater clarity regarding audit expectations. By outlining specific focus areas, the Cybersecurity Topical Requirement enables InfoSec teams to prepare more effectively, reducing the uncertainty and stress often accompanying audits. The guidance also encourages InfoSec teams to adopt a proactive approach by conducting self-assessments and addressing vulnerabilities before they become audit findings. This proactive engagement streamlines the audit process and demonstrates a commitment to continuous improvement, strengthening the organization's cybersecurity posture.

For internal auditors, the requirement represents a significant expansion of responsibilities. Auditors are now expected to better understand cybersecurity, including technical concepts and risk management frameworks, especially those currently used within their organizations. This shift requires auditors to invest in continuous learning and engage more closely with InfoSec counterparts. By doing so, auditors can enhance their ability to assess cybersecurity risks effectively and provide actionable recommendations supporting organizational goals.

Impacts for InfoSec Professionals

For InfoSec teams, the guidance offers a clearer understanding of audit expectations and introduces auditors as allies in the fight against cyber threats.

1. **Predictability in Audit Focus:** The guidance outlines specific focus areas for cybersecurity audits. InfoSec teams can use the guidance to conduct self-assessments, and identify and address vulnerabilities before they become audit findings. Having the audit program from the appendices means you know exactly what kind of questions the auditors will ask.
2. **Support for Resource Allocation:** Auditors can serve as independent advocates for cybersecurity investments, lending credibility to requests for additional funding, tools, or personnel. As cybersecurity experts, the InfoSec team can guide the auditors to areas that need improvement and additional resources. They can present your case to senior management and make a proper argument as long as they understand the details.
3. **Improved Collaboration:** With auditors now equipped to understand cybersecurity risks, InfoSec professionals can work more effectively with them to align priorities and present a united front to leadership. Since auditors will conduct work across the organization, they can push for stronger cybersecurity controls in areas the InfoSec team may never reach directly.

Impacts for Internal Audit Professionals

For internal auditors, the Cybersecurity Topical Requirement represents both a challenge and an opportunity.

1. **Expanded Responsibilities:** Auditors must understand cybersecurity more deeply, including technical terminology, frameworks, and risk management practices. This requires continuous learning and closer collaboration with InfoSec to understand the organization’s risk appetite for cyber risks.
2. **Enhanced Collaboration:** The guidance emphasizes breaking down silos between audit and InfoSec. A collaborative approach allows auditors to understand the organization’s risk landscape and application of control processes. To be effective, you must learn from your InfoSec partners.
3. **Advocacy for Cybersecurity Investments:** Internal auditors can use their findings to advocate for stronger cybersecurity measures, helping secure needed resources to mitigate risks effectively. The CAE has a unique position as one of the few people who speak directly to the board so they can make a well-informed argument for allocating resources.
4. **Driving Continuous Improvement:** By identifying gaps and recommending actionable solutions, auditors can be trusted partners in enhancing the organization’s security posture. Cybersecurity is not a topic for a single audit but a pervasive concept that permeates the organization. As with fraud risk, cybersecurity risk should be considered in every audit.

The Cybersecurity Topical Requirement introduces a new collaborative dynamic between InfoSec professionals and internal auditors. Traditionally, InfoSec teams have often viewed audits as adversarial, focusing on identifying deficiencies rather than fostering collaboration. The IIA's guidance seeks to change this narrative by positioning internal auditors as partners in strengthening the organization's cybersecurity posture.

Richard Chambers, AuditBoard's Senior Advisor, Risk and Audit, and the former CEO of The IIA, points out, "**close collaboration with internal audit is particularly beneficial for InfoSec teams that have struggled to secure adequate resources**. As an independent source of assurance, internal auditors can lend credibility to requests for additional funding, personnel, or technological investments."

The collaborative approach emphasized by the requirement has broader organizational benefits. By fostering a shared language and common objectives, **the requirement helps to break down silos between audit and InfoSec teams**. This alignment enhances trust, reduces friction, and creates a more cohesive approach to managing cyber risks. Ultimately, the guidance empowers both groups to work together more effectively, creating a united front in the face of increasingly sophisticated cyber threats.

How to Survive a Cybersecurity Audit Under the New Requirement

Preparation Strategies

Preparation is critical to successfully navigating a cybersecurity audit.
Before the audit starts, both internal audit and InfoSec teams should consider the following steps:

1. **Understand the Guidance**
   Familiarize yourself with The IIA's Cybersecurity Topical Requirement and its implications for your role. For the audit team, this could be the first time learning the details associated with cybersecurity. Use this as an opportunity to identify knowledge gaps and continue your education. Likewise, for InfoSec teams, it could be your first time reading an IT audit program written from a non-technical perspective. You will be more prepared for the sometimes general questions posed by auditors.

2. **Organize Documentation**
   Knowing what topics will be covered in the audit means you can start gathering documentation early. Both teams must compile information, so centralizing key documents, including risk registers, control frameworks currently in use by InfoSec (e.g., NIST, COBIT, PCI, ISOs), and security policies, is a good practice to streamline audit preparation. While much of this will be accessible to both teams, the InfoSec team may have more detailed documentation that the auditors would not have seen before, like playbooks and standard operating procedures (SOPs).

3. **Update Policies and Procedures**
   Depending on your time before the formal audit, the InfoSec team can use the guidance as a checklist to proactively identify and address potential gaps. For example, when compiling policies and procedures, you may notice that policies have not been reviewed for more than a year, or your Incident Response Plan may need to be updated to reflect recent changes made to the organization.

4. **Establish Communication Channels**
   Build strong communication between audit and InfoSec teams to ensure alignment and reduce misunderstandings. Even before the audit starts, the teams can work together to strategize the scope and approach. Key individuals may be selected to represent each team and work together to ensure expectations are clear on both sides and help facilitate information gathering.

5. **Choose a Testing Approach**
   Many InfoSec teams have adopted an agile way of working. Auditors may find it useful to perform this type of audit using an agile audit approach to meet the InfoSec team's expectations. One way to accomplish this is to consider each of the three domains as sprint goals. This way, audit would plan, test, and conclude on each topic during a sprint. During testing, the InfoSec contact can join daily scrum meetings to stay informed, and audit can hold sprint reviews to present issues and confirm the scope of the upcoming sprint. The approach allows InfoSec to openly communicate with audit throughout the process, and audit can adapt to the business's concerns.

During the Audit

The audit process should be approached as a collaborative effort. During the audit, both teams can work together as partners by focusing on the following:

1. **Transparency**
   Information sharing works both ways. The audit team will share the audit program and its intended approach to testing, documentation requests, and raising issues. To demonstrate a proactive approach, the InfoSec team should likewise share known vulnerabilities and ongoing remediation efforts with auditors. Otherwise, the audit team will find these in their testing and spend time trying to learn about something you already know.

2. **Focus on Solutions**
   Findings are inevitable, but these do not necessarily mean the InfoSec team is doing anything wrong. The cybersecurity audit is meant to show a point in time position on a maturity spectrum. Emphasize actionable recommendations that address findings and improve the organization's cybersecurity posture.

3. **Leverage Technology**
   Use integrated platforms to facilitate data sharing, control testing, and reporting. Technology that facilitates information exchange will keep the audit moving efficiently. By conducting the audit on a platform like AuditBoard, internal audit and InfoSec teams can easily share relevant information and audit evidence while cross-referencing existing controls with internal audit to eliminate redundant testing and minimize confusion during the audit.

Post-Audit

A well-executed audit provides valuable insights that can guide continuous improvement and help the organization adopt best practices related to cybersecurity.

1. **Present a United Front**
   Once the audit is complete, audit and InfoSec teams can strengthen the organization's defenses against cyber threats by addressing findings and implementing recommendations. Since the teams worked collaboratively during the audit, both sides should agree on the details and prioritization of the findings and how to present these to the organization.

2. **Continue to Build the Relationship**
   An additional benefit can be a stronger, ongoing partnership between internal audit and InfoSec. Once both teams agree on the findings, they can define the investment needed to bolster the organization's defenses against cyber threats. Internal audit can then take these findings and advocate to the board for the budget InfoSec needs to implement the action plans.

3. **Embrace Combined Assurance**
   A potential long-term benefit of the partnership is a shared commitment to work toward combined assurance. By providing InfoSec teams with the tools to conduct self-assessments, internal auditors can rely on the evidence and testing and focus their resources on other areas of the organization.

Leveraging Technology to Meet the Cybersecurity Topical Requirement

Audit and InfoSec teams often operate in silos, relying on unrelated processes and disconnected systems that hinder effective collaboration and alignment. The lack of integration leads to inefficiencies, redundancies, and confusion, making it challenging to meet The IIA's Cybersecurity Topical Requirement. Without centralized platforms, automated tools, and real-time monitoring, organizations will struggle to meet the requirement.

Technology will play a pivotal role in meeting the demands of the Cybersecurity Topical Requirement and streamlining the cybersecurity audit process for all involved. Instead of relying on fragmented workflows and manual testing processes, technology like AuditBoard's integrated platform centralizes risk and control management to create a single source of truth for cybersecurity policies, frameworks, and evidence. Both teams working in a unified platform designed for information sharing ensures alignment throughout the process.

Automation further strengthens the audit by facilitating control testing and gap assessments, enabling organizations to evaluate the effectiveness of their cybersecurity controls quickly and consistently, identifying areas that require improvement. Continuous monitoring capabilities enhance compliance by providing real-time insights into cybersecurity risks and helping organizations adapt to emerging threats.

Perhaps the greatest advantage of technology like AuditBoard is fostering communication between audit and InfoSec teams. By improving communication between these teams, technology bridges gaps, clarifies scope, and creates a more cohesive approach to cybersecurity audits. Ultimately, leveraging technology simplifies conformance with The IIA requirement and strengthens the organization's overall cybersecurity position.

Seamlessly Meet The IIA Cybersecurity Topical Requirement

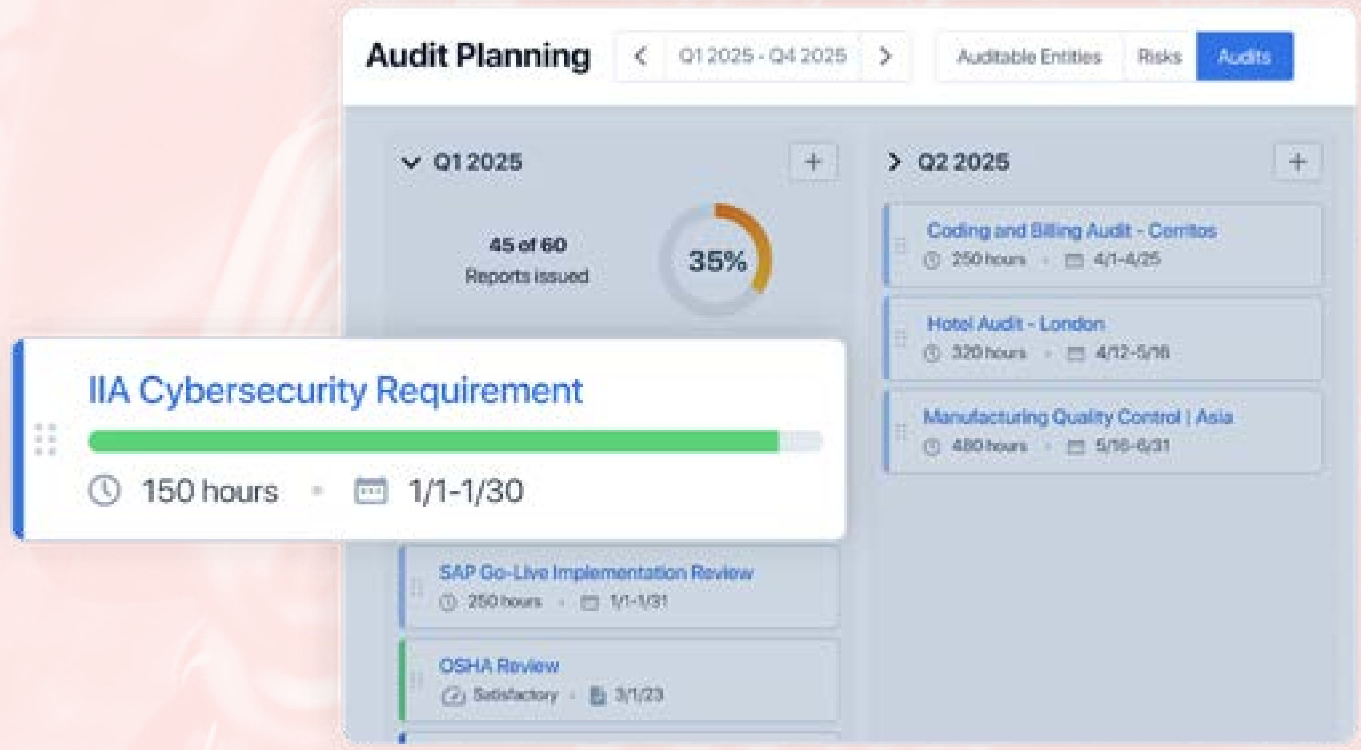
Internal Audit

- Easily add cybersecurity to audit plans, testing, and reporting
- Perform self-assessments against The IIA Cybersecurity Topical Requirement
- Easily review and test cyber controls

Information Security

- Showcase year-round security initiatives and enable seamless data sharing
- Map existing policies and controls to the new requirement
- Centralize frameworks, controls, and evidence

To learn how AuditBoard can strengthen your organization's cybersecurity posture and simplify compliance, visit auditboard.com to learn more.



45 of 60
Reports issued

IIA Cybersecurity Requirement
150 hours • 1/1-1/30

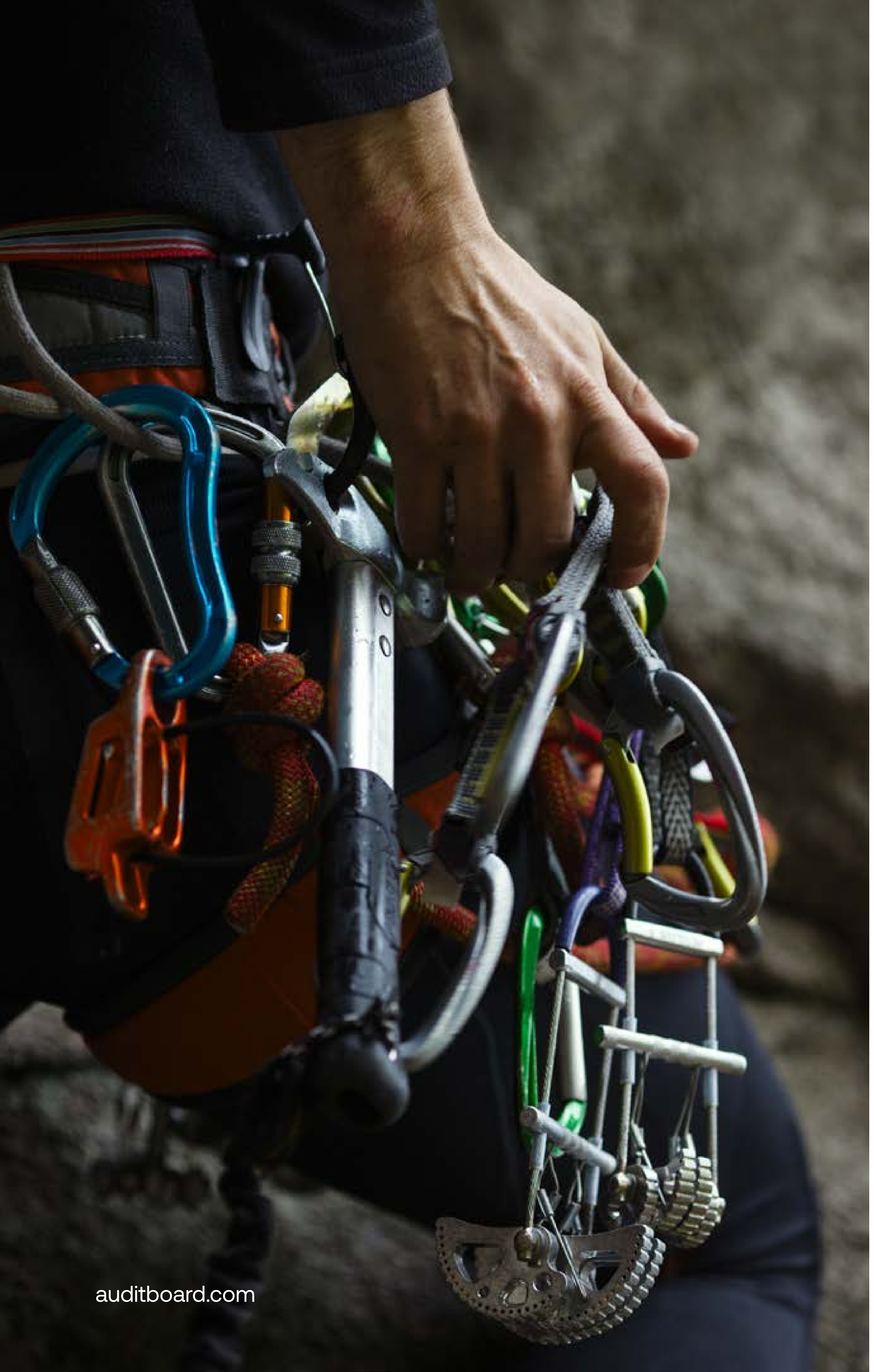
SAP Go-Live Implementation Review
250 hours • 1/1-1/31

OSHA Review
Satisfactory • 3/1/23

Coding and Billing Audit - Cerritos
250 hours • 4/1-4/25

Hotel Audit - London
320 hours • 4/12-5/16

Manufacturing Quality Control | Asia
480 hours • 5/16-6/31



Checklist: Cybersecurity Audit Readiness

Before the Audit

Internal Audit Teams

- □ Understand the Cybersecurity Topical Requirement.
- □ Update audit plans to incorporate cybersecurity risks where applicable.
- □ Engage InfoSec teams to identify key risks and controls.
- □ Review past cybersecurity audits to establish a baseline.
- □ Evaluate risk management processes, incident response protocols, and disaster recovery plans.
- □ Confirm what cybersecurity frameworks the InfoSec team is using to manage their program.
- □ Choose a team member to act as the primary contact with InfoSec.
- □ Identify any known InfoSec issues that have not been remediated to avoid redundant testing.

InfoSec Teams

- □ Familiarize yourself with The IIA's guidance.
- □ Centralize policies, SOPs, frameworks, and evidence for audits.
- □ Maintain an up-to-date risk register and incident management log.
- □ Address potential control gaps through self-assessments.
- □ Align priorities and expectations, including audit scope, with internal auditors.
- □ Choose a team member to act as the primary contact with internal audit.
- □ Inform any team members involved in the audit about the need to participate proactively in the audit.

Checklist: Cybersecurity Audit Readiness *cont'd*

Governance

Internal Audit Teams

□ Review policies, procedures, and other relevant documentation utilized by the organization to manage daily cybersecurity responsibilities.

□ Review roles and responsibilities to support the achievement of the cybersecurity strategy.

□ Review materials presented to the board about cybersecurity strategy, objectives, risks, and controls.

□ Review management's cybersecurity-related communications with relevant stakeholders.

□ Review the analysis and communication of resource requirements by management.

InfoSec Teams

□ Provide all cybersecurity-related policies and procedures to the audit team.

□ Verify which frameworks InfoSec uses as a basis for policies and procedures (e.g., NIST CSF, COBIT, NIST 800-53), including the version or release.

□ Provide information related to board communications, budgets, and software used in the cybersecurity program.

Risk Management

Internal Audit Teams

□ Review how management initially identifies cybersecurity risks.

□ Review how management identifies risk management team members, their qualifications, positions, and evidence of cybersecurity discussions.

□ Review the process to update policies and procedures.

□ Review the process for risk prioritization and escalation.

□ Review the process for managing third-party cybersecurity risks.

□ Review the process for communicating cybersecurity operational risks.

InfoSec Teams

□ Provide current cybersecurity risk registers and assessments, along with the risk scoring methodology.

□ Provide a roster for the risk management team, ideally for the InfoSec team and the enterprise risk management function.

□ Provide a list of critical applications and vendors.

□ Provide any communications related to cybersecurity risks sent to senior management, the organization, and vendors.

Checklist: Cybersecurity Audit Readiness *cont'd*

Control Activity

Internal Audit Teams

- □ Review the cybersecurity control strategic plan.
- □ Review management's process for control evaluation.
- □ Review the cybersecurity training and awareness program.
- □ Review the SDLC process to ensure cybersecurity is considered.
- □ Review process for protecting hardware, software, and network resources.
- □ Review controls over service delivery and third parties.
- □ Review controls over communications systems.
- □ Review incident response procedures.

InfoSec Teams

- □ Provide the cybersecurity strategic plan that should include budgeting, resourcing, test plans, and vendor assessment plans for the year.
- □ Provide the annual training plan and any specific training built into the development process, such as secure coding training.
- □ Provide the current list of formal, documented controls and any operating procedures for protecting hardware, software, and networks.
- □ Provide results from tabletop incident response simulations with resulting improvement plans.

After the Audit

Internal Audit Teams

- □ Document all findings in the audit management software with owners, dates, and action plans.
- □ Establish a follow-up frequency for corrective actions.
- □ Hold a retrospective with the InfoSec team to gather ideas for continuous improvement.
- □ Ensure cybersecurity procedures are added to applicable future audits.
- □ Draft a report highlighting the cybersecurity program's strengths and areas for improvement while supporting InfoSec's plans for future maturity.
- □ Set up a recurring touchpoint meeting with the InfoSec team to discuss findings and issues from future audits.

InfoSec Teams

- □ Draft realistic action plans for all audit findings with owners and implementation dates.
- □ Communicate the action plans to appropriate members of the team and leadership.
- □ Update policies and procedures based on audit results.
- □ Create a cybersecurity maturity plan that incorporates audit results and future objectives.
- □ Meet with the internal audit team regularly to gather information from their future audits.

Roadmap to Cybersecurity Resilience

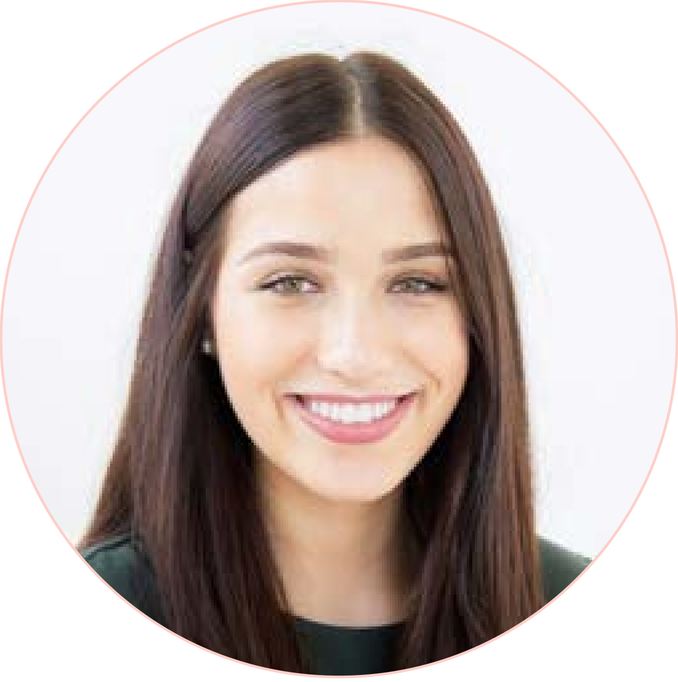
Now is the time for internal audit and InfoSec to join forces to elevate your organization's cybersecurity resilience. The IIA's Topical Requirement may spark a long-awaited shift toward internal audit and cybersecurity risk management collaboration. By providing clear, actionable guidance, the requirement addresses longstanding challenges in the audit process, fosters collaboration, enhances understanding, and promotes consistency. For internal auditors, it offers a roadmap for more effectively assessing cybersecurity risks. At the same time, InfoSec professionals can align with audit objectives and secure the resources needed to strengthen defenses. The IIA Topical Requirement is a game-changer that can drive real collaboration and risk management improvements.

We hope that you will share this guide and the Cybersecurity Topical Requirement with your audit and InfoSec colleagues to discuss its impact and advocate for its integration into your processes. Your leadership in this conversation can shape a stronger, more secure future for your organization.

Preparation, proactive engagement, and the strategic use of technology are essential to leveraging the full benefits of the guidance. By adopting these practices, organizations can survive and thrive in cybersecurity risk management's complex and dynamic landscape. Ultimately, the IIA Cybersecurity Topical Requirement is more than an obligation — it is **a catalyst for building stronger, more resilient organizations capable of navigating the challenges of the modern threat environment**.

To learn how AuditBoard can strengthen your organization's cybersecurity posture and simplify compliance, visit auditboard.com to learn more.

About the Authors



Celene Ennia
Product Marketing Manager, ITRC
AuditBoard

Celene Ennia is a Product Marketing Manager of ITRC Solutions at AuditBoard with a robust background in IT audit and compliance. Prior to joining AuditBoard, Celene held a range of IT audit and product marketing roles at A-LIGN, where she oversaw audit teams and led audits for SOC 2, SOC 1, HIPAA, and other critical standards. At AuditBoard, she leverages her deep understanding of customer needs to shape data-driven product marketing strategies and translate regulatory complexities into clear, customer-centric solutions.

Jimmy Pfleger
Manager of Product Solutions
AuditBoard

Jimmy Pfleger is a Manager of Product Solutions at AuditBoard and has over 11 years of IT audit, compliance, and security experience. He started his career at KPMG in the IT Advisory practice where he led external audit and assurance activities for some of the largest companies in the St. Louis area. In addition to managing the IT Internal Audit function at both Caleres and RGA, he built and managed the SOC 2 program as the Manager of Security Compliance at Express Scripts. His experience working across the traditional lines of defense within various organizations has given him valuable insight into how companies are truly managing IT risk.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit AuditBoard.com.