Topical Requirements

Topical Requirements: Routines That Raise the Bar

February 24, 2026

Welcome

Audit Routines

Turning Expectations into Repeatable Practice

Our Operating Manual

Topical Requirements and User Guides

Our Virtues

Widom. Discipline. Courage. Justice.

Agenda

- What Topical Requirements are. What is included?
- Dates and Triggers
- Deep Dives: Cybersecurity, Third-Party Risk, and Organizational Behaviour
- How Topical Requirements will be assessed (QAIP & EQAs)
- Leveraging our Past: Implementation
- Questions

Hands up!

Question

Have you read the topical requirements?

1. Yes (Hands up)
2. No (Hands down)

Why Topical Requirements Matter

Mandatory, Globally Consistent Minimum Baselines

Consistency and Quality

Improves the reliability, comparability, and quality.

1

2

Mandatory for Assurance Engagements

Applied whenever a relevant risk topic is identified in the audit plan, during an engagement, or via a stakeholder request.

Risk-Based and Professional Judgement

Document why requirements are included or excluded

3

4

Elevates the Profession

Formalizing expectations for how to audit complex topics.

Regulatory Alignment

Designed to work alongside external frameworks.

5

6

Resource and Scope Management

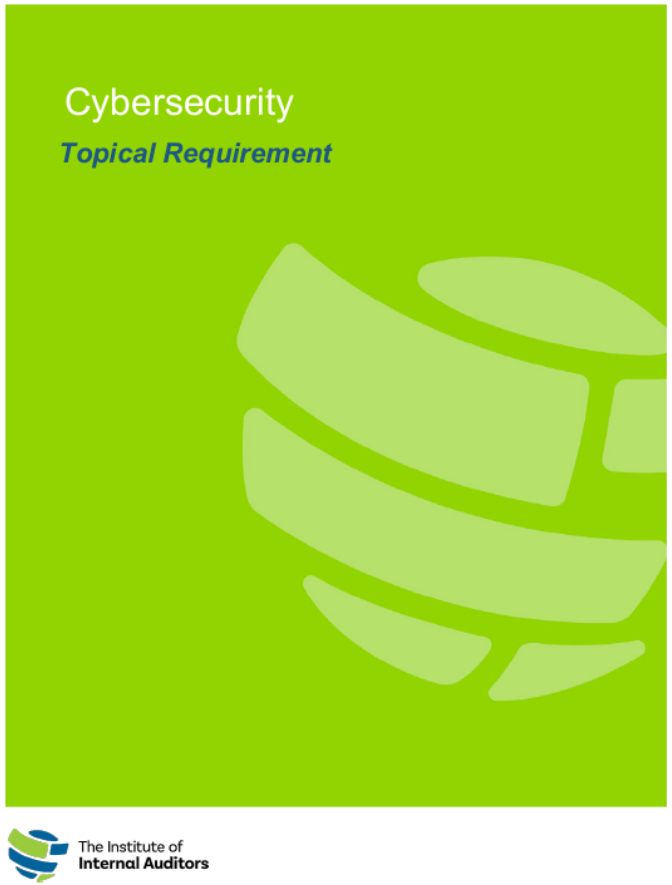
Keeps audit coverage risk-aligned and stakeholders informed.

Reading

Let’s get wiser together

What is included?

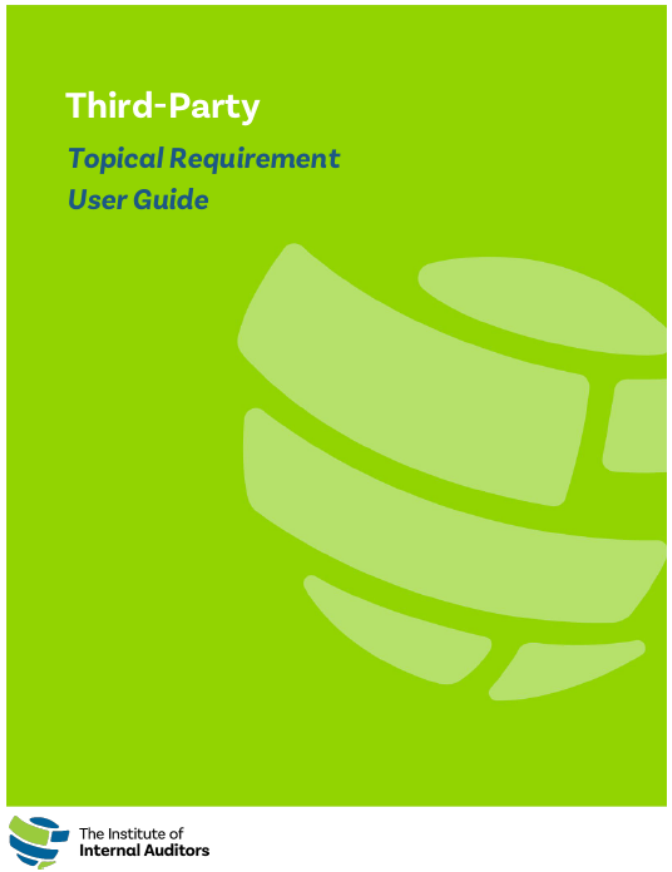
Topical Requirement - Contents



- Applicability Rules
- List of Mandatory Requirements
- Organized by Governance, Risk Management and Controls
- Lists out minimum requirements
- Established documentation expectations
- Conformance will be explicitly tested during QAIP and EQAs

What is included?

User Guide - Contents



- Rationale and importance
- Detailed considerations and examples
- Practica application scenarios
- Mapping to frameworks
- Optional documentation tools
- Evidence of reasonable application for quality reviews
- Case studies & FAQs

Tropical Requirements

Current and Upcoming Requirements

Cybersecurity

Effective February 5, 2026, mandatory cyber risk coverage includes controls and incident response protocols.

Third-Party Risk Management

Starts September 15, 2026, focusing on vendor risk frameworks, contract reviews, and continuous monitoring.

Organizational Behaviour and Resilience

Effective December 15, 2026 will focus on culture, leadership, and adaptability for organizational success and risk mitigation.

Hands up!

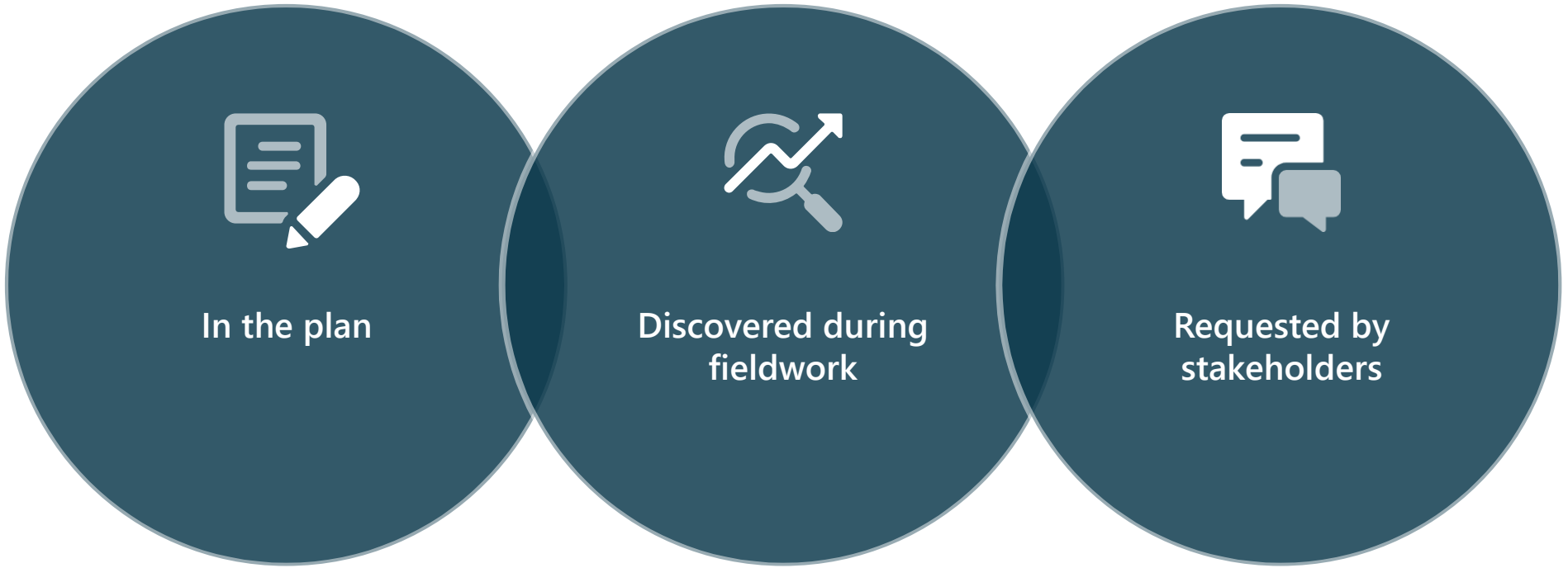
Question

Which area is least covered in your 2026 plan?

1. Cybersecurity
2. Third-Party Risk Management
3. Organizational Behaviour and Resilience

Three Triggers

When the apply



Cybersecurity

Cybersecurity

About

Definition

The ability to protect or defend the use of cyberspace from cyberattacks.

Cybersecurity

Example: How the Topical Requirements Would Have Helped

Cybersecurity: What's in scope

Balance governance, risk, and controls

Governance

1. Formal cybersecurity strategy and objectives
2. Policies and procedures
3. Roles and responsibilities
4. Stakeholder engagement

Risk Management

1. Risk assessment and management
2. Enterprise-wide coverage
3. Accountability
4. Escalation process:
5. Risk awareness and remediation
6. Incident response and recovery

Controls

1. Internal and vendor controls
2. Talent management
3. Continuous monitoring
4. IT asset lifecycle
5. Technical controls
6. Network controls
7. Endpoint security

User Guide

Examples

Governance Considerations

To assess how the governance processes are applied to cybersecurity objectives, internal auditors may review:

A. Formalized, documented cybersecurity strategic plan and objectives, including evidence that the board periodically (generally quarterly) reviews the cybersecurity updates provided by the head of the information security function, such as the chief information security officer (CISO). Evidence may include reporting on:
   - Monitoring the achievement of strategic objectives.
   - Budgetary needs to support cybersecurity goals and objectives.
   - Focus on risks and internal controls, including remediation progress.
   - Key performance indicators (KPIs) to measure success.
   - Human resources needed to hire, train, and develop cybersecurity personnel.

User Guide

Examples

Governance Requirements	Framework References		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
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.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Policies and procedures related to cybersecurity are established, periodically updated, and strengthen the control environment.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11

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.		

Hands up!

Question

In your last audit, did you document exclusions and rational for requirements not in scope?

1. Yes (Hands up)
2. No (Hands down)

Third-Party Risk Management

Third-Party Risk Management

About

Definition

A third party is an external individual, group, or entity with whom an organization (“the primary organization”) establishes a business relationship to obtain products or services.

The relationship may be formalized through a contract, agreement, or other means to provide the organization with products, services, labor, manufacturing, or information technology solutions, such as data storage, processing, and maintenance.

Third-Party Risk Management: What's in scope

Balance governance, risk, and controls

Governance

1. Formal strategy and approach
2. Policies and procedures
3. Roles and responsibilities
4. Stakeholder engagement

Risk Management

1. Comprehensive risk management processes
2. Regular risk assessment
3. Risk responses
4. Escalation and accountability

Controls

1. Due diligence
2. Contracting and approval
3. Contract management
4. Onboarding
5. Ongoing monitoring
6. Corrective action protocols
7. Renewal and expiration
8. Offboarding

Third-Party Risk Management

Lifecycle

Selecting Contracting Onboarding Monitoring Offboarding

Third-Party Risk Management

Example: How the Topical Requirements Would Have Helped

Third-Party Risk Management

Risk Areas

- Strategic risk
- Reputational risk
- Ethical risk
- Operational risk
- Financial risk
- Compliance risk (local, national, international regulations)
- Cybersecurity and data protection risk
- Information technology risk
- Legal risk
- Sustainability risk (environmental, social, governance)
- Geopolitical risk

Organizational Behaviour and Resilience

Role of internal auditing in organizational behavior

Culture is often seen as a vague topic. Listen to behavioral experts explain how reframing culture as organizational behavior makes it a concrete, risk-based subject that can be assessed using the Organizational Behavior Topical Requirement.

Organizational Behaviour and Resilience

Example: How the Topical Requirements Would Have Helped

Organizational Behaviour and Resilience

About

Definition

Organizational behavior is the observable choices employees make in doing their jobs and how they work with others. This behavior influences performance and the achievement of organizational objectives. Simply put, organizational behavior is "the way we do things" and is considered a subset of culture.

Organizational Behaviour and Resilience: What's in scope

Balance governance, risk, and controls

Governance

1. Roles and responsibilities
2. Accountability for behavioral expectations
3. Monitoring and evaluation of behavioral alignment
4. Policies and procedures for behavioral risk

Risk Management

1. Approach to managing behavioral risks
2. Monitoring of organizational behavior
3. Communication of gaps and root causes
4. Resolution of gaps with stakeholder input

Controls

1. Identifying and mitigating risky behavioral patterns
2. Tone and communication of expected behaviors
3. Reporting mechanisms for behavioral issues
4. Incentive and disincentive programs
5. Issue management and escalation
6. Training and awareness programs
7. Talent acquisition and onboarding

Leveraging our Past: Implementation

How Topical Requirements will be assessed

January 28, 2026 — A Deep Dive on Application and Current Releases

How we will be assessed

- QAIP
- EQA

Professional judgment is expected.
Documented judgment is required.

What reviewers may look for:

- Applicability decision is visible
- Exclusions are documented and justified
- Traceable evidence (scope → work performed → conclusions)
- Risk-based proportionality (depth matches risk and objectives)

Closing

- **Gaps:** Map coverage. Document exclusions.
- **Roadmap:** Sequence work, rotate and consider resourcing
- **Skills:** Upskill cyber, third-party, and behavior
- **Artifacts:** Record applicability, evidence, and exclusions
- **Governance:** Align charter, board, and resources
- **Discipline**: Routines, sprints, and small wins

Thank You!

Paul Groch, CPA, CA, CIA
Partner, Internal Audit

E: paul.groch@mnp.ca

LinkedIn: linkedin.com/in/paulgroch


MNP
MNP
MNP
Wherever business takes you
MNP.ca
PRAXITY
A member of the Praxity Global Alliance