Addressing New Topical Requirements within the IPPF Framework

Kat Seeuws

CIA, CGAP, CRMA, CFE, CISA
Vice President,
Standards & Guidance

International Professional Practices Framework®
(IPPF)

The Institute of Internal Auditors®

Agenda

Addressing New Topical Requirements within the IPPF Framework

- Topical Requirements within the IPPF
- Topical Requirement Cybersecurity
- Applying Topical Requirements
- Workshop Exercise
- What's next?
- Q&A

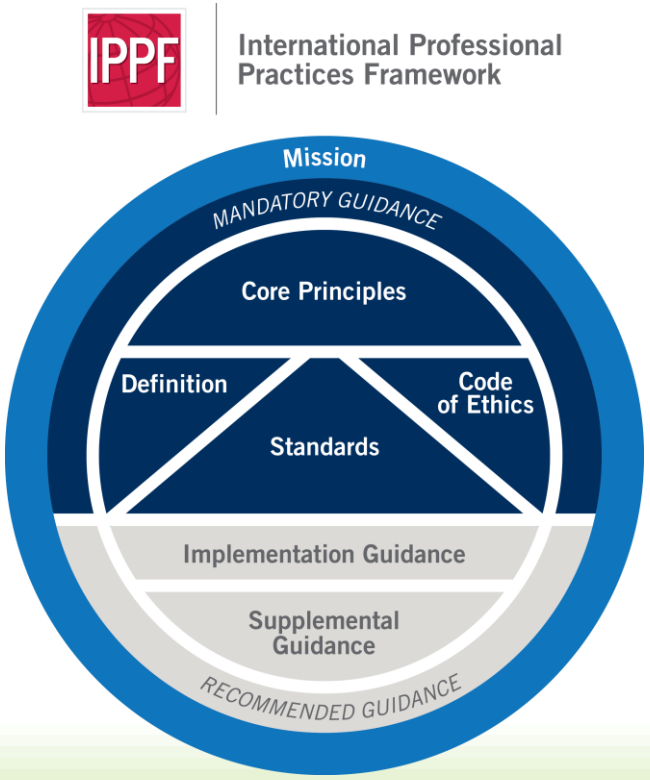
International Professional Practices Framework®
(IPPF)

Topical Requirements within the IPPF

International Professional Practices Framework®
(IPPF)

Topical Requirements within the IPPF

2017



2024

Topical Requirements

Are

- Required when providing **assurance** on a specific risk area.
- Applicable when the topic is identified based on the **risk assessment**. Limitations must be documented.
- **Baseline criteria** when performing engagements in the specific risk area.
- Inclusive of aspects of **governance, risk management,** and **control processes**.
- Subject to **external quality assessment**.

Are Not

- **Required** by the internal audit function to audit the specific risk area unless indicated by a risk assessment.
- Comprehensive **work programs.**
- Designed to address **emerging topics.**
- Substitutes for risk assessments or **professional judgment**.
- Designed to circumvent or replace **legal and regulatory requirements.**

Topical Requirements

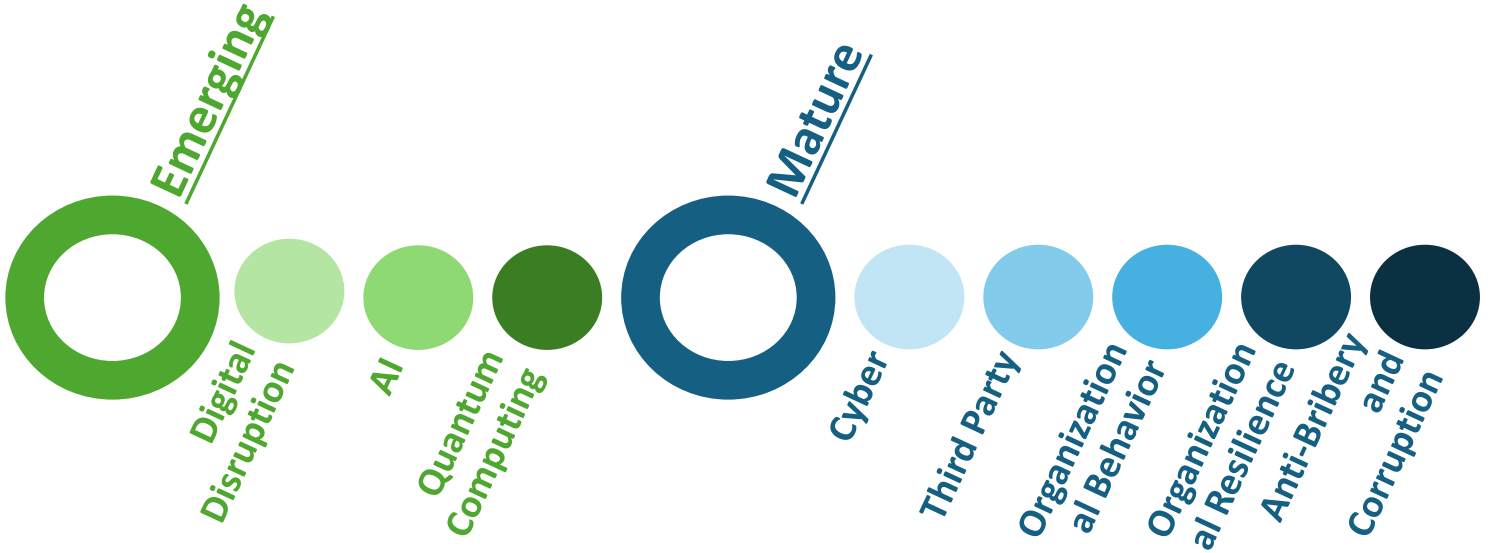
Why?

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

How?

- Developed by **experts and internal audit leaders globally** representing various sectors and industries.
- Includes **broad proactive stakeholder outreach and feedback** through a public consultation period.
- Involves **ongoing oversight of due process** by the IPPF Oversight Council, an independent body comprising representatives of global organizations.

Topic Progression in IIA Portfolio



Research

Thought Leadership

Guidance

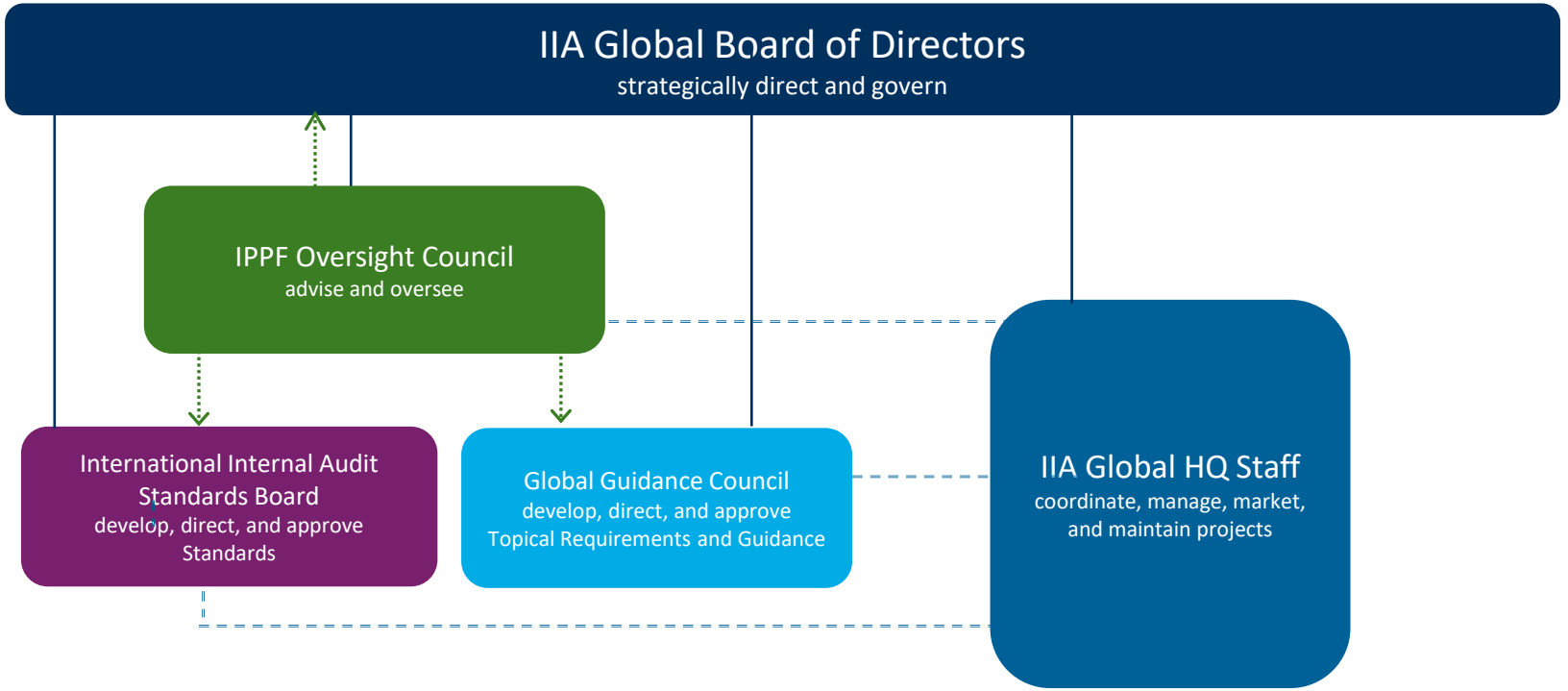
Topical Requirements

Standards

IIA Learning Programs

Global Certifications

IPPF Governance Process



Stakeholder Groups

provide knowledge, feedback, & input

- Affiliates and Chapters
- IIA Member Volunteers (Knowledge Groups)
- Direct Stakeholders (IIA members and other in the internal audit profession)
- Indirect Stakeholders (Public, non-IA Profession)

Polling Question

What is the biggest challenge when implementing Topical Requirements in your internal audit function?

1. Lack of resources and expertise in specialized areas.
2. Confusion about the applicability.
3. Resistance from stakeholders or management.
4. Keeping up with evolving risks.
5. None – the Topical Requirements support me as an internal auditor.

Topical Requirement Cybersecurity

International Professional Practices Framework®
(IPPF)

Polling Question

Is cybersecurity on your audit plan for this year?

1. Yes
2. No
3. Unsure

Definition of Cybersecurity

- **The National Institute of Standards and Technology (NIST)** defines cybersecurity simply as, **"The ability to protect or defend the use of cyberspace from cyberattacks."** Cybersecurity is a subset of overarching information security, which NIST defines as, **"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."**
- Cybersecurity reduces risk by **strengthening** the overall control environment and **protecting** an organization's information assets from unauthorized access, disruption, alteration, or destruction. Cyberattacks can lead to direct and indirect impacts that are often significant, as computers, networks, programs, data, and sensitive information are critical components of most organizations.

Specifics

Protecting:

- Digital data assets:
  - Customer and employee data.
  - Intellectual property.
  - Financial data.
  - Operational data.
- Digital systems and infrastructure:
  - Core IT systems.
  - Operational technology.
  - Network infrastructure.

Data security objectives:

- Confidentiality.
- Integrity.
- Availability.

Vulnerable areas:

- Employee and vendor accounts.
- Third-party integrations.

Cybersecurity

Risk exposure:

- Business impact.
- Threat likelihood and velocity.
- Regulatory and compliance risks.
- Interconnected systems and dependencies.

Prioritizing:

- Reliance of critical processes on digital systems.
- Data sensitivity.

Professional judgment:

- Worst-case scenario.
- Trends or increased exposure.
- Control effectiveness.

Governance

- Establish and periodically update a **cybersecurity strategy and objectives**; report progress and resource needs to the board.
- Maintain **policies and procedures** aligned with recognized frameworks (such as NIST, COBIT), reviewed at least annually.
- Define **roles and responsibilities** with clear reporting lines and periodic skills assessments.
- Engage relevant **stakeholders** (senior management, risk, HR, legal, vendors) to identify vulnerabilities and emerging threats.

Risk Management

- Integrate cybersecurity into **the organization's risk assessment and risk-management process** (identify, analyze, mitigate, monitor).
- Assign **accountability** and ensure cross-functional coordination.
- Define **escalation protocols** for risks exceeding tolerance levels.
- Maintain **risk communication and awareness** programs; include training and regular updates to management and board.
- Implement and test a **cyber incident-response and recovery plan** (detection, containment, restoration, post-event learning).

Controls

- Maintain strong **internal and vendor control environments**; review SOC reports and remediation actions.
- Build **competent talent** through training and technical upskilling.
- Continuously **monitor threats and vulnerabilities** and improve defenses.
- Embed cybersecurity in the **IT-asset life cycle** (selection → use → maintenance → retirement).
- Strengthen **technical safeguards**: configuration, patching, access management, encryption, DevSecOps integration.
- Implement robust **network and endpoint security controls** (firewalls, segmentation, ZTNA, IoT controls, multi-factor authentication).

Polling Question

I have discussed the Cybersecurity Topical Requirement with:

1. Board/audit committee.
2. Senior/executive management.
3. Both the board/audit committee and senior/executive management.
4. The internal audit team.
5. I have not discussed it with anyone yet.

Applying Topical Requirements

International Professional Practices Framework®
(IPPF)

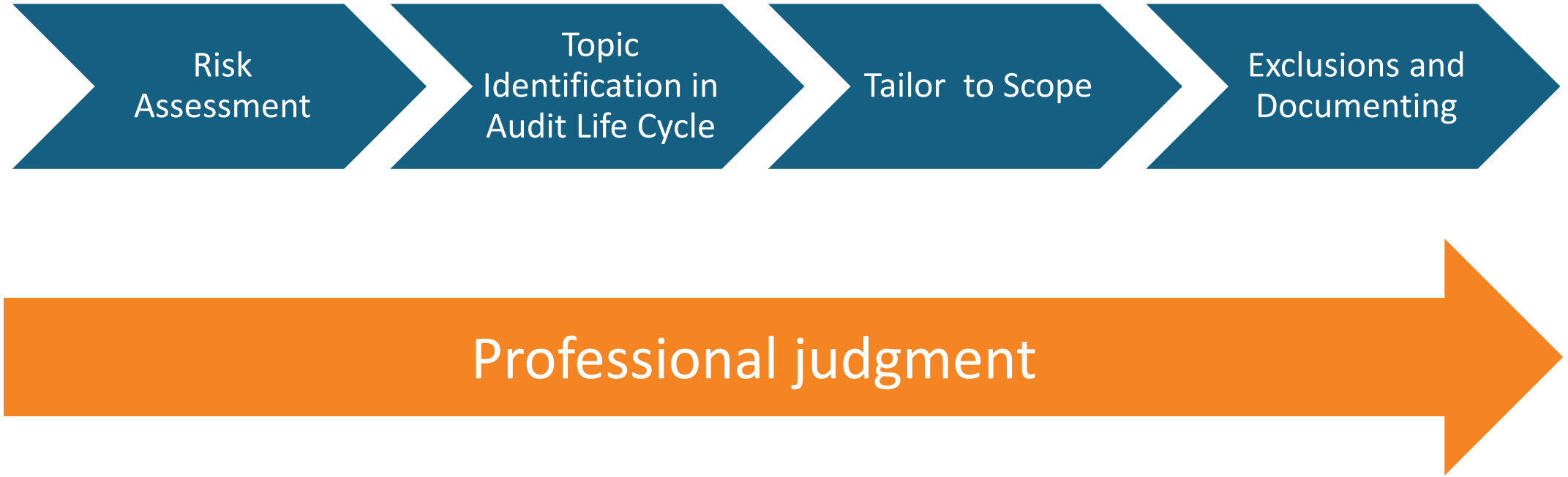
Application

Purpose: Ensure consistent, risk-based application of Topical Requirements (TRs) throughout the audit lifecycle.

Core principles:

- **Professional Judgment** – Adapt TRs to organizational context, risk profile, and audit objectives.
- **Risk-Based Approach** – Apply TRs when a topic exceeds the organization's defined significance threshold.
- **"Conform or Explain"** – If full conformance isn't feasible, document rationale and alternative actions.

Application Steps



Step 1 – Risk Assessment

Determine scope based on risk significance

Use the organization's **risk assessment results** and **risk appetite** to shape the depth of audit coverage. Apply the GIAS and common consulting practice:

Consideration	Application
Risk Likelihood and Impact (+ other criteria)	Significant risks (such as known vulnerabilities, prior incidents) suggest broader TR coverage.
Risk Appetite (Standard 9.3)	If risks exceed the organization's stated appetite, audit scope should expand accordingly.
Inherent vs. Residual Risk	In control focused areas (material decrease in residual risk compared to inherent risk).

GIAS Reference: Standard 13.2 Engagement Risk Assessment
Cyber TR User Guide: p. 2–3, p. 5–6 on linking scope to residual risks and mitigation needs.

Step 2 – Applying TRs in the Audit Lifecycle

Integration across stages:

- **Plan Level** – Include significant TR topics as identified and prioritized in audit plan; record in audit universe.
- **Engagement Level** – Include relevant TR requirements aligned to risk objectives.
- **Fieldwork** (not initially in scope) – Include relevant TR requirements only when aligned to (rescoped) audit objectives. Avoid scope creep.

Step 3 – Tailor to Scope

Stage	Tailoring to Scope
Plan Level	Apply TR-related risks (Standard 9.4) as: • **Standalone audits** dedicated to the topic. • **Integrated coverage** across multiple engagements. • **Phased approach** over several audit cycles or years. Always reference applicable TRs in the audit universe, risk assessment, and planning records to ensure transparency and alignment.
Engagement Level	Apply the relevant TR domains (Governance, Risk Management, Controls) related to the audit objectives.
Fieldwork	Adjust scope only when risk significance justifies and apply only relevant requirements.

Step 4 – Handling Exclusions, Maturity and Resources

Situations and Recommended Actions:

- **Partial Applicability** – Document rationale + link to risk rating and scope boundaries.
- **Low Maturity Area** – Use TR as framework in advisory mode; raise awareness to board.
- **Resource Constraints** – Inform board (Std 8.2); train, co/outsourcing or rescope with approval.
- **Nonconformance** – Apply “Conform or Explain”; keep evidence for QA reviews.

Regulatory Alignment and Multiple TRs

Regulatory Alignment:

- TRs set the minimum baseline; regulatory standards (NIST, ISO 27001, SOC, laws) may be stricter.
- Map TR requirements to existing frameworks to avoid duplication.
- Leverage external audit evidence with professional judgment and documentation.

Applying Multiple TRs:

- Third-party cyber services – Apply Cybersecurity + Third-Party TRs.
- Vendor contract compliance only – Apply Third-Party TR only.

Good Practices and Documentation Tools

Tools:

- TR Applicability Matrix (Appendix C User Guide).
- Risk Assessment Summary Template (link risk rating → TR scope).
- Mapping Table (TR ↔ Regulation/Framework ↔ Evidence Source.

Good Practices:

- Use clear logic for inclusions/exclusions.
- Align scope with risk severity and audit objectives.
- Maintain traceability for QA and EQA reviews.
- Leverage TRs to promote risk-aware governance and consistency across functions.

QA View on TR Application

Level	What Assessors Review	Evidence Expected
Audit Plan Level	• Identification of TR-relevant topics in the risk-based plan. • Documented applicability assessment. • Integration of TR coverage across the audit universe.	• Audit plan and risk assessment files. • TR applicability matrix or summary table.
Engagement Level	• Evidence that TRs were applied in scope definition and testing. • Justification for any exclusions. • Conformance with Domain V – Performance of Internal Audit Services.	• Engagement workpapers and reports. • Documented rationale for exclusions. • Evidence of testing and conclusions.

Appendix C – Optional Documentation Tool

Cybersecurity – Governance

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
A. A formal cybersecurity strategy and objectives are established and periodically updated. Updates on the achievement of cybersecurity objectives are periodically communicated and reviewed by the board, including resources and budgetary considerations to support the cybersecurity strategy.		
B. Policies and procedures related to cybersecurity are established, periodically updated, and strengthen the control environment.		
C. Roles and responsibilities that support cybersecurity objectives are established, and a process exists to periodically assess the knowledge, skills, and abilities of those filling the roles.		

Workshop Exercise

International Professional Practices Framework®
(IPPF)

The Institute of Internal Auditors®

Scenario 1: Health Care Provider – Regional Hospital Group

Organization Overview:

- **Name: MedLink Health Network**
- **Size:** 3 regional hospitals, 12 outpatient clinics, 1,500 employees
- **Digital Assets:** Electronic Health Record (EHR) system (cloud-based), patient mobile app, connected medical devices (IoT)
- **Budget:** $300 million annually
- **IT Team:** 6 full-time staff; no CISO
- **Audit History:** Last cyber audit was 4 years ago; no ransomware incidents reported, but phishing attempts rising

Scenario 1: Health Care Provider – Regional Hospital Group

Risk assessment of a Cyberattack *

- **Unauthorized Access to Patient Data - High**
  - Risk: Unauthorized individuals could access Electronic Health Records (EHR).
  - Potential Impact: Critical - HIPAA violations, patient privacy breaches, reputational damage, and regulatory penalties.
- **Inadequate Network Segmentation Across Medical Devices - High**
  - Risk: Medical IoT devices (such as infusion pumps, imaging systems) are connected to the hospital network with minimal isolation, creating lateral movement paths for malware.
  - Potential Impact: High - Compromised patient care systems, operational disruptions, and safety risks to patients.
- **Dependence on IT Infrastructure for Critical Services - High**
  - Risk: A cybersecurity incident (e.g., ransomware or targeted attack) could compromise the availability of essential IT systems such as EHR or diagnostic platforms.
  - Potential Impact: High - Delays in care delivery, patient safety risks, prolonged outages, and financial/reputational damage.

* *Risk of a cyberattack can be defined as moderate.*

Discussion Questions

- **Provide for an audit plan or engagement plan addressing the specific risks from the risk assessment (*)**
  - Define approach and type of audit
  - Provide for scoping
  - Assess the Cybersecurity applicability
  - Document potential exclusions

- **Additional discussion questions**
  - How to address insufficient resourcing to address the identified risks?
  - What in case the maintenance of certain applications are outsourced to an IT vendor? How would you deal with the applicability of the Cybersecurity and Third-Party Topical Requirements?
  - The organization has performed a COBIT audit “Audit of IT Governance, Strategic Alignment, and Risk Management” with controls APO01, APO02 and EDM03. What is your approach?

** Make additional assumptions in the scenario if necessary.*

Scenario 2: Food Manufacturer

Organization Overview:

- **Name: VitalGrain Foods Inc.**
- **Sector:** Packaged grain and meal products (non-perishable food)
- **Scale:** 2 plants, 600 employees, mostly regional distribution
- **Systems:** ERP (on-prem), basic OT integration, low customer data dependency
- **Risk Profile:** No sensitive data; minor operational downtime impact
- **Recent Activity:** IT Governance audit 9 months ago

Scenario 2: Food Manufacturer

- **Unauthorized Access to Operational Systems**
  - Risk: Unauthorized individuals could potentially access shared production workstation credentials or the basic ERP system.
  - Potential Impact: Moderate - limited sensitive data at stake; limited disruption as most production records are maintained manually.
- **Dependence on Networked Systems in Production Processes**
  - Risk: Manual production lines operate largely independently from IT systems, limiting exposure to malware propagation or lateral movement.
  - Potential Impact: Moderate - operational inefficiencies; fallback to paper-based processes ensures continuity.
- **Downtime Due to Cyber Attack**
  - Risk: A cybersecurity incident (such as ransomware) could affect the availability of the ERP used for billing and stock records.
  - Potential Impact: Minimal - Temporary delays in invoicing and inventory updates; low business impact due to short recovery time from offsite backups.

* *Risk of a cyberattack can be defined as moderate.*

Discussion Questions

- **Provide for an audit plan or engagement plan addressing the specific risks from the risk assessment (*)**
  - Define approach and type of audit
  - Provide for scoping
  - Assess the Cybersecurity applicability
  - Document potential exclusions

- **Additional discussion questions**
  - How to address insufficient resourcing to address the identified risks?
  - What in case the maintenance of certain applications are outsourced to an IT vendor? How would you deal with the applicability of the Cybersecurity and Third-Party Topical Requirements?

** Make additional assumptions in the scenario if necessary.*

What’s next?

International Professional Practices Framework®
(IPPF)

Topical Requirements: Plans and Next Steps

Topics Approved by the Global Guidance Council

- Cybersecurity
- Third-Party
- Organizational Behavior
- Organizational Resilience
- Anti-Bribery and Corruption
- People Management

Next Steps

Cybersecurity: Effective 2026 Feb

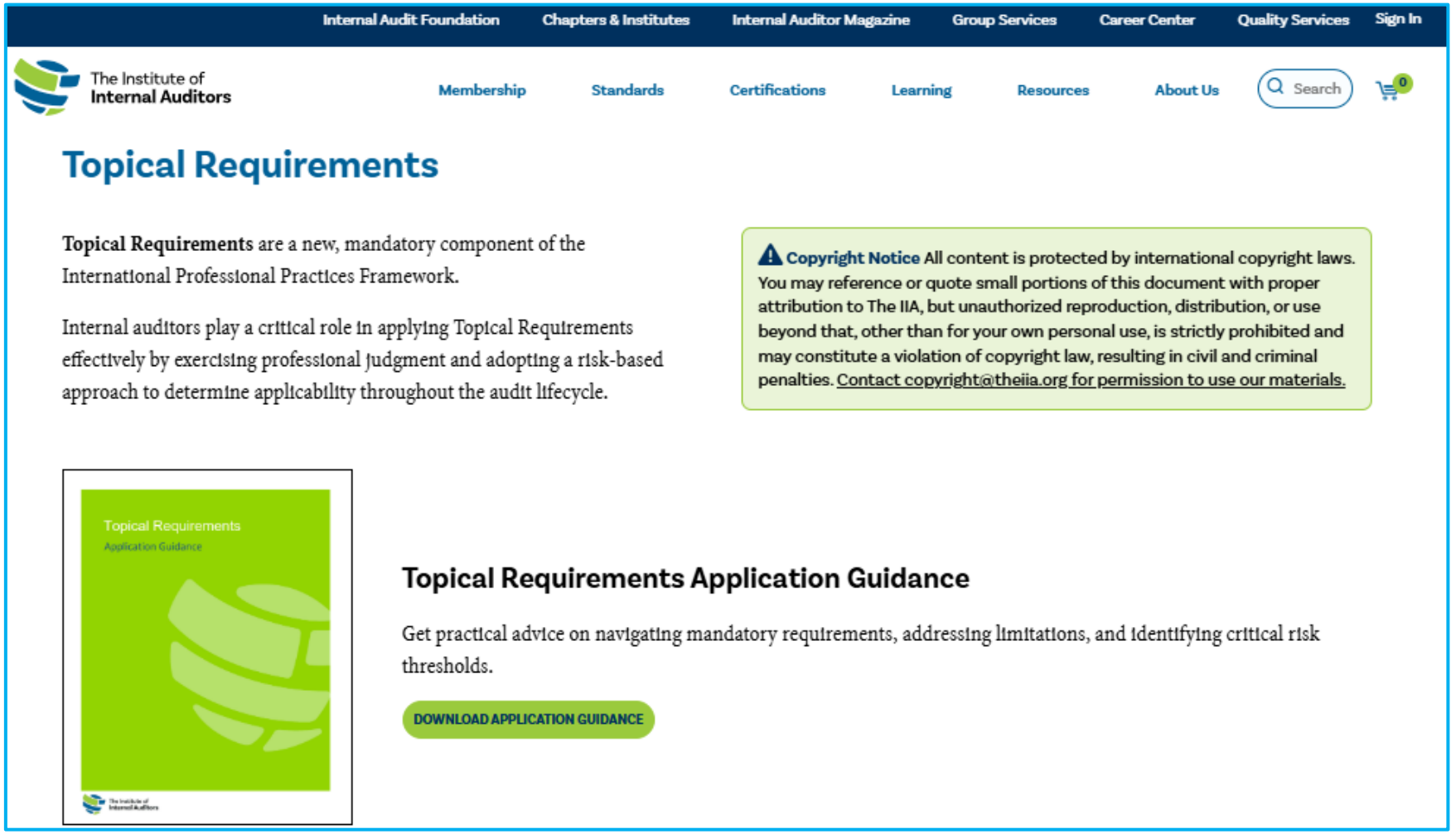
Third-Party: Effective 2026 Sept

Organizational Resilience: Public Consultation closes 17 Nov

Organizational Behavior: Publishing 4Q2025

Organizational Resilience: Publishing 2026

www.theiia.org/TopicalRequirements



Q&A

International Professional Practices Framework®
(IPPF)

Key Session Takeaways

What are the key takeaways you received from this session?

International Professional Practices Framework®
(IPPF)

The Institute of Internal Auditors

Copyright Notice