The Institute of Internal Auditors
Elevating Impact

Cybersecurity Topical Requirement Webinar

The IIA global webinar "Elevating Performance and Adding Value: Get to Know the New Cybersecurity Topical Requirement" was held on 6 February 2025 to accompany the launch of the first Topical Requirement. Questions not answered due to time constraints touched on a variety of topics:

Q: Are the Topical Requirements only applicable to cybersecurity engagements? Or do they apply to any engagements that have a cybersecurity component?

> **A**: The requirements apply to cybersecurity engagements and engagements that have a cybersecurity component. Topical Requirements are applicable when the topic is one of the following:
>
> - The subject of an assurance engagement in the internal audit plan.
> - Identified while performing an engagement.
> - The subject of an engagement request not on the original internal audit plan.
>
> Not all individual requirements may apply in every assurance engagement. The risk assessment will help determine which requirements to include in the internal audit plan and individual engagements. Thus, the applicable requirements may be limited to those addressing certain processes, controls, or other relevant aspects of the topic.

Q: If we are performing a cybersecurity audit that does not touch on governance, do we need to explain why those requirements are not covered in the engagement?

> **A**: Yes. Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented. Not all individual requirements may apply in every assurance engagement; if requirements are excluded, justification must be documented and retained.

Q: If we conduct an audit of a topic covered by a Topical Requirement and do not assess its applicability, will it imply nonconformance with the Standards?

> **A**: When a risk assessment identifies that the topic of a Topical Requirement will be included in an engagement or the internal audit plan, internal auditors must assess the requirements. If certain requirements are not within the scope of work, then justification must be provided. The justification will be reviewed as part of the quality assessment. Disregarding the requirements completely or not providing justification for excluded requirements or sections is a gap and may contribute to an assessment of nonconformance with the Standards.

Q: What documentation will quality assessors expect as demonstration of conformance?

> **A:** The Quality Assessment Manual's methodology indicates how to verify conformance with Topical Requirements in the testing of Standards 13.2 Engagement Risk Assessment and 13.3 Engagement Objectives and Scope using the D5 and D6 templates.

Q: Are the Topical Requirements and user guides free to download? Where can we find them?

> **A**: The Cybersecurity Topical Requirement and its user guide are available for free in 20 languages at www.theiia.org/TopicalRequirements. Other Topical Requirements and user guides also will be available for free as they are issued.

Q: Can we already start adopting these requirements in our audit engagements or do we have to wait for the effective date in February 2026?

> **A:** The IIA recommends adopting the Topical Requirements as soon as possible after they are issued because they will help internal auditors provide assurance over pervasive risks. Topical Requirements become effective 12 months after they are issued, meaning the internal audit function has 12 months to begin applying them before they are reviewed as part of quality assessments**.**

Q: Is the Cybersecurity Topical Requirement mapped to frameworks like NIST, COBIT, and ISO?

> **A**: Yes. Appendix B in the user guide maps the Cybersecurity Topical Requirement to three commonly used frameworks: NIST Cybersecurity Framework 2.0, COBIT 2019, and NIST 800-53. These frameworks were chosen because they are readily available at no cost.
>
> The IIA recognizes that organizations may have their own cybersecurity efforts, using these or other risk management and governance frameworks. Internal auditors may have already developed audit programs and testing procedures based on these frameworks. Internal auditors should reconcile their current cybersecurity assurance activities to the Topical Requirement to ensure adequate coverage.

Q: Will Topical Requirements be updated periodically?

> **A:** Yes. The Global Guidance Council has committed to reviewing and updating Topical Requirements on a regular basis as part of its due diligence.

Q: The Topical Requirement document is currently not available in my local language. How can I volunteer to help translate?

A: The IIA has created an online system for practitioners to volunteer their time for a variety of projects, including translations. Please visit our website to submit your volunteer application.

Q: Will Topical Requirements be part of the body of knowledge required for the CIA certification exams?

A: In accordance with our current policy, scored exam questions on new Topical Requirements will not appear on the CIA exam until at least 6 months after the effective date. The Cybersecurity Topical Requirement effective date is 5 February 2026. Please check CIA Updates/General FAQs frequently for additional information.