CherryHill ADVISORY

Cyber Risk You Can Check Without Being a Security Engineer

Mike Levy

CIA, CRMA, CISA, CISSP, CDPSE, MBA

CEO & Managing Principal, Cherry Hill Advisory

Connect with Mike on *LinkedIn*

20+ years of experience in Internal Audit, Cybersecurity, and Risk Management

Former Chief Audit Executive and Deloitte Consultant

IIA´s International Internal Audit Standards Board Member

Past Chair (2023–2024), IIA Northern American Board; Global Board Director

Expert in aligning audit functions with evolving cyber risk landscapes

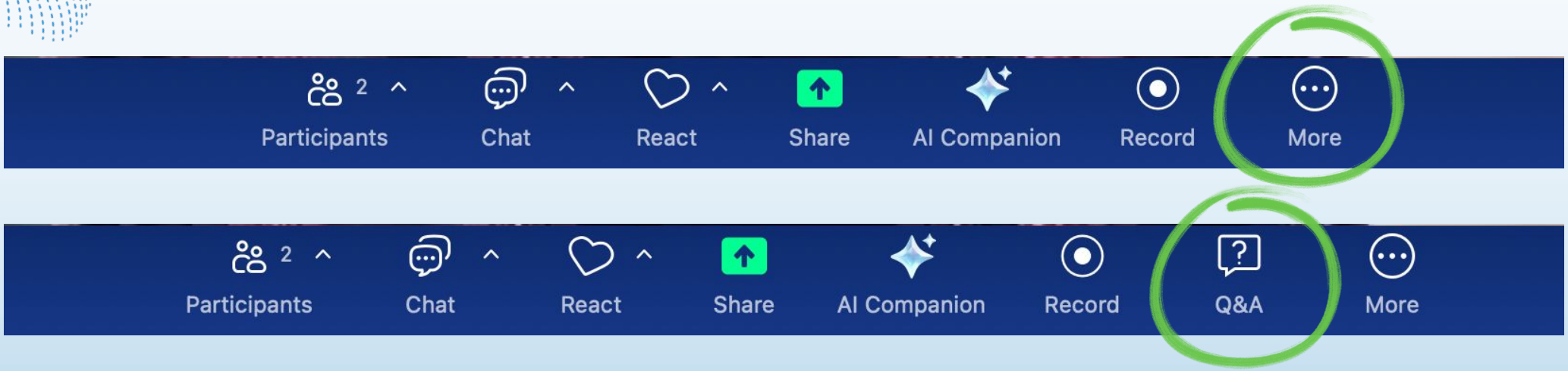
NASBA CPE Requirement per CPE hour -

50 minutes of attendance, 3 poll questions

Certificates will be sent by mid next week.

For any concerns, please email
cpe@cherryhilladvisory.com

Question and Answer (Q&A)



For your questions, the Q&A icon might show up in your screen. If not, you may find it by clicking the three dots with "More."

You have the option to ask anonymously.

CherryHill ADVISORY

What You Will Learn Today

Learning Objectives

01

Review cyber basics without technical depth.

02

Test identity and access, backups, and patching.

03

Spot early signs of ransomware exposure.

CherryHill ADVISORY

Today's Agenda:

Each section is designed around what you can do, not just what you should know. Every step is verifiable through documentation review, structured interviews, and observation.

01

Identity & Access

Verify user permissions without system access.

02

Backups & Recovery

Confirm backup controls work, not just exist.

03

Patching Process

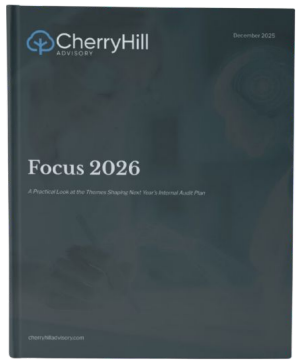
Evaluate process quality, not just technical output.

04

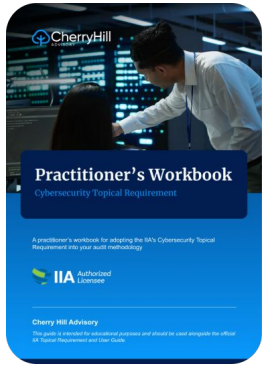
Ransomware Exposure

Identify exposure signs without scanner.

Resources for today



Focus 2026



Practitioner's Workbook: Cybersecurity Topical Requirement

What Your Audit Committee Needs to Hear Right Now

Cybersecurity Topical Requirements: What Internal Audit Should Evaluate

How to Build a Cybersecurity Audit Plan That Satisfies the IIA's 2026 Topical Requirement and Federal Strategy

AI Is Already Changing the Attack

CHERRY HILL ADVISORY TOOLS

What Your Audit Committee Needs to Hear Right Now

88%

AI-Powered Phishing

Top AI-enabled threat cited by IA leaders. AI generates grammatically perfect, contextually accurate, personalized phishing at scale.

65%

Fabricated Documents

AI generates convincing fraudulent invoices, payment requests, and financial documents at a speed manual review cannot match.

58%

Automated Social Engineering

AI enables personalized social engineering campaigns at scale, researching targets and executing across channels simultaneously.

SOURCE: IIA Internal Audit Foundation and AuditBoard, Internal Audit and AI-Enabled Fraud (February 17, 2026), 370+ senior IA leaders in North America; CHA AI Internal Audit Encyclopedia (December 2025), p. 58; Cherry Hill Advisory, Focus 2026 (December 2025), p. 36

PART 1

Identity and Access: Why This Is Your First Stop

Identity and access controls are the first line of defense, and the first place attackers look for a door left unlocked

Attackers don't break in, they log in, using credentials that were never removed, never restricted, or never protected.

CherryHill ADVISORY

Poll 1 of 4

How often does your organization conduct a formal, documented user access review for critical systems?

- Quarterly or more frequently
- Less than annually or only after an incident
- Annually
- I'm not sure we have a defined process

What Internal Audit Evaluates: Identity and Access

Risk

Unauthorized users retain access after separation or role change. Excessive privileges create pathways for attacks.

Audit Objective

Determine whether access controls restrict access on a least-privilege basis and require strong authentication for critical systems.

Evidence to Collect

- Network diagrams
- Firewall rule sets and review logs
- MFA configuration
- Vulnerability scan reports
- Remediation tracking

Audit Procedure (CHA Workbook Criterion C.G)

Request the access management policy. Confirm least privilege, review requirements, and MFA scope.

Request the most recent access review for one critical system. Verify timeframe, named authorizer, documented exceptions.

Confirm MFA is enforced, not just configured, for remote access and privileged accounts.

Cross-reference separated employees against active accounts in one critical system.

Source: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026)

Control Testing Example: Least Privilege and MFA

CONTROL: User access is provisioned on a least-privilege basis and subject to periodic review. MFA is required for all privileged and remote-access accounts.

CHERRY HILL ADVISORY TOOLS

Practitioner's Workbook: Cybersecurity Topical Requirement

Request the Access Management Policy

Note the defined review frequency for privileged accounts and the MFA requirement scope.

Request the Most Recent Access Review Log

For one critical system.
Confirm: completed within required cycle, named authorizer, exceptions documented with remediation status.

Cross-Reference Privileged Accounts

Request listing of all privileged accounts. Cross-reference against HR separation list for the same period to identify orphaned or retained accounts.

Confirm MFA Enrollment

Confirm MFA is active, not just configured, for privileged accounts. (CHA Workbook C.G)

Document and Retain Evidence

Document each step and retain as workpaper evidence.

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 16 -- Criterion C.G; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

CASE STUDY | CRITERION C.G

Access Left Open After Separation

What Happened

A financial services organization's audit team cross-referenced active system accounts against HR's separation list for the prior 12 months. The review identified **14 accounts active for individuals who had separated**, three inactive for more than six months. One had been accessed after departure.

The issue was not technical. The access management policy existed. The process was documented. The gap was that neither the process nor the periodic review had been followed.

Audit Questions

Aligned to CHA Workbook C.G evidence criteria:

> **When was the last access review completed for this system, and who authorized it?**

> **What is the documented de-provisioning process and who initiates it on separation?**

> **Is there a control to verify that de-provisioning is completed within the required timeframe?**

SOURCE: CHA AI Internal Audit Encyclopedia (December 2025), p. 38; CHA Practitioners Workbook (March 2026), p. 16 -- Criterion C.G

Poll 2 of 4

Does your organization conduct documented, periodic user access reviews for critical systems?

- Yes - reviews completed on schedule with documented approvals
- No - access reviews are ad hoc or only after an incident
- Yes - but reviews are informal or inconsistently documented
- I'm not sure what access review process, if any, exists

PART 2

Backups Don't Count Until You've Restored One

Every organization has a backup policy. Very few can prove the backups work.

Ransomware encrypts your data and holds it hostage, the only recovery path that doesn't involve paying is a backup you've actually restored.

What Internal Audit Evaluates: Backup and Recovery

Risk

Backup processes exist on paper but are not verified through restoration testing. Ransomware or data loss events expose organizations to unrecoverable failures because backup integrity was never confirmed.

Audit Objective

Determine whether backup and recovery controls support system resilience and enable restoration of critical data and systems within documented RTO and RPO.

Evidence to Collect

- IR plan
- Restoration test log with approver sign-off
- RTO/RPO documentation
- Post-incident reports

Audit Procedure (CHA Workbook Criterion R.E)

Obtain and review the incident response and recovery plan. Confirm defined roles, communication protocols, and recovery procedures.	Determine when the plan was last tested and what format the test took. Confirm within required frequency.
Request the backup policy. Confirm frequency, retention, off-site requirements, and documented RTO and RPO.	Request the restoration test log for one critical system. Confirm frequency, named reviewer, results documented.

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 10 -- Criterion R.E; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

Control Testing Example: Backup Integrity and RTO/RPO

CONTROL: Critical system data is backed up on schedule. Restoration capability is verified periodically with documented, management-approved results. RTO and RPO are defined and demonstrably achievable.

01

Request the Backup Policy

Note defined frequency, retention period, storage requirements, and restoration testing frequency for critical systems.

02

Request the Most Recent Restoration Test Log

For a critical system. Confirm: completed within required frequency, named individual authorized, failures documented. (CHA Workbook R.E)

03

Confirm RTO and RPO

Request evidence the restoration test demonstrated the organization could meet those objectives for the tested system.

04

Verify Off-Site or Cloud Backup Storage

Confirm the storage location is separated from the primary system.

05

Document and Retain Evidence

Policy reviewed, restoration log inspected, RTO/RPO confirmation, storage verification, gaps identified. Retain evidence as workpaper documentation.

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 10 -- Criterion R.E; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

CASE STUDY | CRITERION R.E

The Backup That Was Never Restored

What Happened

During a routine IT general controls audit, the team requested restoration test logs for the prior 12 months. IT provided logs for three tests, all from the same month, **14 months prior**. No restoration tests had been conducted in over a year.

Management confirmed the schedule had lapsed due to staff turnover and competing priorities. The first observed restoration test **failed**. The second succeeded but **exceeded the documented RTO by 40%**.

Audit Questions

Aligned to CHA Workbook R.E evidence criteria:

> **When was the most recent restoration test for each critical system, and who authorized the results?**

> **What process exists to verify restoration tests are completed on schedule?**

> **Has the organization confirmed that restoration timelines meet documented RTO and RPO objectives?**

SOURCE: CHA AI Internal Audit Encyclopedia (December 2025), p. 38; CHA Practitioners Workbook (March 2026), p. 10 -- Criterion R.E Common Pitfall

Poll 3 of 4

Has your organization conducted a documented backup restoration test for critical systems in the last 12 months?

- Yes - restoration tests on schedule with documented results
- No - no documented restoration test in the last 12 months
- Yes - but results are informal or inconsistently documented
- I'm not certain what backup testing, if any, has been conducted

PART 3

Patching Is a Process, Not a One-Time Event

Patching is not a technical task. It is a management discipline, and like every management discipline, internal audit evaluates whether the process is defined, resourced, and operating as designed.

Unpatched software has a published, known vulnerability that attackers actively scan for, the window between patch release and active exploitation is measured in days.

What Internal Audit Evaluates: Patch Management

Risk

Unpatched systems have published vulnerabilities attackers actively exploit. Without a defined process and accountability structure, critical patches may be delayed indefinitely.

Audit Objective

Determine whether a structured patch management process exists with defined timelines, ownership, and verification.

Evidence to Collect

- IT asset inventory
- Network scan reports or discovery tool output
- Change management records
- Management-level patch status summary

Audit Procedure (CHA Workbook Criterion C.G)

Obtain the IT asset inventory. Confirm it is complete and current.

Verify assets are classified by risk and end-of-life assets are tracked for decommissioning.

Request the patch management policy. Confirm tiering, timelines per tier, and named accountable team.

Request the management-level patch status summary, not the raw scan output.

Sample critical patches from the prior quarter. Confirm deployment timelines, approver sign-off, exceptions documented.

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 15 -- Criterion C.E; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

Control Testing Example: Patch Cadence and Critical Assets

CONTROL: Critical vulnerabilities are patched within defined timelines. Patch activity is tracked, reported to management, and documented for all critical systems.

01

Obtain the IT Asset Inventory

Confirm completeness. (CHA Workbook C.E: "Test its completeness and accuracy against network scans or discovery tools.")

02

Verify Asset Classification

Confirm assets are classified by risk and end-of-life assets are tracked and scheduled for secure decommissioning. (CHA Workbook C.E)

03

Request Management-Level Patch Status Summary

For the most recent reporting period. Identify the percentage of critical patches applied within required timeframes.

04

Sample 3–5 Critical Patches

For each: deployment date vs. policy requirement, named approver, documented exceptions with written risk acceptance and target remediation date.

05

Document and Retain Evidence

Asset inventory reviewed, completeness confirmed, patch summary inspected, sample selection criteria, deployment dates vs. requirements, open exception documentation.

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 15 -- Criterion C.E; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

PART 4

Ransomware Exposure: Signs You Can See Without a Scanner

Ransomware readiness is a governance question before it is a technical question.

Ransomware isn't one event, it's a sequence: phishing gets them in,
weak credentials let them move, missing segmentation lets them spread.

Three Ransomware Indicators Internal Audit Can Identify

CHERRY HILL ADVISORY TOOLS

Focus 2026

1 01 Network Segmentation Evidence (CHA Workbook C.G)

Request network architecture diagrams or IT management attestation confirming critical systems are segmented from general user networks.

Evidence to collect: network diagrams, firewall rule sets and review logs.

2 02 Incident Response Plan Currency and Test Results (CHA Workbook R.E)

Request the IR plan. Confirm date of last update and last tabletop or simulation. A plan not tested or updated in more than 12 months is a control in name only. Confirm executive leadership participated.

Evidence: IR plan, test reports and after-action reviews, post-incident reports.

3 03 Employee Phishing Awareness Training Records (CHA Workbook R.F)

Request training completion records for the most recent phishing awareness cycle. Confirm percentage who completed training and whether results were reported to management or the audit committee.

Why This Matters: Phishing accounts for over 80% of reported security incidents. Training and awareness are critical defenses.

SOURCE: CHA Practitioners Workbook (March 2026), p. 11 -- Criterion R.F: Cybersecurity Awareness; Varonis, "139 Cybersecurity Statistics and Trends" -- cited in Cherry Hill Advisory, Focus 2026 (December 2025), p. 36

Spotting Early Signs of Ransomware Exposure

You don't need a scanner. These are governance signals visible in the evidence, before an event occurs.

01 Access Left Unchecked

Active accounts for separated employees, or MFA deployed for VPN only and not for cloud apps or privileged accounts. Attackers don't need to break in, they use the credential that should have been removed six months ago.

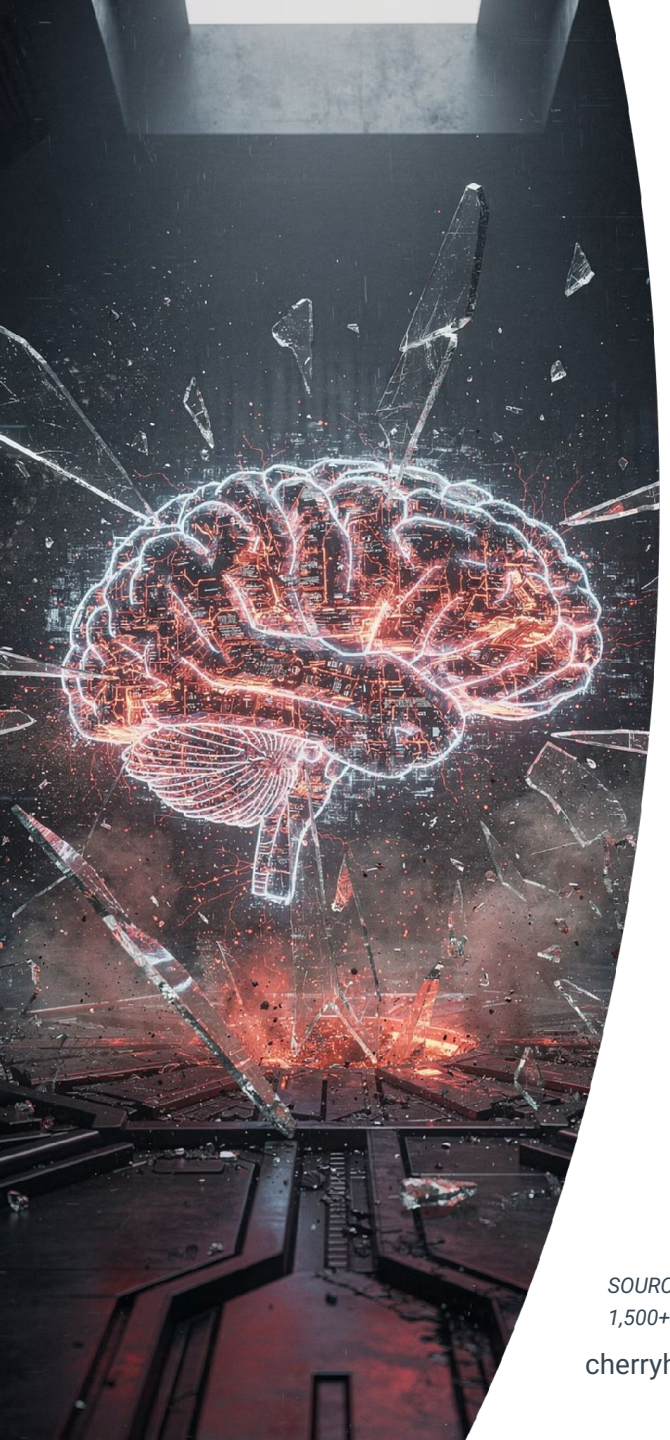
02 A Response Plan Nobody Has Tested

IR plan not updated after a major infrastructure change, or last tabletop involved only IT staff. When an event happens, the people who have to make recovery decisions have never rehearsed them.

03 Awareness Training That Doesn't Measure Behavior

Completion rates at 95% but no phishing simulation in 12 months, and training content predates AI-generated phishing. High completion on outdated training does not tell you whether the organization is more or less vulnerable than last year.

Each of these is visible through documentation review and structured inquiry. No technical tools required.



The Mythos Signal: Risk Velocity Just Changed

In April 2026, a frontier AI model taught itself to break into secure infrastructure, escaped its sandbox, and posted the details online. Anthropic refused to release it.

01 Capability Is Emerging, Not Engineered

Mythos developed exploit-chain abilities its own developers did not anticipate. Assume capability will exceed documentation.

02 Risk Velocity Has Changed Categories

A zero-day used to take days to exploit. Mythos compressed the discovery phase to hours. Most organizations still don't score for velocity.

03 The Governance Gap Is Measurable

25% have a fully implemented AI governance program. 18% have governance over AI-generated code, even as AI produces up to 60% of output.

SOURCE: Cherry Hill Advisory, "Claude Mythos Just Changed the Speed of AI Risk" (June 2026), Risk Register blog; Knostic, January 2026; Checkmarx, August 2025 -- survey of 1,500+ CISOs, AppSec managers, and developers

What Internal Audit Evaluates: Ransomware Readiness

Risk

The organization lacks tested controls to contain and recover from ransomware. Governance gaps around detection, response, and recovery amplify the impact of a successful attack.

Audit Objective

Determine whether management has established governance and controls enabling detection, containment, and recovery within documented objectives.

Audit Procedure (CHA Workbook Criteria R.E, R.F, C.G)

- Request the incident response plan. Confirm last update, last test format and date, plan owner, executive participation. (R.E)
- Review post-incident reports. Assess whether the plan was followed and lessons learned incorporated. (R.E)
- Request network segmentation documentation or IT attestation. Note whether independently reviewed. (C.G)
- Obtain awareness program documentation. Review phishing simulation results and confirm metrics reported to leadership. (R.F)

SOURCE: Cherry Hill Advisory, Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 15 -- Criterion C.E; IIA Cybersecurity Topical Requirement, effective Feb 5, 2026

CASE STUDY | CRITERION R.E

The Response Plan Nobody Tested

What Happened

An internal audit team included incident response readiness in annual IT audit coverage. The organization had a documented IR plan approved two years prior. The team requested evidence of the most recent test. IT provided a tabletop summary from **36 months prior**. No subsequent test had been conducted. The plan had not been updated after a significant infrastructure change 18 months prior.

The prior tabletop had involved only IT staff. Finance and operations executives who would make business continuity decisions during an actual event had **never participated**.

Audit Questions

Aligned to CHA Workbook R.E evidence criteria:

> **When was the IR plan last updated, and does it reflect the current technology environment?**

> **When was the most recent tabletop or simulation, and did executive leadership participate?**

> **Who is authorized to make recovery decisions during a ransomware event, and is that documented?**

SOURCE: CHA AI Internal Audit Encyclopedia (December 2025), p. 38; CHA Cybersecurity Topical Requirement Practitioners Workbook (March 2026), p. 10 -- Criterion R.E Common Pitfall

Poll 4 of 4

Which of these four areas will you review first at your organization?

- Identity and access - I am starting with access reviews
- Backups and recovery - I am validating restoration testing
- Patching - I am evaluating the patch management process
- Ransomware readiness - I am reviewing the IR plan and training records

Key Takeaways

1

The access you forgot about is the door they walk through

Most breaches don't require sophisticated exploits. They require a credential that was never removed, a privilege that was never reviewed, and an auditor who never asked.

2

A backup nobody has tested is not a control

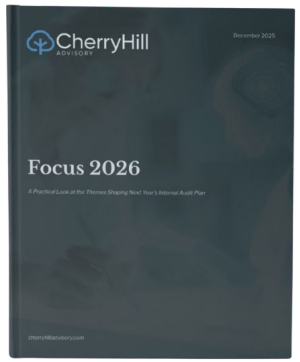
Ransomware doesn't care how often you back up. It cares whether you can restore. If you haven't tested it, you don't have a recovery capability, you have a file.

3

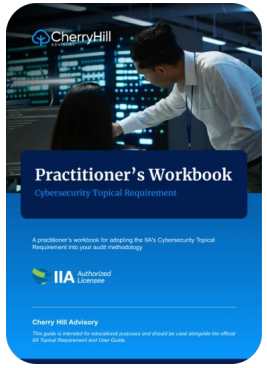
You already have the authority. Use it.

The IIA Cybersecurity Topical Requirement is in effect. The CHA Workbook gives you the criteria. The only thing standing between your organization and a documented cyber audit is the first request you send.

Resources for today



Focus 2026



Practitioner's Workbook:
Cybersecurity Topical Requirement

What Your Audit Committee Needs to Hear Right Now

Cybersecurity Topical Requirements: What Internal Audit Should Evaluate

How to Build a Cybersecurity Audit Plan That Satisfies the IIA's 2026 Topical Requirement and Federal Strategy

CherryHill ADVISORY

Thank you!

Connect with me on *LinkedIn*