Report on the Development and Public Consultation Processes for the Cybersecurity Topical Requirement

The Institute of
Internal Auditors

Contents

Introduction

This report describes The IIA's objectives and processes for setting the Cybersecurity Topical Requirement for the internal audit profession. The report is intended to promote confidence among IIA members and stakeholders in the rigor, inclusivity, and oversight applied to the processes. The report is divided into these sections:

- Governance and content development processes.
- Processes for exposing a draft for public consultation and receiving, analyzing, and resolving comments to create the final publication.
- Resolution of major themes in the public comments.

Governance and Content Development Processes

The governance and development processes for the Cybersecurity Topical Requirement, like those for all content comprising The IIA's International Professional Practice Framework® (IPPF®), are designed to ensure that the needs of practitioners and stakeholders are met and that the requirements serve the public interest.

Inception

In 2023, IIA Standards and Guidance staff, together with IIA volunteer boards and councils, began work to create Topical Requirements as part of the IPPF Evolution project, a reevaluation and transformation of the IPPF. The project included updating the 2017 *International Standards for the Professional Practice of Internal Auditing*, resulting in the incorporation of the Code of Ethics, Core Principles, and Definition of Internal Auditing into the revised and newly named Global Internal Audit Standards™. The IPPF Evolution project also resulted in a new IPPF structure that added Topical Requirements as a core element of the IPPF.

A Topical Requirements Task Force made up of members of The IIA's Global Board of Directors, International Internal Audit Standards Board (IIASB), Global Guidance Council (GGC), and staff finalized the details of the Topical Requirements, including their purpose, name, mandatory nature, and the governance process for their development and maintenance.

Purpose

The purpose of Topical Requirements is to enhance the consistency and quality of internal audit services, strengthen the internal audit function's ongoing relevance in the evolving risk landscape, and raise the professionalism and quality of internal auditors' performance. Each Topical Requirement must align with this purpose.

Governance

The due diligence process for Topical Requirements established requirements for the ideation, prioritization, development, public review, approval, and publication of Topical Requirements.

The IIA Global Board authorized the GGC to work with IIA staff to develop and approve Topical Requirements. GGC members are certified, highly qualified, and experienced internal audit practitioners representing diverse industries and regions of the world. Members are nominated and vetted for selection for their volunteer roles, which have defined criteria and term limits to promote opportunities for varied perspectives. The GGC is also responsible for reviewing Global Guidance.

The IPPF Oversight Council (IPPFOC) is authorized by the Global Board to monitor The IIA's adherence to the criteria and processes for developing IPPF content, including the Topical Requirements. Council members are representatives from global organizations not directly linked to internal auditing; for example, members represent the International Federation of Accountants, Organisation for Economic Co-operation and Development, World Bank, International Foundation for Ethics and Auditing, Global Network of Director Institutes, and International Organization of Supreme Audit Institutions. The Council evaluates and advises on the rigor of the standard-setting process and The IIA's adherence to established guidelines. Such oversight promotes inclusiveness, transparency, and confidence in the quality of internal audit services among stakeholders globally, which ultimately serves the public interest.

The IIA and IPPFOC published "Framework for Setting Internal Audit Standards in the Public Interest," which describes a methodology for setting standards to promote quality internal audit services globally. The methodology leverages the combined experience of qualified, competent professionals in a rigorous, professionally directed process to achieve these objectives:

- Determine whether changes to the IPPF are needed by reviewing its existing elements at least once every three years.
- Determine whether elements or concepts should be added to or removed from the IPPF based on research into and an evaluation of the needs of the internal audit profession.
- Update content as determined by the review.
- Expose proposed changes to mandatory content for public consultation.
- Encourage formalized and inclusive stakeholder participation in meetings.
- Review feedback on the proposed content to identify opportunities for improvement or clarification.
- Identify groups of similar comments and organize them into "themes" for disposition, an agreed-upon approach to addressing the comments.
- Publish the new IPPF content and the translations completed by IIA national institutes.
- Develop and publish supplemental materials to create public awareness of the changes and to facilitate implementation.

These and other IPPFOC recommendations to advance The IIA's standard-setting processes were incorporated into the governance process for Topical Requirements.

Overview of the Content Development Process

The Global Board's approval of a new type of content, Topical Requirements, outlined the intention to provide requirements for assessing governance, risk management, and control processes over specified risk areas.

It was determined that Topical Requirements would:

- Ensure consistency and quality in engagement performance.
- Build confidence among internal audit stakeholders.
- Increase the focus on the resource investments required for internal audit functions.
- Strengthen the IPPF's ongoing relevance by addressing pervasive and evolving risks.

These goals were incorporated into the process for developing the Cybersecurity Topical Requirement. The stages of the process are described generally here, with further details in later sections.

Ideation and Prioritization

IIA staff gathered suggestions for topics from key stakeholders, including IIA members, the public, and IIA volunteers (engaged as "knowledge groups") via surveys, focus groups, questionnaires, discussions, and other interactions. IIA staff then compiled this information into a report and presented it to the GGC for consideration. As part of the GGC's annual planning process, the council reviews a list of suggested topics for relevance. The GGC identified and unanimously agreed to cybersecurity as the initial topic. Future annual reviews will include evaluating Topical Requirements that have already been proposed as well as new topics.

Drafting

Experienced IIA technical staff and a designated staff project lead produced a draft of the Cybersecurity Topical Requirement. The draft was prepared for public consultation through a rigorous process that included editorial reviews and discussions between IIA staff and GGC members, cybersecurity experts, IIA national institute leaders, and numerous stakeholders. IIA staff led the effort to solicit input from nonaudit stakeholders, which was intended to foster the consideration of diverse perspectives. Additionally, The IIASB appointed two members to evaluate the draft's consistency with the Standards. The draft was revised based on this input before being finalized and approved by the GGC for public consultation.

Public Consultation

The public consultation draft was available on The IIA's website in English and six additional languages for 90 days. During that time, the public could download and read the draft,

answer survey questions indicating degrees of agreement or disagreement, and comment directly in response to the survey's open-ended questions. During this time, IIA staff directly solicited stakeholder feedback through scheduled video conference sessions and in-person meetings.

Following the public consultation, IIA staff and the GGC considered all input, applying a process of organizing the public comments by themes and discussing the themes to reach conclusions and agree on dispositions of the themes. Based on the dispositions, IIA staff, project team members, and subject matter experts with extensive, relevant experience made revisions through successive iterations. External cybersecurity experts also evaluated the requirements to confirm that the intended "baseline" quality had been achieved. Details of the public consultation and disposition processes are described in later sections of this report.

Approval and Publication

The revised draft was submitted as a final version to the GGC for review and approval. Two designated IIASB reviewers conducted a Standards consistency check, and the full IIASB approved that the document was consistent with the Standards. The required two-thirds of the 17 GGC members voted to approve the final version, including a decision that re-exposure for public consultation was not necessary.

The approval included an agreement to separate the draft content into two publications: the mandatory requirements and a separate nonmandatory user guide of considerations to assist internal auditors with implementation.

Subsequent to GGC and IIASB approval, the IPPFOC conducted a final review and determined the due diligence process was adhered to.

Public Consultation Details

Public comments were solicited and received in three ways:

- An online survey available in seven languages and promoted through extensive marketing and communications efforts.
- Manual submissions, such as letters, marked-up versions of the exposure draft, and emailed messages.
- Feedback received directly through solicited meetings and events during which representatives of The IIA and GGC delivered presentations to promote awareness of the draft Topical Requirement.

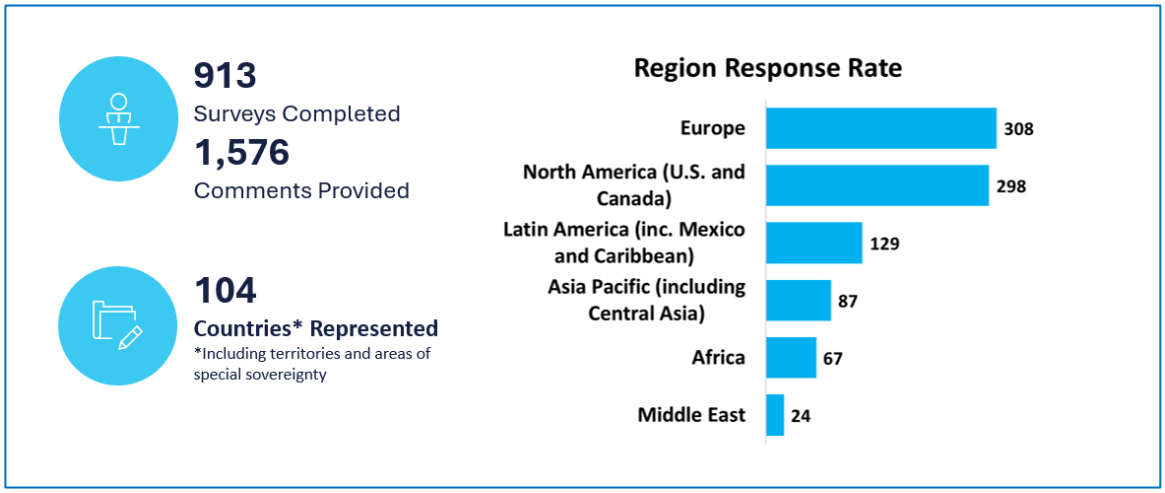
Survey for Public Comment

The primary option for submitting comments was via an online survey. The public comment survey was managed and administered by the Research and Insights department of The IIA, which is experienced in designing and conducting surveys. The survey tool was configured to gather information about each element of the Topical Requirement, including the concept, structure, and cybersecurity details. The survey also solicited respondents' level of satisfaction with the proposed draft and feedback for improvement. Several IIA national institutes collaborated to translate the draft and the public comment survey. The draft and survey were provided via theiia.org website in Arabic, Chinese Simplified, English, French, German, Portuguese, and Spanish. Additionally, instructional and informational materials were provided in English, and institutes were invited to translate those materials.

The survey opened on 3 April 2024. The IIA used email, social media, a webinar, public relations, theiia.org website, and other forms of outreach to invite the public worldwide to submit feedback. The survey closed on 3 July 2024.

Ultimately, 913 surveys were completed, providing 1,576 specific comments. Figure 1 illustrates the number of survey responses from each defined region. The responses represented 104 countries, demonstrating a global response.

Figure 1. Cybersecurity Topical Requirement Survey Response Data



Survey Tool

The survey contained 18 questions. For categorization purposes, survey respondents were required to select whether they were answering as an individual, official representative of an organization, or on behalf of the internal audit function.

Excluding administrative questions, the survey contained two types of items. One type asked respondents to select from a set of choices registering a level of agreement with the content of a particular element on a five-point scale: strongly agree, agree, neither agree nor disagree, disagree, or strongly disagree. The other type of item invited respondents to provide free-form text comments on each element for a total of five comment boxes.

The questions focused on various aspects of Topical Requirements:

- Clarity of key concepts, including their purpose, application, and documentation.
- Structure, format, and content, including the number of requirements, inclusion of considerations, and sections focusing on governance, risk management, and controls.
- Relevance to the evolving risk landscape.

Manual Submissions

Presentations and Meetings

Throughout the public comment and analysis period, IIA staff, GGC members, and relevant expert volunteers gave presentations and conducted meetings with stakeholder groups to promote awareness of the proposed Topical Requirements and solicit feedback. The presentations were given to IIA national institutes, professional service organizations, and other industry and stakeholder representative groups. More than 3,000 people worldwide registered for a free informational webinar.

Meetings with significant nonaudit stakeholders were held primarily to gather feedback with a public interest perspective on how the Topical Requirement and its effect on the internal audit profession would be perceived and valued. Significant nonaudit organizations that participated include the Basel Committee on Banking Supervision, Global Network of Director Institutes, International Corporate Governance Network, International Monetary Fund, Organization for Economic Co-operation and Development, U.S. Government Accountability Office, and the World Bank Group, among others.

Letters

More than 25 individuals and organizations submitted letters instead of or in addition to surveys. The letters often provided helpful context about issues or concerns.

Analyses and Identification of Themes

To analyze the public consultation results, GGC members were assigned to one of four content review working groups, each assisted by a dedicated IIA staff member.

Grouping the public comments and tagging them with "themes" signifying common ideas had been established and found to be an effective process during the analyses of survey responses related to the 2024 publication of the Global Internal Audit Standards™. The IPPFOC recommended this methodology to promote quality and enable systematic quantification and a determination of the relative frequency of ideas.

Potential themes were initially identified using an artificial intelligence tool, then carefully vetted by staff, and approved by the GGC. Each working group was responsible for assessing the themes based on a combination of quantitative and qualitative factors, using data from the public comment survey tool and manual submissions (for example, the main points in the letters were also assigned corresponding themes) as well as the members' professional judgment.

The working groups recommended how to respond to (dispose of) the themes, and the dispositions benefited from the reviewers' professional competence and due professional care. To promote transparency, all GGC and other project team members had full access to each working group's public comments and analyses. Themes and the details of the dispositions were refined in successive rounds of reviews, which provided additional opportunities to raise and resolve issues.

The GGC voted to approve all final dispositions by surpassing the two-thirds requirement.

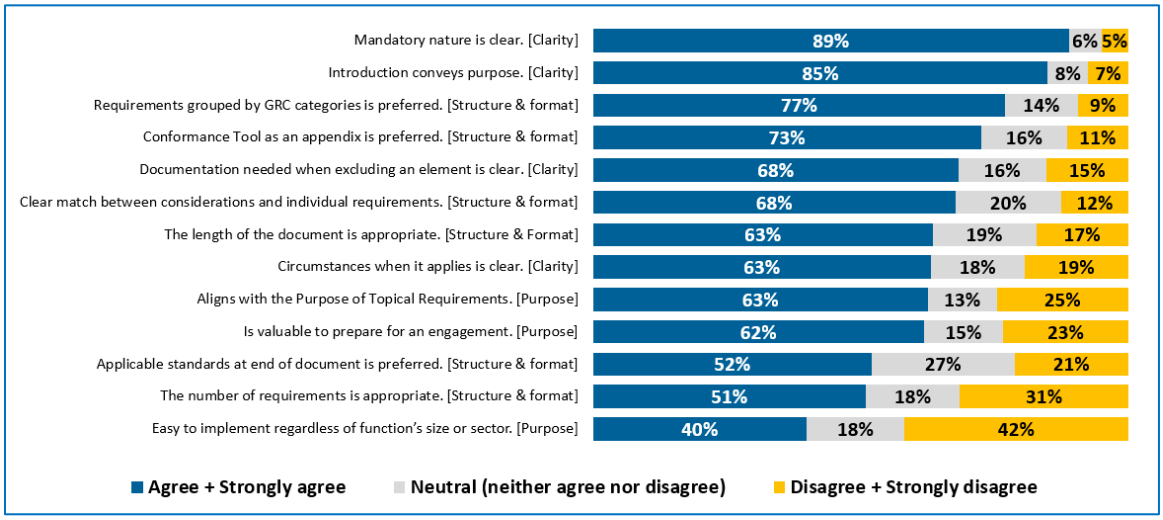
The processes for identifying, assessing, and disposing of themes were documented and presented to the IPPFOC for review. The council verified that the processes were consistent with expectations for standard-setting in the public interest.

Public Agreement

The public comment survey's "agreement" rating questions attempted to gauge satisfaction with the elements of the proposed Cybersecurity Topical Requirement. A stratified view of the results revealed general satisfaction.

Figure 2 shows that the "Strongly Agree + Agree" scores for the mandatory questions ranged from 89 to 40 percent. No matter the level of agreement with each various aspects of the Cybersecurity Topical Requirement, however, disagreements and questions raised were analyzed to detect the reasons and were treated as opportunities to enhance the final version.

Figure 2. Percentage of agreement



Considerations for Re-exposure

During the development of the 2024 Global Internal Audit Standards, the Global Board established criteria to determine whether the revised draft should be re-exposed through an additional public consultation. Since these criteria proved to be effective, the same criteria were applied to determining whether to re-expose the Cybersecurity Topical Requirement.

The GGC and two IIASB members voted that re-exposure was not required as:

- No new content was added compared to the exposed version.
- The requirements had not become more restrictive or stringent compared to the exposed version.
- The changes were based on the comments collected, and no decisions contradicted the majority of the comments or feedback received.

Approvals

Using an online survey tool, the GGC voted to approve the Cybersecurity Topical Requirement, a publication date of 5 February 2025, and an effective date of 5 February 2026.

IIA staff met several times with the IPPFOC to review and provide documentation supporting the due diligence exercised in adhering to the criteria for standard-setting in the public interest. The process documentation included steps for reviewing, approving, and issuing the Cybersecurity Topical Requirement. After a thorough review of the supporting documentation, the IPPFOC approved the adequacy of the due diligence on 28 January 2025. The IPPFOC's approval released the document for publishing, translation, and promulgation.

Disposition of Comments by Major Theme

The GGC working groups read each public comment received through surveys, letters, and interactions with stakeholders. They analyzed the comments grouped by theme. This section describes the 13 major themes, providing context and the resulting dispositions. The order of the listing is alphabetical and does not indicate the level of importance.

Theme: Applicability and Scope

Brief Description

Concerns were raised about when and how to apply the requirements, particularly in relation to risk-based auditing and the scope of different audit engagements.

Disposition and Rationale

The Topical Requirement was revised to be clearer about applicability. The audit plan based on a risk assessment performed at least annually, along with any engagements that address aspects of the topic, are the basis for assessing the relevant requirements outlined in the Topical Requirement. A rationale for the exclusion of specific requirements as nonapplicable must be documented. Chief audit executives should apply professional judgment based on their organization's circumstances. When the topic is identified during planning and included in the risk-based internal audit plan, the requirements of the Topical Requirement serve as the basis for assessing the subject in each relevant engagement. One or more internal audit engagements may address the requirements collectively.

New language added to the Cybersecurity Topical Requirement states:

> *The Topical Requirement is applicable when the topic is one of the following:*
>
> *A. The subject of an engagement in the internal audit plan.*
>
> *B. Identified while performing an engagement.*
>
> *C. The subject of an engagement request not in the original internal audit plan.*
>
> *Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented and retained. Not all individual requirements may apply in every engagement; if requirements are excluded, a rationale must be*

documented and retained. Conformance with the Topical Requirement is mandatory and will be evaluated during quality assessments.

Theme: Burden and Complexity

Brief Description

Some commenters perceived that the new requirements would add significant administrative and documentation burdens, making audit engagements more complex and bureaucratic and less efficient without adding corresponding benefits or value. Some respondents considered the requirements excessive and potentially counterproductive or expressed concerns about the impact on planning.

Disposition and Rationale

Content was added to clarify that, where appropriate, the assessment of individual requirements at the engagement level may be replaced with an assessment at the audit plan level, providing a broader view of how a topic is covered across multiple engagements in the plan.

New language in the Cybersecurity Topical Requirement states:

> *Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented and retained. Not all individual requirements may apply in every engagement; if requirements are excluded, a rationale must be documented and retained. Conformance with the Topical Requirement is mandatory and will be evaluated during quality assessments*.

New language in the user guide states:

> *Coverage of the Topical Requirement can be documented in either the internal audit plan or the engagement workpapers based on auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions*.

Theme: Clarity and Interpretation Issues

Brief Description

Some commenters expressed a need for clearer definitions, specific references, explanations, and guidelines on how to implement the requirements, including specific references to the Standards and detailed steps. The exposed requirements were seen as vague and open to interpretation. Commenters stressed the need to avoid ambiguous terms

and suggested that additional guidance and examples tailored to different sectors and organizational sizes could make the requirements more accessible and easier to apply.

Disposition and Rationale

The Topical Requirement and user guide were revised to clarify that determining the applicability of a Topical Requirement begins with the risk assessment. Once determined to be applicable, the requirements become mandatory, providing criteria throughout the engagement and supporting engagement performance in alignment with the principles and standards of Domain V: Performing Internal Audit Services. Additionally, it was clarified that the chief audit executive retains ultimate responsibility for ensuring conformance with the Topical Requirements when cyber risk assessments or audit engagements are outsourced. Additional details on this responsibility were added to the user guide. No changes were made regarding applicability by sector or size.

Theme: Communication and Training

Brief Description

Commenters requested greater communication, training, and support, including the provision of templates, to ensure all parties understand and can comply with the new requirements. Requests included specific guidance on effectively engaging and communicating with stakeholders to facilitate a smooth transition and clarity when implementing the new requirements. Comments highlighted that a perceived need for significant training and resources could be challenging for some audit functions.

Disposition and Rationale

The Topical Requirement was not impacted by the request for additional guidance. Examples in the user guide provide the necessary implementation details to support practical applications.

Theme: Documentation of Exclusions

Brief Description

The documentation required to justify exclusions of certain elements from engagements was seen as excessive and/or too time-consuming.

Disposition and Rationale

These comments aligned with previously addressed themes. The justification for the applicability or nonapplicability of Topical Requirements is based on the risk assessment. According to the Standards, the risk assessment must be documented. The documented risk assessment may require additional clarification to ensure completeness and transparency regarding any nonapplicable requirements. This could be outlined in a single

document per Topical Requirement annually, at a minimum. However, if a cybersecurity element is not identified and documented during such planning but is later identified during an assurance engagement, its applicability must be determined and documented in the engagement workpapers.

Theme: Evaluation and Feedback

Brief Description

There were suggestions for ongoing evaluation and feedback mechanisms to continuously improve the requirements based on practical experiences.

Disposition and Rationale

While these comments did not affect the content of the Topical Requirement, the development and governance processes include a phase for collecting feedback and conducting periodic reviews to ensure continuous improvement and relevance.

Theme: Explanation of Cybersecurity-Specific Details

Brief Description

Comments highlighted the need to provide additional details and explanations specific to the cybersecurity topic.

Disposition and Rationale

The Cybersecurity Topical Requirement was updated to include a definition of "cybersecurity" and its relationship to overall information security. Clarifications were added to explain the baseline concept, including how the individual requirements within the sections on governance, risk management, and control processes align with widely adopted frameworks such as COBIT and NIST. Additional clarifications address the chief audit executive's responsibility when the internal audit function lacks cybersecurity audit qualifications or when cybersecurity audit services are outsourced. Additionally, the requirements were refined to be more succinct, reduce duplication, and focus more directly on baseline aspects of cybersecurity.

Theme: Flexibility and Professional Judgment

Brief Description

Some commenters expressed the need for more flexibility and the ability to apply professional judgment rather than adhering to strict, prescriptive requirements. Comments emphasized the need for a more flexible, principles-based approach rather than a one-size-fits-all, with the ability to tailor the requirements to accommodate various organizational contexts, sizes, sectors, and audit function maturity levels.

Disposition and Rationale

Clarifications were added to the user guide to acknowledge that the requirements can be applied flexibly at the individual engagement level while ensuring that critical aspects of governance, risk management, and controls are effectively evaluated and communicated in a summarized manner. The user guide also added emphasis on the principle that professional judgment remains a fundamental element of internal audit performance, particularly when assessing the applicability of Topical Requirements within the organization's specific context and circumstances. Documenting the justifications for the nonapplicability of certain requirements ensures transparency and accountability and allows such judgments to be reviewed during the quality assessment process.

Theme: Impacts on Small Audit Functions

Brief Description

Some commenters suggested that the new requirements could disproportionately affect small audit functions and that they may not be able to comply fully without substantial increases in time and resources.

Disposition and Rationale

Clarification was added to highlight that the risk-based approach applies regardless of the internal audit function’s size. Language was added to specify that compliance with a Topical Requirement may be satisfied through the results of engagements conducted under another equivalent set of standards, such as NIST or COBIT. Furthermore, language was added to the user guide to clarify that organizations already aligned with COBIT or NIST may find these frameworks sufficient for meeting the requirements within the Cybersecurity Topical Requirement, but that the internal audit function’s cybersecurity control testing must be thoroughly reconciled with the specified requirements to ensure adequate coverage.

Theme: Implementation Challenges

Brief Description

Concerns were raised about the practical challenges of implementing numerous new requirements, including staffing constraints, disruptions to current audit practices, and a potential diversion of resources from other important efforts. Commenters highlighted the need for specialized expertise, the potential increase in auditing costs, and the lack of consideration for the varying sizes and risk profiles of different organizations. Commenters also emphasized the need for adequate preparation time, with some suggesting a phased approach or flexibility based on organizational maturity and size.

Disposition and Rationale

This theme summarizes comments included in previous themes, and its disposition aligns with those proposed. Setting minimal baseline requirements for auditing cybersecurity is not expected to lead to implementation challenges. The requirements will be effective one year after release, allowing time for adjustment. Additionally, the Global Internal Audit Standards already instruct that internal audit functions experiencing resource limitations, lack of expertise, or other issues must communicate such concerns to the appropriate governance levels to ensure proper resourcing and support.

Theme: Mandatory versus Guidance

Brief description

The Topical Requirements were determined to be a mandatory element of the IPPF at their inception, and therefore, the survey did not include a question on that subject. However, many commenters expressed a preference for the Topical Requirement to be recommended guidance.

Disposition and Rationale

The GGC maintained that keeping the Topical Requirements mandatory is essential to ensuring consistency and quality in internal audit engagement performance. Clear requirements that align practices across the profession help build confidence among internal audit stakeholders by setting expectations and reinforcing the internal audit function's valuable contributions to the assessment of governance, risk management, and control processes. Additionally, such requirements emphasize the necessity of investing in the resources necessary for internal audit functions to operate effectively and meet the demands of an evolving risk landscape. By addressing pervasive and emerging risks, Topical Requirements play a critical role in strengthening the ongoing relevance of the International Professional Practices Framework (IPPF) as a foundational resource for internal auditors worldwide.

Theme: Overlap with Existing Standards

Brief Description

Commenters expressed concern that the new requirements overlap with existing standards, frameworks, and sector-specific regulations (such as NIST, ISO, COBIT, CIS, and local government standards), adding unnecessary complexity, duplication of efforts, potential conflicts, and duplication of roles with other bodies. Recommendations included aligning the new requirements with existing frameworks and standards instead of creating additional requirements.

Disposition and Rationale

Content was added to the user guide, clarifying that organizations already aligned with other frameworks, such as COBIT or NIST, may find them sufficient for meeting the requirements within the Cybersecurity Topical Requirement. However, a reconciliation between the internal audit function's existing cybersecurity control testing and the requirements remains necessary to ensure adequate coverage. When a different framework is applied, documentation can reference the relevant audit steps or tests to demonstrate alignment and coverage with the Topical Requirement. An appendix mapping the requirements to NIST and COBIT was added to the user guide.

Theme: Relevance and Added Value

Brief Description

Commenters questioned the added value of the new requirements and whether they are relevant to all types of engagements and organizations. They expressed skepticism about the benefits and practicality of the requirements in addressing current and future-oriented challenges and raised concerns that the Topical Requirements promote a checklist mentality. Some respondents questioned whether the requirements would be effective in improving the quality of internal auditing or adding value to the organization's cybersecurity.

Disposition and Rationale

Language was added to clarify the value of Topical Requirements. The internal audit function provides assurance to stakeholders that baseline cybersecurity expectations are met, reinforcing the importance of these assessments beyond a simple checklist approach. Auditing a subject covered by a Topical Requirement adds value by addressing pervasive risks warranting organizations' awareness. Assurance engagements linked to these requirements contribute to ensuring consistent, minimum coverage of cybersecurity risks, ensuring a structured and comprehensive approach. The Topical Requirement supports a globally consistent framework for auditing cybersecurity, enhancing the reliability and comparability of internal audit practices.

Theme: Risk of Overreach

Brief Description

Some commenters viewed the new requirements as an overreach by The IIA that could diminish the perceived value and agility of the internal audit function. They were concerned about the requirements' practicality and relevance, especially for mature audit functions already following recognized standards.

Disposition and Rationale

Additional context was added to clarify that Topical Requirements establish a baseline of performance for internal auditors when conducting assurance services related to the subject of a Topical Requirement. The new content emphasizes that audit coverage should be risk-based, with the level of detail and scope determined by factors such as risk exposure, expertise, organizational structure, technical complexity, and available staffing.

Acknowledgements

The IIA is grateful to the stakeholders that provided guidance and assistance in developing the Cybersecurity Topical Requirement and particularly recognizes members of the Global Guidance Council, a global group of internal auditors who have generously volunteered their time and expertise to ensure the Topical Requirements elevate the professional practice of internal auditing.

For initiating the project, The IIA thanks members of the Topical Requirements Task Force, including Sally-Anne Pitt (lead), Jose Esposito, Marthin Grobler, Michael Levy, Mouri Naohiro, J. Michael Peppers, Paul Sobel, and Tania Stegemann. The IIA appreciates members of the Global Board of Directors and International Internal Audit Standards Board for their contributions to the quality of the publication and the IPPF Oversight Council for its role in promoting a standard-setting process that serves the public interest.

Finally, The IIA thanks these advisors who provided technical expertise: from The IIA's IT Knowledge Group, Scott Moore and Jim Enstrom; from Deloitte, Dawn Jones and Brittany Long; from Protiviti, Ari Sagett, Kristen Kelly, Jennifer Boyle, and Andrew Struthers-Kennedy; from PwC, Shaun Wilcocks, Amanda Herron, Deborah Mack, Rachel Nelson, Lisa Bowgren, and Pieter Joubert; and digital security expert Marc Vael.

About The Institute of Internal Auditors

The Institute of Internal Auditors® (The IIA) is an international professional association that serves more than 260,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information www.theiia.org.

Disclaimer

Copyright

February 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101