We'll get you there

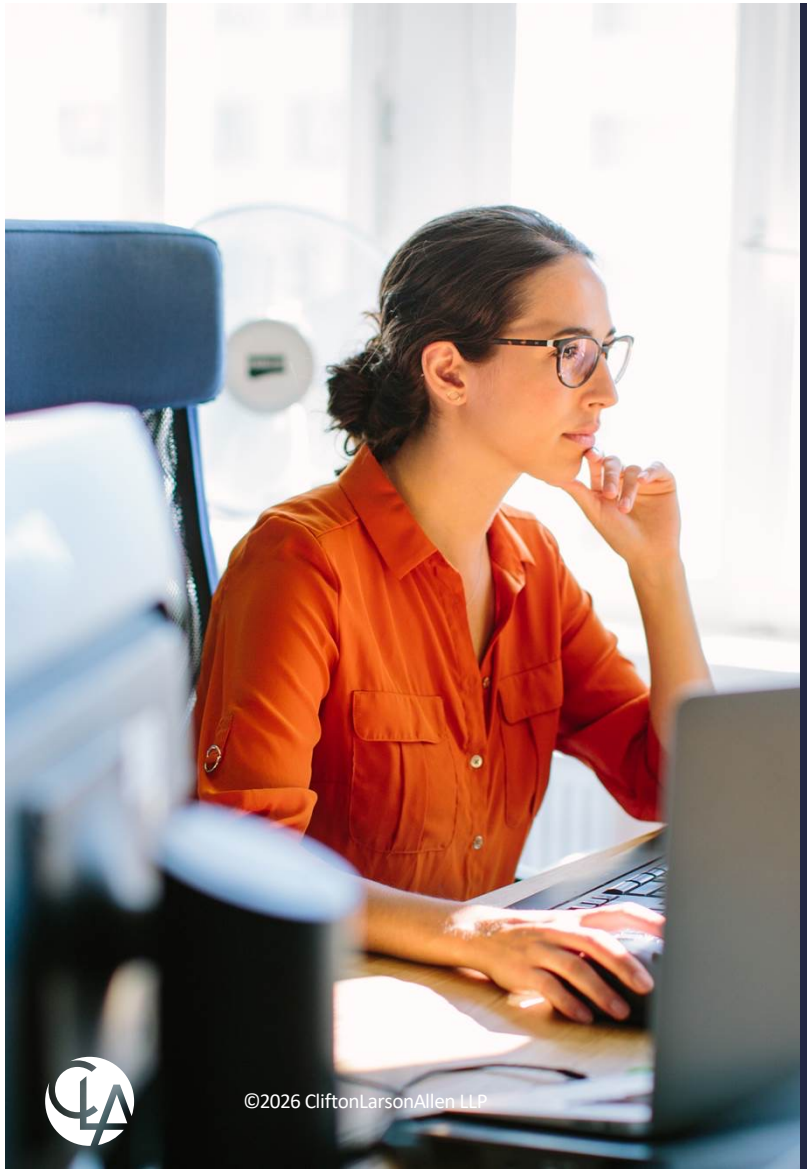
CPAs | CONSULTANTS | WEALTH ADVISORS

IT for Non-IT Auditors: What You Need to Understand *Now*

Atlanta IIA TAC 2026

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.



Learning Objectives

1. Explain why IT risk is no longer isolated to the IT department
2. Recognize the core IT concepts every internal auditor needs to understand
3. Identify IT risk indicators during operational, financial, compliance, and process audits
4. Ask better, plain-English questions of IT and business stakeholders
5. Determine when to handle IT risk within the audit team and when to involve specialist
6. Define practical steps to built IT fluency without becoming overly technical

Every Audit is Technology Enabled

Section 1

Goals

You ***do not*** need to become an IT auditor. You ***do*** need to become IT-risk fluent.

Understand the ***business impact*** of technology risk

Recognize where ***IT risk*** shows up in non-IT audits

Ask better ***questions***

Know what matters and when to involve specialists

Where do you feel least comfortable?

- Access and user permissions
- Change management
- Cybersecurity/resilience
- Cloud/SaaS/vendor risk
- Data/interface controls
- AI and automation
- Knowing what evidence is enough

Audience Poll

The IT Risk Landscape Has Changed

Section 2

The Old Mental Model vs. Today's Reality

	Current Reality
IT Risk Belongs to IT	Technology risk is embedded in every business process.
Systems are behind the scenes	Systems drive decisions, workflows, approvals, reporting, and customer experience.
Cybersecurity is a specialist topic	Cyber, identity, vendors, and resilience are board-level risks.
Audit can rely on visible approvals	Audit must understand system-driven evidence and automated workflows.

What has changed in the Risk Environment?

Today, organizations face:

- More cloud-based systems
- More vendors and connections
- Access controls matter more
- Data moves further and faster
- AI is reshaping processes
- Resilience matters as much prevention

TECHNOLOGY HAS BECOME FASTER, MORE DECENTRALIZED, MORE OUTSOURCED, AND MORE AUTOMATED

IT Risk is Business Risk

What Non-IT Auditors Actually Need to Understand

Section 3

The Practical IT Risk Map

Identity and Access: Who Can Do What?

Ask Yourself: Who has access, what can they do, and should they still have it?

Key Concepts

- User provisioning
- Termination access removal
- Role changes
- Segregation of duties
- Periodic access reviews
- Privileged/admin access
- Service accounts

Red Flags

- Shared accounts
- Users with more access than their role requires
- Access reviews completed mechanically
- Terminated users not removed promptly
- Admin access not separately monitored

Privileged Access

Who can override the normal rules?

- Admin accounts
- Database access
- Emergency access
- Developer access to production
- Elevated permissions

Change Management: *What Changed and Who Approved It?*

Request & Documentation

Change never documented

Review & Testing

No approval or testing evidence

Production Deployment

Developer moves own changes to production

Monitoring & Follow Up

Emergency changes never reviewed

Interfaces and Data Flows: Where does the data go?

1

How data moves between systems

Includes system integrations, APIs, batch jobs, and manual uploads/downloads that transfer information across applications.

2

How information is verified

Includes reconciliations and exception reporting used to confirm data is complete, accurate, and processed correctly.

3

How issues are identified and resolved

The timing of each audit is driven by real-world factors like recent changes, new systems, regulatory pressure, incidents, or leadership concerns.

Automated Controls: When the System Becomes the Control

Automated Control Risk

- ***Our job*** – Determine if the system is configured correctly and has not changed.

Important for Audits:

Auditors need evidence that the configuration is appropriate and protected from unauthorized change.

Common Examples:

- Three-way match
- Credit limits
- Approval routing
- Duplicate payment prevention
- System-enforced segregation of duties
- Required fields
- Automated exception reporting

Cloud, SaaS, and Vendors

The Control Environment You Do Not Fully Own

Managing the Third Party Risk

- Shared Responsibility
- Vendor Oversight
- Access & Security
- Connected Systems

So What? Moving to the cloud does not transfer accountability — organizations must understand, monitor, and verify the controls they rely on from vendors.

Cyber Resilience: How to be Prepared

Identify threats quickly and respond before they become major disruptions.

Restore critical systems and data fast enough to meet business needs.

Keep the organization operating through incidents and recovery events.

AI and Automation: Governance

Where is AI being used?

- Use Case Inventory
- Data inputs
- Shadow AI

What decisions does AI influence?

- Human review
- Bias & Fairness
- Explainability

Who is accountable?

- Approval
- Monitoring
- Model drift

Internal Audit’s Role Has Changed

Section 4

Internal Audit's Role Has Changed

- Internal audit ***does not*** own technology risk.
- Internal audit ***does*** need to understand how technology affects the risk and control environment.

Internal Audit Should Move Toward:

1. From checklist testing to risk-based questioning.
2. From isolated IT Audits to integrated audit coverage.
3. From technical assurance only to business-impact assurance.

What Should IA Be Providing?

IA should provide assurance over the organization's ability to manage technology-enabled risk by:

1. Identifying technology dependencies in business processes.
2. Testing whether key technology controls are designed and operating.
3. Connecting IT risk to business outcomes.
4. Challenging governance and ownership gaps.
5. Coordinating with IT audit, cybersecurity, compliance, privacy, and risk functions.

Where non-IT Auditors Add the Most ***Value***

You know the process. IT knows the system. Risk lives in the connection.

How to Listen for IT Risk in Any Audit

Section 5

Tune into IT Risk in Any Audit

Key Questions when you hear these things from Management

"System won't allow XYZ"	"Access is role-based"	"Report comes from the System"	"Vendor handles that"	"It's automated"
Who configured that rule, and how do we know it still works?	Who approves roles, and when are they reviewed?	What data feeds the report, and can it be changed?	What are we responsible for?	What controls protect the automation?

Five Questions that Work in Almost Any Audit…

Non-technical, but powerful questions:

1. What systems support this process?
2. Who can initiate, approve, change, or override transactions?
3. What data is used, and where does it come from?
4. What parts of the process are manual, automated, or vendor-managed?
5. What would tell management that something went wrong?

What Proves the Control Worked

Claim

Management says:

1. "We review access.“
2. "Changes are approved.“
3. “The system won’t allow it."

Evidence is Reviewed

Examples include:

1. System generated access listing with evidence of review
2. Change tickets with approval, testing, and migration evidence
3. Configuration screenshots with date/time/context

Audit Conclusion

Control objectives achieved when:

1. Reviewed
2. Completeness and Accuracy verified.
3. Discrepancies resolved.

Mini Case Study

Payroll introduces a new timekeeping system integrated with HR and the general ledger. Management says implementation went well and “the system handles approvals.”

Think through these questions:

- Where could IT risk show up?
- What could go wrong?
- What evidence would you request?
- What questions would you ask?

Key Takeaways

- Technology changes how controls operate.
- Automated approvals require configuration assurance.
- Interfaces require completeness and accuracy checks.
- Access drives authorization risk.
- Vendor involvement changes evidence needs.
- Business ownership still matters.

Building the Skillset

Section 6

IT Fluency Roadmap for Internal Auditors

Build *IT confidence* step-by-step: understand, apply, collaborate, and lead.

		Practical Skills
Foundational	• Understand core IT control concepts	Access, change, data, vendors, resilience
Applied	• Recognize IT risk in business audits.	Ask better process and evidence questions
Collaborative	• Work better with IT specialists	Scope clearly, translate risks, review findings
Strategic	• Advise leadership on technology-enabled risk	Connect IT risk to business objectives and governance

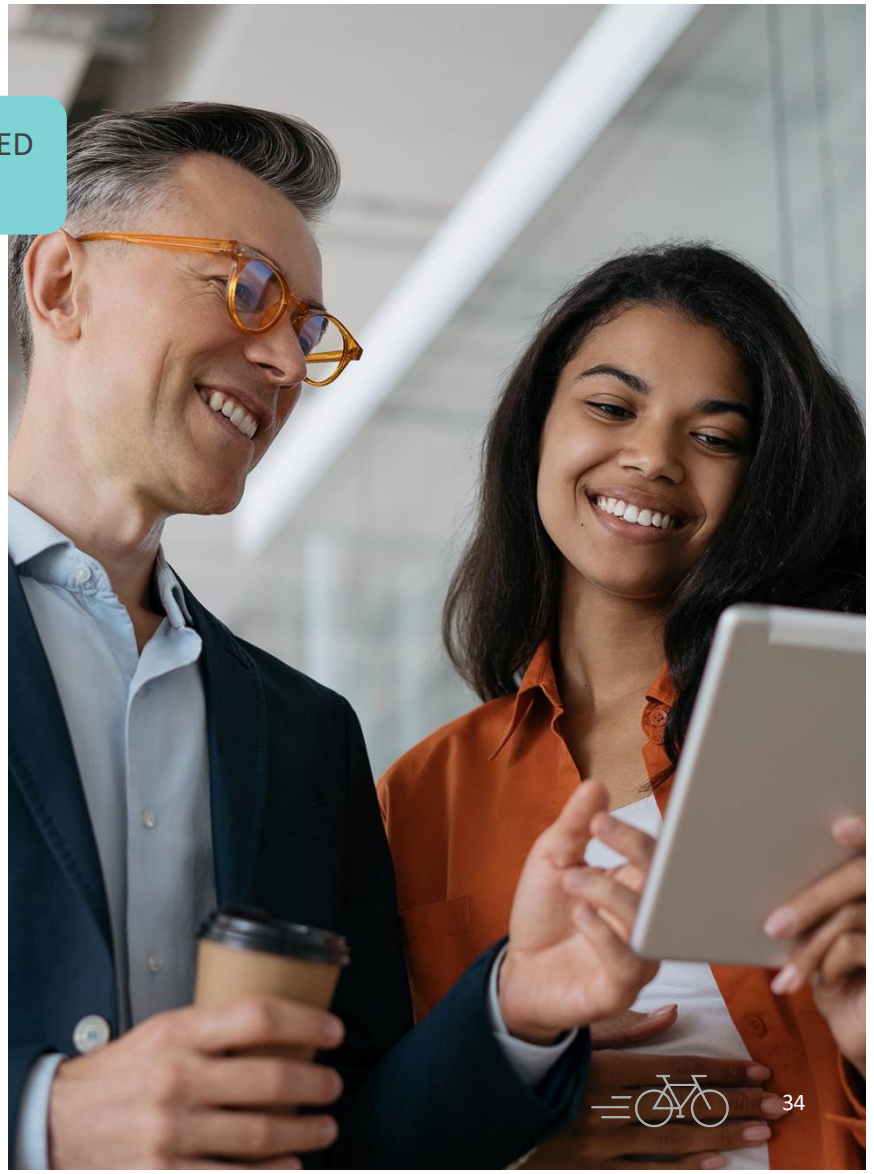
How Early-Career Auditors Can Start

- Learn the top 10 IT terms used in your organization
- Ask what system supports each process you audit
- Shadow an ITGC walkthrough
- Review one SOC report and identify user controls
- Practice mapping process steps to system steps
- Ask “what could go wrong if access, data, or change controls fail?”

When to Bring in an IT Specialist

KNOWING WHEN SPECIALIZED SUPPORT IS NEEDED

- Highly Technical Controls
- Complex Privileged Access
- Cybersecurity & Cloud
- Data & Analytics
- AI Governance
- System Implementation



Bringing it all Together

Section 7

What You Should Understand

The best auditors connect business objectives, technology, controls, and risk.

Understand the ***business objective & impact***

Recognize ***technology dependency***

Understand ***IT controls*** and interpret ***evidence***

Enforce ***ownership & accountability***

Takeaway Tool: The IT Risk Conversation Guide

- Systems Involved
- Access
- Change
- Data/Interface
- Vendor & Cloud
- Cyber Resilience
- AI & Automation
- Evidence
- When to involve specialists

Final Q&A

If you have additional questions, please contact:

Matthew Hoverman
704-816-8542
matthew.hoverman@CLAconnect.com

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS