Chief Audit Executive Roundtable
IIA Chicago

The Institute of Internal Auditors
Chicago

April 24, 2025

Agenda

8:30-8:45	Arrival; Welcome and briefing from Metra
8:45-9:30	IIA Cybersecurity Topical Requirement – practical application of new requirements
9:30-10:00	Networking break
10:00-10:45	Risk Assessment in Disruptive Times – mechanisms for response in a time of rapid change and uncertainty
10:45-11:00	Update on CAE Feedback/CAE Feedback

The Institute of
Internal Auditors
Chicago

Thank you!

Thank you to Metra for hosting!

We really appreciate you Andrell and Sin Yu!

The Institute of
Internal Auditors
Chicago

IIA's Cybersecurity Topical Requirement: Background and Overview

On February 5, 2025, the Institute of Internal Auditors (IIA) published its first Topical Requirement, focused on Cybersecurity. This Topical Requirement defines a minimum required scope to be included in audits that address (or may address) cybersecurity risks. These requirements are intended to establish a consistent approach to assess the design and operation of cybersecurity governance, risk management, and control processes. Conformance with this Topical Requirement is required for assurance engagements, recommended for advisory engagements, and will be included in IIA-mandated quality assessment reviews of Internal Audit. A user guide is also available from the IIA that provides scoping considerations and further implementation guidance. The Topical Requirement will be effective 12 months after the issuance date (above).

What are the three core areas of the Cybersecurity Topical Requirement?

Governance [4 requirements]

clearly defined baseline Cybersecurity objectives and strategies that support organizational goals, policies, and procedures

- The cybersecurity governance program is effectively designed and implemented
- Policies and procedures are established and regularly updated
- Cyber-specific roles and responsibilities are defined
- Cybersecurity team members are adequately skilled (and skills are assessed)
- Stakeholders participate in assessing threats, vulnerabilities, and relevant risks

Risk Management [6 requirements]

processes to identify, analyze, manage, and monitor Cyber threats, including a process to escalate Cyber risks promptly

- Risk management practices incorporate cybersecurity risk identification, analysis, monitoring, escalation, and reporting
- Designated team members report on cyber risk management items
- Monitoring dashboards are in place to track cyber risks (mitigation status, priority, etc.)
- A cyber response plan exists and is tested
- Incident response capabilities are in place to communicate (escalate) relevant details to stakeholders

Controls [7 requirements]

management established and periodically evaluated control processes to mitigate cyber risk

- Cyber-specific controls are designed and implemented, and accountable resources are assigned to sustain effective practices
- Cyber training is provided to relevant stakeholders and end users
- Controls exist to manage and protect IT assets, data, and related systems
- Cyber practices consider strong configurations, data governance / encryption, patch management, secure development, network architecture, etc.

Applicability

The new Cybersecurity Topical Requirement is not a mandate to audit cybersecurity, and the user guide is not a "required" work program.

Assurance engagements that identify cybersecurity as a subject of the audit must assess the Topical Requirement for applicability, and this assessment must be documented (including a rationale for any exclusions). This also applies when cybersecurity was not part of the stated scope but is identified as a risk while performing an engagement. For advisory engagements, the requirements are recommended but not required.

Key Considerations

The Topical Requirement emphasizes the importance of professional judgment, allowing internal auditors to tailor their assessments based on the specific risk profiles of their organizations. The standards are relevant and applicable to a wide range of scenarios and can be scaled for small businesses up to large enterprises.

Where to Start?

Risk Assessment and Planning

Internal auditors must assess the organization's strategies, objectives, and risks at least annually to determine the engagements to include in the annual audit plan. On audits where cybersecurity is identified as a significant risk, the Topical Requirement must be applied.

Documentation and Evidence

Audits that are identified during the risk assessment as having relevant cyber risks must be assessed against the Topical Requirement, and any exclusions must be documented and retained. This documentation should include rationale and will be reviewed during quality assessments.

Framework Mapping

Internal auditors should reconcile their intended cybersecurity control testing to the Topical Requirement to provide adequate coverage. The user guide provides a mapping of the requirements to widely adopted frameworks.

Professional Judgment

Internal auditors must use professional judgment to determine which elements of the Topical Requirement may be applicable and should be included within relevant engagements.

Quality Assurance

The quality assurance function must conduct assessments to determine if the internal audit function is appropriately considering cybersecurity risks in audit risk assessments and documenting exclusions appropriately.

As internal audit experts, Protiviti helps audit leaders balance the critical elements of compliance, enabling technology, and innovation. By staying aligned with industry standards and leveraging technology and data, we enhance the effectiveness of audit functions and help transform them into pivotal components of organizational strategy.

We have a dedicated team of Technology Audit and Advisory professionals with deep experience in planning and executing cybersecurity audits, and we were actively involved in reviewing several iterations of this inaugural Topical Requirement from the IIA. Our team offers tailored guidance to modernize your audit processes and elevate your function's relevance and effectiveness in a variety of areas, including cybersecurity.

How are we feeling about risk?!

Mechanisms for response in a time of rapid change and uncertainty.

- Continue to Improve the Risk Assessment
  - Frequency
  - Changing Audit Universe
- Agile Auditing
- Upskilling and Adaptability
- More Real Time Monitoring

The Institute of
Internal Auditors
Chicago

Chapter Annual Meeting & Awards Ceremony

Please join us on **Thursday, May 22nd** to honor membership milestones, recognize certification awardees and present chapter member awards with food and drinks at our in-person Annual Meeting.

During the annual meeting, we will welcome the incoming officers and board members and recognize our Past Presidents.

Please RSVP!

Date: Thursday, May 22, 2025
Time: 3:30 pm – 7:00 pm CT

GIBSONS
BAR • STEAKHOUSE

Where:
Gibson's Bar & Steakhouse
1028 North Rush Street
2nd floor
Chicago, IL 60611

The Institute of Internal Auditors
Chicago

IIA Chicago Annual Golf Classic
Monday, August 25, 2025
Cog Hill Golf & Country Club – Course #2

Registration is now open! - https://na.eventscloud.com/832944

Cog Hill
GOLF & COUNTRY CLUB

Mark Your Calendars

Date	Title	Speaker	Time - CST
Upcoming IIA Chicago Chapter Events Visit - https://www.theiia.org/en/chapters/united-states/illinois/chicago/			
4/30/25	Audit 201: Auditor in Charge	Danny Goldberg	9:00 am – Noon
05/16/25	An Introduction to Information Technology General Controls	Chris Stoneley	12:00 pm – 4:00 pm
05/22/25	IIA Chicago Chapter Annual Meeting	@Gibson's Steakhouse	3:30 pm – 7:00 pm
06/05/25	NextGen Kickball Game & Happy Hour		4:00 pm – 7:00 pm
8/25/25	2025 Annual Golf Classic at Cog Hill		7:30 am – 4:30 pm
9/16/25	Staff Auditor Training	Danny Goldberg	TBD
11/12-11/13/25	11th Annual IT Hacking Conference	multiple	8:00 am – 5:00 pm

The Institute of
Internal Auditors
Chicago

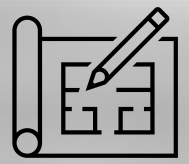
AUDIT LEADERS NETWORK

Benefits:

***Find Your* Network.**
***Find Your* Solution.**

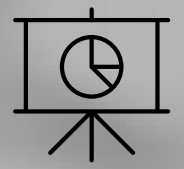
Executive Virtual Roundtables

Connect with other business leaders and discuss the latest trends and challenges in your industry.



Tools and Templates

Take advantage of our exclusive library of risk and fundamentals-based tools and templates to support and enhance your audit function.



Benchmarking

Access our Benchmark Hub™ and Pulse Check reports to compare your function's performance with those of peers.

Audit Leaders Network
Benchmark. Lead. Succeed.

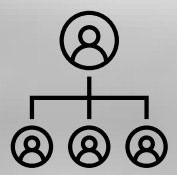
AUDIT LEADERS NETWORK

Benefits:

***Find Your* Network.**
***Find Your* Solution.**

Knowledge Briefs

Stay up-to-date with the latest industry trends and insights with our quarterly Knowledge Briefs.



CAE Bulletins

Stay informed on the latest news and developments in the internal audit profession with our bi-weekly CAE Bulletins.

What's New Newsletters

Keep up-to-date with new learning resources, events, and networking opportunities.

Audit Leaders Network
Benchmark. Lead. Succeed.

Exclusive invite to join up to two Upcoming ALN Roundtables for CAEs. *Scan the QR code to select your topics.*

Audit Leaders Network
Benchmark. Lead. Succeed.