Comments IIA NL on Proposed Topical Requirement Cybersecurity

Comment Type

Are you commenting as an individual or as a representative of a larger group?

- (●) As an individual
- ( ) On behalf of my internal audit function
- ( ) As an official representative of a stakeholder (regulators/government, shareholders/investors, customers, third parties)

X

Key Concepts Related to Topical Requirements

Please indicate your level of agreement with the clarity of key concepts related to Topical Requirements.

	Strongly agree	Agree	Neutral (neither agree nor disagree)	Disagree	Strongly disagree
The information provided in the Introduction section of the Cybersecurity Topical Requirement clearly conveys the purpose of a Topical Requirement.		X			
It is clear that a Topical Requirement is a mandatory component of the International Professional Practices Framework.		X			
It is clear when a Topical Requirement must be applied.		X			
When an element within a Topical Requirement is not relevant to the engagement, it is clear that documentation is required to explain the decision to exclude that element of the Topical Requirement from the engagement.		X			

Do you have any additional comments regarding key concepts related to Topical Requirements, particularly in areas of disagreement (optional)?

No additional comments

Instituut van Internal Auditors Nederland

Comments IIA NL on Proposed Topical Requirement Cybersecurity

Structure of Topical Requirements

Please indicate your level of agreement regarding the structure and format of a Topical Requirement, based on your review of the Cybersecurity Topical Requirement.

	Strongly agree	Agree	Neutral (neither agree nor disagree)	Disagree	Strongly disagree
The length of the document is appropriate.					X
The number of requirements is appropriate.					X
It is clear that each consideration matches an individual requirement.		X			
It is helpful to have requirements grouped by governance, risk management and internal controls.					X
It is best to list the applicable Standards at the end of the document (rather than listing the applicable Standards throughout the document).					X
It is helpful to have the Requirements Conformance Tool as an appendix.			X		

Additional comments

- The TR lacks a clear structure, failing to start with audit objectives or provide concrete areas to be audited.
- The requirements should begin with a proper definition of cybersecurity, which the TR currently lacks.
- While the included requirements are relevant, they are too high-level and lack specific cybersecurity measures such as network security, information security, application security, operational security, disaster recovery and business continuity security, endpoint security, and Identity and Access Management (IAM). IAM is only briefly mentioned under policy considerations for risk management.
  Additionally, the TR does not explicitly cover user education, identification and monitoring of cyber incidents (e.g., Security Log Management, SIEM, SOC), vulnerability scanning, software patching (currently only mentioned for hardware), hardware hardening/baseline, business continuity, and regular penetration testing (which should be defined not only during development but also in production). It also fails to address various types of cyber threats like malware, phishing, ransomware, and social engineering. For organizations with proper risk management practices, cybersecurity controls should stem from risk management, making the controls in this TR unnecessary.
- The requirements are structured under "governance, risk management, and controls" with underlying generic requirements that seem to overlap. However, they are written in a way that does not support easy reading and understanding. Policies and procedures are mentioned in all sections - governance, risk management, and controls - but they do not need to be included in every section.
- The current TR setup focuses on assessing compliance with policies, procedures, and frameworks. While compliance is important, it should not be the sole focus of a cybersecurity audit. It is essential to also consider the effectiveness and efficiency of controls in mitigating risks and protecting critical assets, tailored to the organization's typology, risk appetite, and security budget.
- The way this TR is published does not allow organizations the flexibility to address and audit cybersecurity in a manner most appropriate for their specific needs.
  The TR seems to imply that the full TR must be applied to every cybersecurity-related audit. Many organizations however conduct several cybersecurity audits at different times and frequencies based on a risk-based approach. This practice appears to be unsupported or even prohibited under the current TR setup.
- The list of Standards is useless as all standards are related to each risk; just mentioning them doesn't add any value.

Comments IIA NL on Proposed Topical Requirement Cybersecurity

Cybersecurity Topical Requirement

Please indicate your level of agreement regarding the relevance and applicability of the Cybersecurity Topical Requirement.

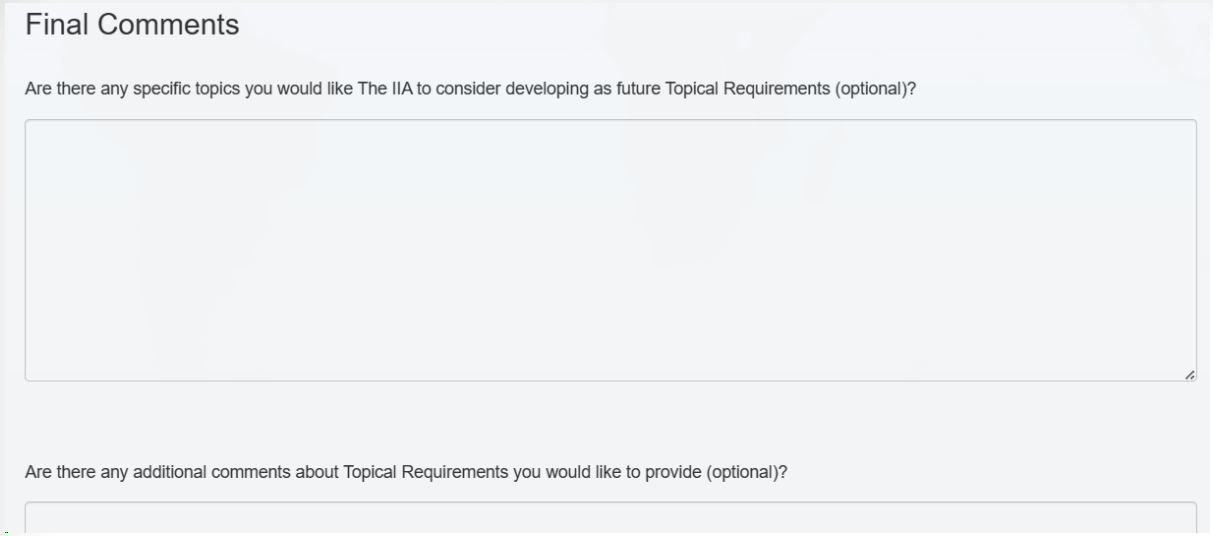
	Strongly agree	Agree	Neutral (neither agree nor disagree)	Disagree	Strongly disagree
The Cybersecurity Topical Requirement aligns with the Purpose of Topical Requirements, which is to enhance consistency and quality of internal audit services; strengthen the ongoing relevance to the evolving risk landscape; and raise professionalism and performance of internal auditors.					X
A practitioner would find the Cybersecurity Topical Requirement valuable when preparing for a cybersecurity engagement.					X
This Topical Requirement is easy to implement regardless of an internal audit function's size or sector.			X		

Please indicate whether the Cybersecurity Topical Requirement provides the right amount of detail for the following elements:

	Not enough detail	The right amount of detail	Too much detail
Mandatory requirements			X
Nonmandatory considerations	X		

Additional comments

- Its added value is unclear, especially given the availability of ready-to-use assurance programs from sources like ISACA, ISO and NIST.
- Consistency of auditing Cybersecurity between different organizations can be conflicting with the desired risk-based approach, by which audits are tailored to the specific situation and needs of the organization.
    - Organizations differ in size, complexity, and industry, necessitating varied approaches to cybersecurity governance, risk management, and control processes. Introducing flexibility or tailoring options within the requirements could better accommodate these differences.
- Considering the previous question: this TR will not inherently enhance the quality of cybersecurity assurance engagements. The requirements are quite generic, supporting an approach rather than providing depth. Quality will still rely on well-known reference models, not on this TR.
    - The requirements are generic and broadly applicable beyond cybersecurity risk, resembling a general risk management approach. However, they lack depth and remain general in IT security, often applicable to traditional environments. The term "cybersecurity" could be replaced with any other type of security without losing relevance. When reading the TR, the requirements remain generic and lack concreteness.
    - Specific examples or case studies demonstrating the application of topical requirements in ambiguous areas are missing. Although the requirements reference widely adopted frameworks, explicitly aligning them with specific industry standards or best practices could be beneficial.
    - Topical requirement considerations would benefit from specific metrics or measurement criteria that organizations can use to assess the effectiveness of their cybersecurity governance, risk management, and control processes. Some requirements could be more specific, providing clearer guidance on expected outcomes or actions (e.g., requirement D under the risk management section), which would help better understand and meet the requirements.
- Additionally, the TR (the tool in Appendix B) requires additional administration without any value for the organization and its IAF.
  Every audit is based on a risk analysis that shows what is and is not in the scope of the audit. That should be sufficient to then apply parts of the TR in accordance with the risk assessment.



Comments IIA NL on Proposed Topical Requirement Cybersecurity

Final comments

- We would like the IIA to reconsider the mandatory character
  We disagree with mandatory character, because 1) the quality of execution of all types of audits is already assured in GIAS; 2) it entails (unnecessary) work in documenting the application/non-application; 3) the requirements are so general in nature that they provide insight into the 'what', but are less helpful than specific models in this area.
- However, we recognize that changing the mandatory character would be a major shift - the mandatory character has already been incorporated in all publications. So when keeping the mandatory it is strongly recommended that the (each) TR be accompanied by an explanation in which a comparison is made between the TR and the most commonly used reference models in the relevant field (here e.g. NIST Cybersecurity Framework, ISO2700X, …)
  This would also mean that if such a framework is used, sufficient conformance is immediately demonstrated (and the tool in the appendix therefore does not have to be completed (per requirement))