Topical Requirements – Practical Application Guidance and Notes from External Quality Assessments

Management Summary

With the introduction of the Global Internal Audit Standards 2024 (hereinafter referred to as the "Standards"), The Institute of Internal Auditors (IIA) created a new mandatory element within the International Professional Practices Framework (IPPF): the Topical Requirements (TR). These requirements define a mandatory minimum scope for audits in certain risk areas and are intended to support consistent quality standards for internal audit worldwide.

The first TR will take effect in 2026, requiring internal auditors to align their planning and audit processes accordingly. The IIA provides several official documents that clarify key questions and support practical implementation. A key implementation point is that TR must be used only when a topic is classified as material in the context of the periodic overall risk assessment (or during the engagement-level risk assessment) and an assurance engagement is planned for that topic. Materiality is assessed in the context of the organization's risk appetite and strategic objectives. Whether a TR must be applied depends on the results of the risk assessment and the resulting scope of the engagement, and requires the internal auditor's professional judgment.

The IIA expressly emphasizes the importance of a clear and understandable justification process. If a TR is not applied, or is applied only in part, even though a material risk has been identified within the scope of a TR, the rationale for why the relevant TR or requirement is not applicable or does not address the root cause of the risk must be documented.

With this in mind, the IIA Switzerland Professional Services Firms Group developed this white paper. It combines findings from initial application pilots in the Swiss market with perspectives from external quality assessments. Its purpose is to support auditors in the consistent, risk-based, and pragmatic implementation of the new requirements. This document is not intended to be exhaustive or officially binding; it reflects only the views and interpretation of the author team and the working group at the time of publication, and is intended to serve as practical guidance.

Getting Started – Orientation to TR and Official Sources

The IIA provides all essential information about the TR centrally on its website.

- Link to page: https://www.theiia.org/en/standards/2024-standards/topical-requirements/

This content is continuously updated and forms the primary basis for applying TR in day-to-day internal audit practice. It includes published TR, ongoing consultations, and future publications. For each TR, the IIA clearly indicates when mandatory application begins - usually one year after publication.

The first TR take effect as follows:

- Cybersecurity: February 5, 2026
- Third Party: September 15, 2026
- Organizational Behavior: December 15, 2026
- Organizational Resilience: April 30, 2027

In addition to the TR themselves, the IIA provides several supporting materials that promote consistent application:

- The Topical Requirements Application Guide, available in multiple languages, provides general and practical implementation guidance.
  - https://www.theiia.org/en/content/topical-requirements/topical-requirements-application-guidance
- An FAQ section is available on the TR website.
- The document Assessing Topical Requirements Conformance (Insights to Quality) provides guidance on how TR conformance is considered in internal and external quality assessments, and how internal audit functions can prepare through meaningful implementation and transparent documentation.
  - https://www.theiia.org/globalassets/site/content/insights-to-quality/insights-to-quality-assessing-topical-requirements-conformance.pdf

For internal audit functions, it is advisable to establish structured and regular monitoring so that updates can be considered in a timely manner. This includes, in particular:

- early identification of new or revised TR,
- participation in consultation processes,
- timely implementation.

Outlook on Expected Topics

The IIA has additional TR in development. At the time of publication of this paper, the consultation process for the Anti-Corruption TR is under way. In addition, a TR on Talent Management has been announced, with the consultation process scheduled for October 2026. These two TR will not be applicable before 2027.

In addition, the IIA regularly presents its Risk and Topic Radar at events and webinars. Topics shown as "Mature" in the graphic below (see Fig. 1, in blue) are considered established; TR are particularly likely for these areas.

Important, highly dynamic topics that appear in the radar as "Emerging" (see Fig. 1, in green) are not currently being translated into TR.

The regular monitoring process recommended in the previous section should therefore also include a periodic review of the IIA website to stay informed early about new consultations and future TR topics.

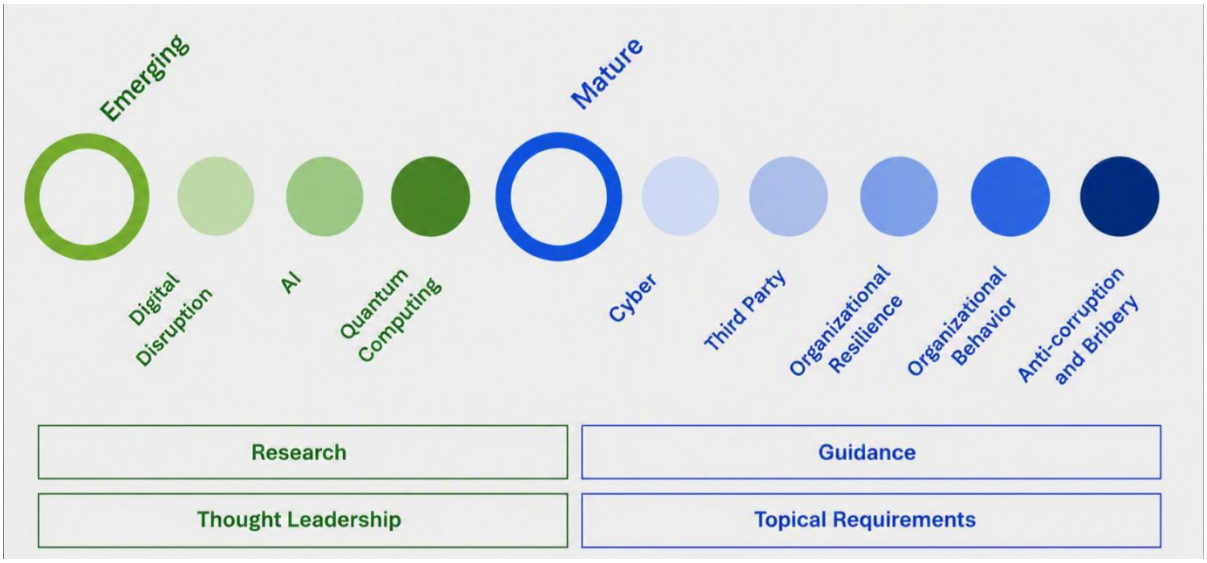

Fig. 1: Extract from "The IIA's Risk and Topics Maturity Radar," source: IIA

Application of TR

The TR are a mandatory part of the IIA's IPPF and must therefore be applied to assurance engagements, similar to the Standards. For advisory engagements in relevant risk areas, their application is recommended but not mandatory.

The TR Application Guide specifies that TR may be used in the following cases:

- if the topic is explicitly included as an audit engagement in the audit plan,
- if the topic is identified during an audit engagement,
- if the topic is included in an audit engagement, even though it was not originally included in the audit plan.

Audit topics are usually identified as part of the periodic risk assessment (in accordance with Standard 9.4), during the engagement-level risk assessment (in accordance with Standard 13.2), or while performing the audit. A TR must be applied as soon as a corresponding risk is identified and assessed as material. Consequently, the relevant risk assessment should determine whether risks related to existing are present. If such a topic is included based on the risk assessment, stakeholder input, or during the execution of an audit engagement, the corresponding TR must be applied.

Once a risk is classified as material and a TR is applied as a result, the internal audit function must consider the TR, meaning that its applicability must be analyzed and documented. The outcome of this analysis may be the application of the TR in the audit, or the partial or complete exclusion of certain TR elements. At a minimum, this consideration must be ensured at the level of the relevant engagement. However, the IIA's supplementary guidance provides the foundation for a holistic approach spanning the entire audit lifecycle—from periodic planning and engagement-level planning through the execution of the engagement in accordance with the applicable Standards.[1] This also applies when an engagement is performed under a co-sourcing or outsourcing arrangement. In such cases, the engaging internal audit function remains responsible for ensuring conformance with the applicable requirements throughout the entire engagement lifecycle.

[1] See, for example, the IIA's *Topical Requirements – Application Guidance*, Chapter 4: *Applying Topical Requirements in the Audit Lifecycle*.

To support this, the IIA Switzerland working group provides a decision tree that systematically presents the process for determining applicability (see Fig. 2). It makes it easier to assess the relevant factors conclusively and consistently. The decision tree also indicates the cases in which clear documentation of the "comply or explain" approach is necessary (see further details in the next section).

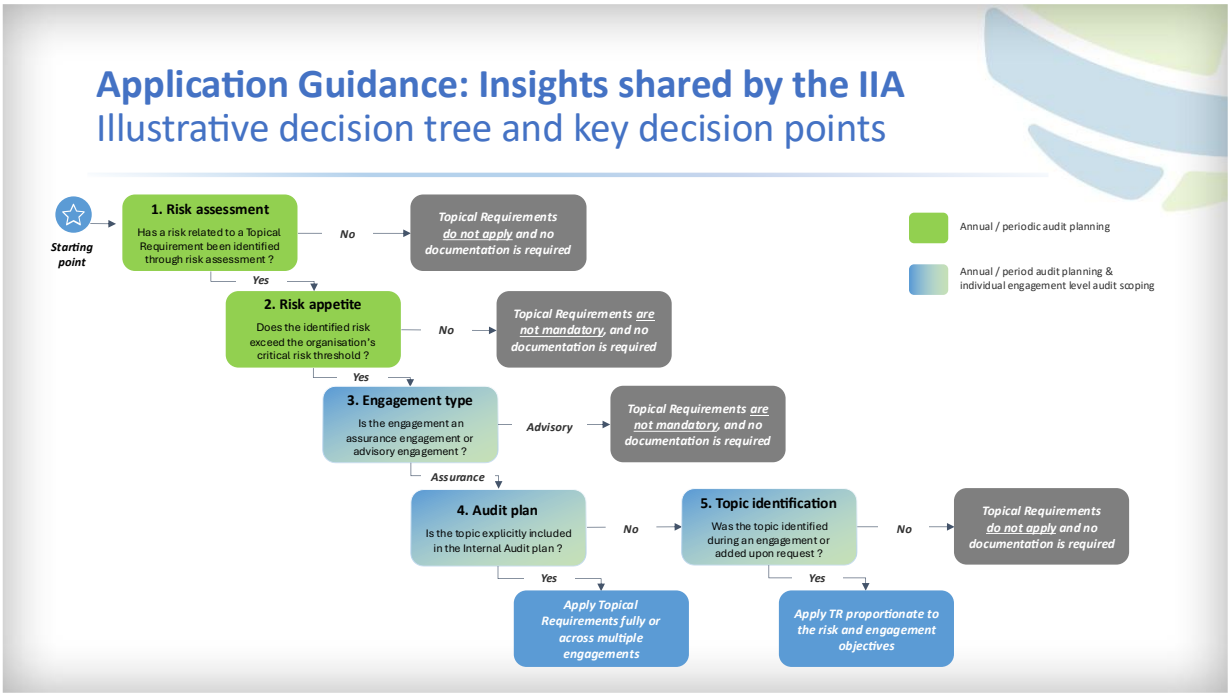

Fig. 2: Decision tree for applying the Topical Requirements, source: IIA Switzerland Professional Services Firms Group

Professional Judgment in Application

Professional judgment is central to all decisions regarding the application of a TR. The IIA explicitly refers to the "comply or explain" approach if an identified material risk makes application of a TR mandatory and the internal audit function nevertheless does not include it in the audit:

- If certain requirements of a TR are not applicable due to the nature, context, or cause of a risk, this must be clearly justified and documented.
- For example, if a risk arises from an operational control weakness, control-specific requirements may be primarily relevant, while certain governance elements of the TR may not be applied.

The Application Guide emphasizes that exceptional circumstances, such as resource constraints or sector-specific characteristics, may also justify deviations. In such cases, the auditor should define alternative measures that align with the purpose of the relevant requirement. Work performed by other internal and external assurance providers may also be considered. Transparent and understandable documentation is essential in these cases.

Coverage of TR Requirements Across Multiple Years or Engagements

If an audit topic is addressed over several years, the corresponding TR must be considered again for each audit engagement and its applicability must be reassessed. Requirements may be covered across several audits, even over multiple years, provided this is clearly documented:

- which elements were covered and when,
- which parts were deliberately deferred to later years,
- and why this decision is technically justified.

This means that not all requirements must necessarily be covered in a single audit engagement.

The Application Guide requires all discretionary decisions (for example, partial application or non-application) to be documented in planning documents, working papers, or applicability matrices, and presented in an understandable manner during quality assessments.

Documentation Expectations

The application of a TR, as well as the partial or complete exclusion of certain elements based on professional judgment, must be documented so that an independent third party can understand the decisions made. Documentation may be prepared directly at the points in the audit lifecycle where applicability is analyzed (see the "Decision Tree for Applying TR" in Fig. 2).

To document the application of a TR in an engagement, the user guide for each TR provides an optional documentation tool or table in the appendix.

In an assessment, for example in the context of an external quality assessment (EQA), it is critical that the decisions made and their justifications are sufficiently documented and understandable to third parties. As an integral part of the IPPF, TR are incorporated into the assessment of the relevant principles, particularly in the context of planning, conducting, and communicating engagements. Individual TR are not assessed separately.

If individual TR are relevant to certain engagements, a Standard can be classified as "fully conforms" in an EQA only if all elements of the underlying Standard have been met.

Application in Conjunction with Regulatory Requirements

As explained in the IIA's official Application Guide, the following applies:

- If laws, regulations, or other external requirements impose stricter or more comprehensive requirements than the TR, those requirements determine the scope of the audit.

In such cases, internal audit must apply a risk-based and comparative approach, balancing regulatory requirements, the TR, and other recognized frameworks.

It should be emphasized that TR do not prescribe the organizational design of the audited topics; rather, they define the audit approach. Their purpose is to ensure a consistent approach in critical audit areas and to meet baseline quality requirements.

Reporting on TR Aspects

Conformance with the TR must be documented as part of audit planning and execution and is also monitored through the Quality Assurance and Improvement Program (QAIP) of the internal audit function.

Separate reporting on TR conformance (for example, to executive management and/or the board) is not required. Rather, these aspects should be considered implicitly in overall QAIP reporting.

Guidance for EQA Assessors

For EQA assessors, the IIA's official content - particularly the materials available on its website - is a key reference point. These materials define the IIA's expectations for TR implementation and for assessing conformance in the context of quality assessments. The document Assessing Topical Requirements Conformance (Insights to Quality) is particularly relevant, as it provides detailed guidance on application.

Topical Requirements are a mandatory component of the IPPF and are therefore assessed in internal and external quality assessments in the same way as other elements of the IPPF, such as the Standards. The IIA's 2024 Quality Assessment Manual states that assessors should review the risk-based audit plan to confirm that TR in effect during the audit period have been properly considered. This review is typically performed, among other procedures, by inspecting working papers at the individual engagement level.

The document Assessing Topical Requirements Conformance clarifies how internal audit functions and assessors should proceed when evaluating TR conformance. In this context, the IIA recommends the following in particular for internal audit functions:

- Integrating TR into planning and audit processes,
- Transparently documenting applicability and the rationale for cases of non-application,
- Ensuring that audit engagement processes, working papers, and other documentation reflect TR conformance in an understandable manner.

Accordingly, depending on how the TR have been implemented within each internal audit function, assessors will consider the various elements of the audit process—beginning with the analysis of the audit universe, the risk assessment, and the internal audit planning process—and assess whether any topics covered by the TR are present.

Authoritative documents used by assessors include:

- Risk assessment and audit plan (periodic planning and engagement-level planning),
- Planning memoranda and working papers at the engagement level,
- Risk and control matrices,
- TR User Guide Documentation Tool or the corresponding checklist,
- Coverage of the TR in the QAIP.

Focus Cybersecurity TR: Overview of Areas to Be Examined

- Governance: Assessment of strategic management and structural embedding. The following is examined:
  - Existence of a formal cybersecurity strategy that is regularly updated and reviewed by the board of directors (including budget approval).
  - Establishment of clear policies and definition of roles and responsibilities within the organization.
  - Assurance and assessment of the necessary specialized knowledge and skills of responsible personnel.
  - Stakeholder management: active involvement of stakeholders such as executive management, HR, legal, compliance, and vendors in discussions about threats and vulnerabilities.
- Risk management: Review of cybersecurity risk management processes. The following is examined:
  - Systematic identification, analysis, mitigation, and monitoring of cyber threats across all organizational units.
  - Clear assignment of responsibilities for ongoing monitoring and reporting of the risk situation.
  - Established processes for rapid escalation when thresholds are exceeded, as well as measures to promote general risk awareness.
  - Validation of a response and recovery process (detection, containment, and follow-up) that is regularly exercised.
- Control processes: Verification of whether internal and supplier-based controls are in place to protect the confidentiality, integrity, and availability of systems and data. This includes, but is not limited to:
  - Lifecycle management of all IT assets (hardware, software, and external services) from selection to decommissioning.
  - Continuous vulnerability monitoring and talent management to promote technical capabilities.
  - Processes to strengthen IT security, including encryption, patch management, access management, software development (DevSecOps), and configuration management.
  - Network controls, such as network segmentation, firewalls, VPN/Zero Trust access (ZTNA), IoT controls, and intrusion detection and prevention systems (IDS/IPS).
  - Endpoint security for services such as email, browsers, videoconferencing, and cloud applications.

Organization and Planning of an Audit Using the Cybersecurity TR as an Example

Trigger for the Audit

In principle, the TR requirements must be applied as soon as cybersecurity is identified as a material risk in the context of the periodic risk assessment and an assurance engagement is planned for the topic. This applies if the topic is explicitly included in the audit plan, if it arises as a material risk in the context of another audit engagement, or if stakeholders request an additional, unplanned audit engagement.

In the detailed planning of the audit engagement, it must be demonstrated that the individual TR requirements have been assessed for applicability. If certain elements are excluded from the scope, or included only in part, this deviation must be justified and documented. The deviation may also be summarized for one of the three TR areas - governance, risk management, or control processes - if, for example, governance aspects are excluded from the planned audit for a clear reason (e.g., reviewed by another assurance provider, included in multi-year planning, etc.).

A single audit is not required to cover all cybersecurity requirements at once. In fact, a targeted audit approach may be advisable for various reasons, because a comprehensive audit can be difficult to execute from both a logistical and technical perspective, particularly for the Cybersecurity TR. The internal audit function may distribute the requirements across several audits and multiple years. However, this approach requires documentation of which topics were covered and when, which aspects were deliberately deferred, and why this is technically justified. The application of the requirements must also be presented transparently in planning documents and working papers so that third parties can understand it.

Audit Planning

From a content perspective, the IIA strongly relies on established standards. The Cybersecurity TR refers to the National Institute of Standards and Technology (NIST) at the outset to establish basic definitions of cybersecurity and information security. In addition, the TR requires the internal audit function to take a comparative approach, particularly if regulatory requirements already exist or if audits are performed based on internationally recognized frameworks. Aligning audit planning with the NIST framework is therefore fully consistent with this approach.

Example of a three-year audit plan based on the minimum requirements:

Year	NIST Core Function	Focus according to the Cybersecurity TR	Specific Audit Objectives and TR Requirements
Year 1	Identify	Governance and Foundation (parts of risk management and controls)	Strategy and Roles: Maintain a formal strategy, define responsibilities, and involve stakeholders. Risk Identification: Processes for analyzing cyber threats across the organization.

			Asset Management: Cybersecurity throughout the lifecycle of all IT assets (hardware, software, and vendors).
Year 2	Protect	Preventive Control Processes (controls and specific risk management)	System and Network Security: Access management, encryption, patch management, and DevSecOps. Infrastructure: Network controls (firewalls, ZTNA, segmentation) and endpoint security (email, cloud, browser). Human Factor: Talent management to maintain technical skills and raise employee awareness.
Year 3	Detect, Respond, and Recover (Detect, Respond, Restore)	Monitoring and Event Management (Residual Controls and Risk Management)	Monitoring: Continuous monitoring of vulnerabilities and use of intrusion detection/prevention systems (IDS/IPS). Escalation: Processes to report unacceptable risks to management promptly. Incident management: Implementation and regular testing of an incident response and recovery process (detection, containment, recovery, and follow-up).

This white paper was prepared by the Professional Services Firms Group of IIA Switzerland. The co-authors, Urgent Azizi, Markus Berger, Christian Jung, and Markus Pfeiler, gathered and incorporated the views and contributions of additional experts as well as those of IIA Switzerland. The purpose of this white paper is to support internal auditors in implementing the Topical Requirements and to serve as practical guidance for their application.