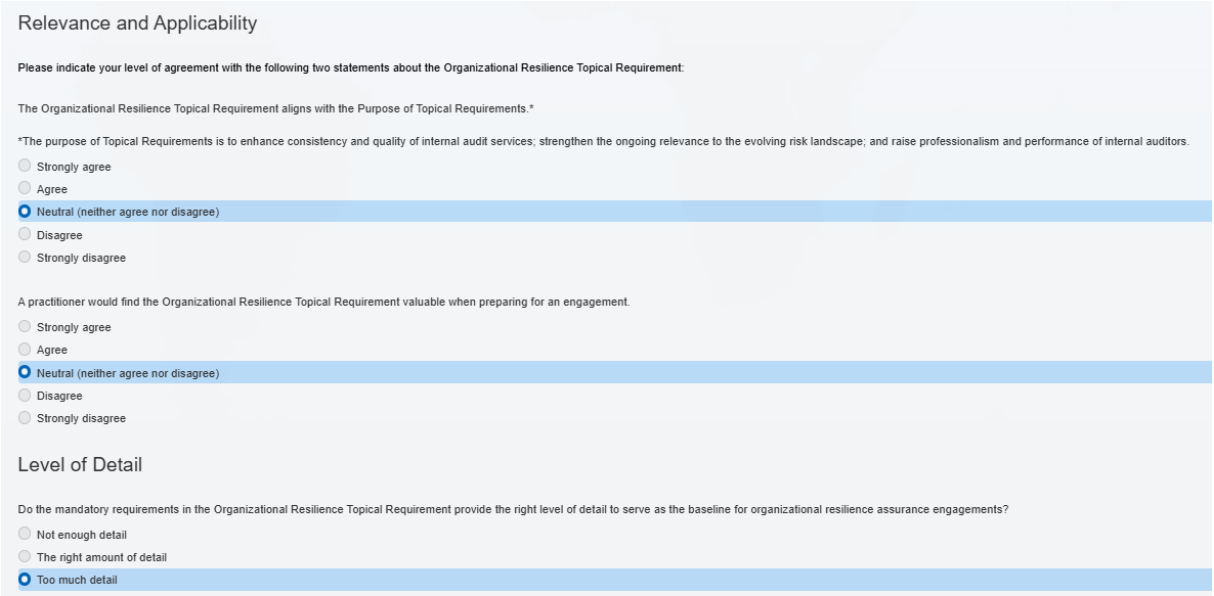
Reactie IIA Nederland op
Topical Requirement Organizational Resilience

IIA heeft een concept versie van de Topical Requirement Organizational Resilience ter consultatie aangeboden: https://www.theiia.org/en/standards/2024-standards/topical-requirements/public-comment-period/

Hierop kan tot 17 november 2025 worden gereageerd.

IIA Nederland heeft haar reactie opgesteld met behulp van een aantal experts op dit gebied. Hieronder staat de reactie die via de daartoe bestemde survey is ingediend.



Relevance and Applicability

Please indicate your level of agreement with the following two statements about the Organizational Resilience Topical Requirement:

The Organizational Resilience Topical Requirement aligns with the Purpose of Topical Requirements.*

*The purpose of Topical Requirements 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.

- Strongly agree
- Agree
- Neutral (neither agree nor disagree)
- Disagree
- Strongly disagree

A practitioner would find the Organizational Resilience Topical Requirement valuable when preparing for an engagement.

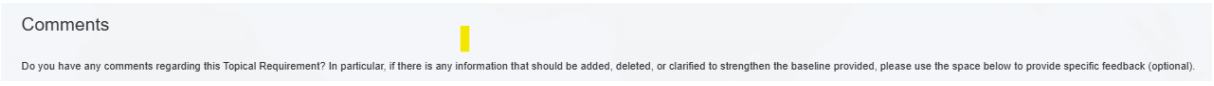
- Strongly agree
- Agree
- Neutral (neither agree nor disagree)
- Disagree
- Strongly disagree

Level of Detail

Do the mandatory requirements in the Organizational Resilience Topical Requirement provide the right level of detail to serve as the baseline for organizational resilience assurance engagements?

- Not enough detail
- The right amount of detail
- Too much detail

Relevance and Applicability	(alleen score; geen toelichting mogelijk)
Purpose	Neutral *- redelijk in lijn met onze eerdere reacties, als IIA NL hadden we het liever als guidance gezien en betwijfelen de toegevoegde waarde*
Valuable	Neutral *- vraag is wat deze TR toevoegt aan de ISO 22300 series*
Detail	Too much detail *- de requirements bevatten veel toelichtingen, die passender in de toelichting zouden zijn*



Comments

Do you have any comments regarding this Topical Requirement? In particular, if there is any information that should be added, deleted, or clarified to strengthen the baseline provided, please use the space below to provide specific feedback (optional).

Governance	• Leadership, culture and psychological safety are lacking. These elements are clearly addressed in the ISO standard. Resilience involves not only plans and processes, but also behavior, collaboration, and learning capacity. Advice add this as G. (F -stakeholder engagement is purely process-oriented and not behavioral). Resilience culture: speaking up, signal detection, and encouraging learning under stress • It is all about processes. The link with roles and responsibilities is missing here – these are mentioned in Risk Management, but are part of governance. • GOV-C: should be **all** processes (not just the 3 mentioned) + not only processes, but also roles should be defined. • GOV-E: 'availability' of the resources should be added

Risk Management	• Requirements B and D are are further elaborations/details of A, so A isn't necessary to include
	• What's the difference between the strategies in GOV- and RM-A? Seems to be redundant.
	• In crisis situations, the emphasis is on speed and decisiveness. These aspects may be emphasized more.
	• The link between specific threats or scenarios and the training, exercises and education of personnel is not yet sufficiently explicit.
	• Examples of more short and powerful description
	  ○ RM-C: An individual or team is identified to periodically monitor and report how organizational resilience risks are being managed AND ITS EFFECTIVENESS
	  ○ RM-D: A process is established to monitor organizational resilience risk levels AND ITS IMPACTS and quickly escalate those that reach a level considered unacceptable
	  ○ RM-E: delete the examples in the requirement itself: ~~The incident response approach includes scenario analyses and periodic stress testing against a range of plausible disruptive events~~

Controls	• Too much operational details; many details in the requirements are not always necessary (sometimes even called 'may'- which should be in the considerations/guide/guidance)
	The TR delves deeply into IT continuity, which might better fit in BCM guidance. F.e. "critical IT assets are inventoried. They include hardware, software, etc." > advice: bundle into one generic control; move operational details to guidance.
	• In detail per requirement (including examples of too much detail) :
	  ○ C-A: add 'manage' → Processess are established to identify AND MANAGE critical …
	  Delete 'The process includes maintaining a list of alternative suppliers' – that's just one of the things and should be in guidance instead the requirement itself

	○ C-B: as in C-A: not only 'identified' but also 'protected and managed' ○ C-D: should be about more than just IT-assets, but all assets: IT, buildings, machines, workplaces, .. ○ C-F seems to be part of C-E ○ C-J seems to be included in C-I and too much details in it: ~~'the analysis should include ...'~~
Other	• Define organizational resilience (OR) as an umbrella framework above Cybersecurity (CYB) and Third-Party Risk (TPR). Prevents duplication and clarifies roles and responsibilities. • The TR has too much focus on the process instead of the outcomes. It mainly describes that processes must be in place, but hardly describes what results they must deliver for true resilience. f the content of the processes and (resulting) documents isn't good (e.g., too limited exercises or too superficial TRPM), you're not resilient. Advice: From: "a process is established to..." to " the organization consistently demonstrates the ability to..." • Reactive word choice predominates: resilience is often linked to "return to normal" and "recovery" instead of adapting, transforming, and looking ahead (f.e. a process to respond to and recover from crises > advice: more anticipation, adapt, transform. • Advice: map this Topical Requirements with broadly used related external frameworks (ISO (multiple) , NIS2, , ….). And explicitly state that there may be overlap with other TRs, such as Cybersec and TPM. F.e. a strategy is required in all of them, while there may be a single overarching strategy. Both will enhance efficient application of the TRs.