# Topical Requirements

## Application Guidance

The Institute of
Internal Auditors

# Topical Requirements Application Guidance

## Contents

# Topical Requirements Application Guidance

The International Professional Practices Framework® comprises Global Internal Audit Standards™, Topical Requirements, and Global Guidance. Topical Requirements are mandatory for assurance engagements and recommended for advisory engagements in specific risk areas. They must be used with the Standards, which provide the authoritative basis for the required practices.

Topical Requirements provide a consistent minimum baseline for coverage in specific risk areas. Internal auditors must apply additional procedures when organizational risks, regulations, or context demand greater depth.

## 1. The Role of Professional Judgment

The application of professional judgment is essential to effectively use Topical Requirements and is explicitly required by the Standards. Professional judgment allows internal auditors **to tailor Topical Requirement application to the organization's unique context, risk profile, and strategic priorities, ensuring that audit coverage is relevant and proportionate**.

Professional judgment is exercised at various stages of the audit lifecycle. It plays a role during the **internal audit planning process**, as described in Standard 9.4 Internal Audit Plan, where decisions are made about which Topical Requirement-related risks are significant enough to warrant coverage. It is also used **when defining the scope and objectives** of an engagement under Standard 13.3 Engagement Objectives and Scope, particularly in determining whether the Topical Requirement should be applied fully or only in part. Furthermore, judgment is **applied when evaluating and documenting applicability and exclusions**, selecting evaluation criteria (Standard 13.4 Evaluation Criteria) and work program steps (Standard 13.6 Work Program), and when **deciding whether audit evidence from external assurance providers**, such as regulatory audits, meets the requirements.

While conformance with the Topical Requirements is expected, there may be exceptional circumstances, such as resource constraints or sector-specific considerations, where full conformance is not feasible. In such cases, the chief audit executive should implement alternative actions that achieve the intent of the requirement and must document and communicate the rationale for the

deviation. This **"conform or explain" approach** aligns with the principles outlined in the Standards.

According to Standards Principle I, Purpose of Internal Auditing, internal auditors must demonstrate integrity and objectivity in using professional judgment. Standard 4.1 Conformance with the Global Internal Audit Standards requires that such judgment be exercised with due professional care. This means that decisions must be reasoned and evidence-based, not arbitrary or intuitive. They should be consistent with internal audit methodology and aligned with organizational risk priorities. **All judgment-based decisions should be clearly documented** in the audit planning records, engagement workpapers, or Topical Requirement applicability matrices, and **must be transparent and defensible during quality assurance reviews or external assessments**. Documentation reflects the importance of a well-reasoned and thoughtful approach: Demonstrating compliance becomes more straightforward when the rationale is clearly documented.

Professional judgment does not replace structure; it enables internal auditors **to adapt structured requirements like Topical Requirements to complex realities**. Professional judgment ensures that audit efforts are not only aligned with the Standards but also tailored to organizational needs, delivering assurance that is both credible and relevant.

## 2. A Risk-Based Approach to Determine Applicability

Audit activities follow a risk-based approach to ensure resources are focused on areas of greatest significance. Identifying audit topics and determining scope should be grounded in a thorough and well-documented risk assessment. A Topical Requirement applies when the topic **is identified during this risk assessment and the risk exceeds a significant risk level**.

To **assess the significance of a Topical Requirement-related risk**, the internal audit function should first identify the risk based on the organization's strategic objectives, known exposures, past incidents, or environmental changes. Next, the inherent risk should be assessed by evaluating its impact and likelihood. This "risk score" can then be compared to the defined risk appetite of the organization to determine whether it exceeds the critical threshold. [1]

[1]Internal auditors may consider using a recognized risk scoring tool such as The IIA's Enterprise and Business Process Risks Tool guidance. Enterprise and Business Process Risks | The IIA.

**Defining the critical threshold** relates to the organization's risk appetite, which is shaped by board and senior management input. Considerations include financial, legal, regulatory, and compliance impacts, and qualitative impacts such as reputational damage or failure to meet strategic or ethical expectations. Leadership provides clear direction on which risk types are only accepted to a limited extent or intolerable, even at lower likelihoods. Clear expectations from the board and senior management, and agreed-upon understanding for ratings, are critical to ensure consistent and risk-aligned judgments on the significance of risks.

Once a risk is identified as significant, it should be **mapped to the relevant Topical Requirement and its governance, risk management, or controls component to determine which requirements apply**. All requirements should be reviewed for relevance. Where specific requirements are deemed not applicable based on the risk's nature, context, or root cause, these exclusions must be clearly documented, including the justification for their omission. For example, if the risk arises from a breakdown in control execution rather than governance, only the control-related components may be relevant. This ensures the audit is both risk-aligned and appropriately scoped.

Finally, **professional judgment** must be applied to confirm the applicability of the decision, and the decision and the rationale should be properly documented.

## 3. Mandatory Requirements Related to the Topic Identification

Topical Requirements are mandatory for assurance engagements when the risk is identified during the risk assessment and exceeds a critical threshold (see 2. A Risk-Based Approach to Determine Applicability). This may refer to the periodic risk assessment used to develop the audit plan and the specific risk assessment conducted to define the scope of an audit engagement. Topical Requirements are recommended for advisory engagements when the topic relates to the engagement's objectives.

Topical Requirements are applicable **when the topic is explicitly included in the internal audit plan as an assurance engagement**. Application may be through a comprehensive topical audit focused entirely on the subject, or the requirements may be addressed across several engagements, potentially spread over multiple years. In such cases, internal auditors must ensure that all relevant requirements are eventually covered and that engagement documentation clearly shows how and when each part is addressed.

Topical Requirements must also be applied **when the topic is identified during an engagement**, which means the topic has reached a prioritized level above the critical threshold, based on the organization's risk appetite. It should be treated as a significant risk requiring attention, in line with the engagement's objectives and risk assessment. Importantly, not all parts of the Topical Requirement must be applied if the identified risk pertains to only a subset of governance, risk management, and control elements (for example, only controls or governance). The scope of application must align with the nature and boundaries of the risk identified and the objectives of the audit. Professional judgment should be used to determine which requirements are relevant and proportionate to the level and type of risk.

A Topical Requirement is also **applicable when the topic becomes part of an engagement added upon request**, even if it was not originally included in the audit plan. In these cases, applying the Topical Requirement must still follow a risk-based approach. Internal auditors may apply either the full set or only a subset of the requirements depending on the materiality of the risk and its alignment with the organization's risk thresholds.

## 4. Applying Topical Requirements in the Audit Lifecycle

Once a risk is deemed significant through the risk assessment and a Topical Requirement is applicable, internal auditors should apply the Topical Requirement consistently throughout the audit lifecycle:

### At the Audit Planning Level

During the development of the audit plan, in line with Standard 9.4 Internal Audit Plan, Topical Requirement-related risks identified as significant should be appropriately reflected by including **a standalone topical audit or integrating the requirements into multiple engagements, potentially spread across audit cycles or years**. In either case, it is important to clearly reference the applicable Topical Requirement in the audit universe, the risk assessment documentation, and the planning records to ensure transparency and alignment with both organizational priorities and professional standards.

### During Engagement Performance

Internal auditors should apply professional judgment to tailor the application of the Topical Requirement to the specific characteristics of the risk. Standard 13.3 Engagement Objectives and Scope includes considering the underlying cause of the risk and identifying which elements of governance, risk management, or

control are most relevant to the risk's manifestation and impact. Based on this analysis, **only those requirements directly aligned with the defined engagement scope and objectives need to be applied**. As a result, certain parts of the Topical Requirement may be justifiably excluded when they fall outside the scope of the identified risk and engagement objectives. These exclusions should reflect a risk-based and proportionate approach and must be clearly documented in the engagement work papers, including a rationale that demonstrates alignment with the engagement's focus.

Internal auditors should then perform **fieldwork** to support conclusions on the applicable requirements to ensure meaningful and targeted coverage.

## 5. Limitations and Scope Exclusions

Applicability and exclusion decisions are required **once the topic is identified as a significant or prioritized risk**, but these decisions can be documented **at different stages in the audit process**. For instance, they may be recorded at the audit plan level when the topic is covered by a dedicated engagement or distributed across multiple engagements over time. Alternatively, they may be documented at the engagement level when the topic is identified during planning or fieldwork, or when stakeholders request coverage.

Good documentation practices involve applying clear and defensible logic when determining and recording the scope of the Topical Requirement application. Practices include assessing the **relevance of the applicable requirement(s) through evaluating the** organizational context and the specifics of the identified risk. Exclusions or partial applications should be supported by appropriate references, such as risk ratings, scope limitations, professional judgment applied, and the rationale behind the selected coverage. Solid documentation and justifications help auditors feel confident in their coverage and reduce the doubt of missing something.

Importantly, a **well-performed risk assessment should already generate much of the required documentation**, making this process an integrated part of audit planning and not an administrative burden. Furthermore, this documentation is critical, as it will be used during **quality assessments** to evaluate whether Topical Requirements were appropriately and consistently applied.

Tools provided in the user guide, such as a **Topical Requirement applicability matrix,** can support consistency, traceability, and alignment with professional standards.

## 6. Addressing High-Risk Areas Not Yet Mature

When a topic is identified as a high-risk area but the organization's governance, risk management, and control maturity around it is low, the internal audit function is still responsible for addressing it.

According to the Standards, the internal audit function must ensure that significant risks are brought to the **board's and senior management's attention**. Clear and candid conversation is required to ensure leadership understands that the risk area contains substantial exposures currently not adequately covered by existing structures or processes.

In such cases, the Topical Requirement may serve within the context of an advisory engagement as recommended guidance and provide a valuable framework to evaluate gaps, highlight exposures, and create awareness across the organization.

Even if full assurance cannot yet be provided, the internal audit function's role is to ensure transparency, promote awareness, and encourage management to take ownership of the issue. In addition, the matter should be elevated to the board to ensure awareness and alignment on the appropriate approach.

## 7. Resource Constraints

If the internal audit function lacks the capacity, such as time, staffing, or budget, or the necessary competencies, including subject-matter expertise or technical skills, to fully apply a Topical Requirement, this does not waive the responsibility to assess the risk or determine applicability. Per Standard 8.2 Resources, **the chief audit executive must inform the board of such resource limitations and explain how they will be addressed**.

In response to resource constraints, the internal audit function **may develop internal capabilities** through targeted training or recruitment. Alternatively, it may **outsource or cosource** the engagement to qualified external specialists. In some cases, the audit may be **rescoped**, but only when this decision is supported by a documented rationale and agreed upon or approved by the board.

The chief audit executive is responsible for ensuring conformance with the Topical Requirement and identifying options to achieve it, such as outsourcing, while retaining overall accountability. In cases of nonconformance, internal audit

must ensure that this **is transparently disclosed** along with the underlying reasons, such as resource limitations. All related mitigating actions must be clearly documented in the audit plan and engagement files, maintaining accountability and traceability throughout the process.

## 8. Regulatory Alignment and Use of Other Frameworks

Topical Requirements are globally applicable and set a minimum baseline for internal audit coverage of specific risk areas, regardless of an organization's size, sector, or maturity. However, organizations may also be subject to **external regulatory requirements, standards, or frameworks**, such as NIST, ISO 27001, SOC reports, laws and regulations, or industry-specific obligations, that overlap with or go beyond the scope of a given Topical Requirement.

Internal auditors are expected to adopt a **risk-based and comparative approach** when this occurs. If a regulatory requirement or external framework imposes a **stricter or more comprehensive obligation** than the Topical Requirement, then that higher standard should guide the scope of the audit. In fact, most regulatory frameworks, particularly in high-risk areas such as cybersecurity, third-party management, or financial services, tend to be more detailed and demanding than the corresponding Topical Requirement. As such, where organizations already conform to these more rigorous standards, demonstrating alignment with the Topical Requirement should generally not require significant additional effort, provided the linkage is documented and the coverage assessed for sufficiency.

**Mapping the Topical Requirement against regulatory requirements and other recognized frameworks** is considered good practice. Mapping enables the internal audit function to demonstrate how requirements are being met — either directly or through reliance on existing regulatory audit evidence — while ensuring that no critical gaps are overlooked. For example, if a cybersecurity audit has already been performed under NIST guidance by another assurance provider, the internal audit function may reference and leverage that work to confirm alignment with the Cybersecurity Topical Requirement. However, it must be explicitly documented, and the sufficiency of the evidence should be assessed using professional judgment (see also Global Practice Guide: Coordination and Reliance: Working with Other Assurance Providers).

Ultimately, applying Topical Requirements in a regulated environment requires **careful coordination**. Internal auditors should ensure their approach reflects the most rigorous applicable standard while avoiding duplication and leveraging

existing controls, assessments, and external audits where appropriate. This supports efficiency and credibility and ensures that internal audit continues to meet its responsibility under the Standards to provide **independent, risk-based assurance** that is both **context-aware and globally consistent**.

## 9. Applying Multiple Topical Requirements

**Applying multiple Topical Requirements** within a single audit engagement depends entirely on the specific significant risks identified through the **organization's risk assessment process.** Rather than assuming that multiple Topical Requirements should be applied together by default, internal auditors must assess whether the nature and scope of the risk actually necessitate the use of more than one Topical Requirement.

For example, if a significant risk is identified in the area of third-party cybersecurity when a third party provides cybersecurity services, it may be appropriate to apply both the Cybersecurity Topical Requirement and Third-Party Topical Requirement. However, if the risk pertains solely to third-party contractual compliance without cybersecurity implications, then only the Third-Party Topical Requirement would apply. This ensures that the audit scope remains **targeted to prioritized risks and avoids any unnecessary coverage expansion.**

Internal auditors should clearly define the scope **based on the significant risks identified** to avoid audit scope creep — where the audit may inadvertently extend beyond its original objectives The audit objectives should align with the organization's risk appetite, strategy, objectives and priorities. The rationale for including or excluding specific Topical Requirements should be documented in the engagement planning records. This disciplined approach helps safeguard the integrity of the audit process, ensures efficient use of resources, and delivers focused assurance on the organization's most pressing risks.

## About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 265,000 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, visit theiia.org.

## Disclaimer



## Copyright



August 2025

The Institute of
Internal Auditors

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