rightworks

Compliance Readiness Checklist for Accounting Firms

Practical steps to protect client data, manage access, and prove reasonable security practices before you are asked.

Accounting firms are trusted with some of their clients' most sensitive information. Compliance readiness does not have to start with fear, complexity, or a scramble after something goes wrong. It can start with practical habits: knowing where client data lives, controlling who can access it, documenting what is in place, and keeping evidence ready for clients, insurers, regulators, or firm leadership.

How to use this checklist:

Work through one section at a time. For each item, mark whether it is in place, identify the evidence you could produce, and note the next practical step. This checklist is not legal advice and does not guarantee compliance, but it can help firms build a stronger, more provable compliance foundation. Requirements depend on the firm's activities, the information it maintains, client locations, contracts, and applicable exemptions.

Section 1: Know What You Need to Protect

Checklist item	Why it matters	Evidence to keep	Status
Identify where client data lives across tax software, cloud apps, email, portals, document storage, payroll systems, and shared drives.	You cannot protect or prove controls around data you have not identified.	Data inventory, application list, storage locations, system owners	☐ Not started ☐ In progress ☐ In place
Document which systems contain taxpayer, financial, payroll, dependent, or other sensitive client information. Identify the applicable retention policy.	Different systems may require different access, retention, and monitoring practices. Customer information generally must be securely disposed of no later than two years after its last use to provide services, unless an exception applies.	Client-data map, system classification notes, retention schedule, exceptions, disposal records	☐ Not started ☐ In progress ☐ In place
Review whether client residence, industry, engagement type, data type, or applicable thresholds create additional requirements.	State privacy and breach notification laws, sector-specific obligations (HIPAA, GLBA), and client requirements may apply based on who the firm serves.	Client-state review, engagement notes, data-type assessment, threshold and exemption analysis, compliance applicability matrix	☐ Not started ☐ In progress ☐ In place

Section 2: Control Who Has Access

Access control is one of the most practical places for a busy firm to start. Many compliance, insurance, and client due diligence questions eventually come back to the same proof point: can the firm show who has access to client data, how that access is protected, and what happens when access is no longer needed?

Checklist item	Why it matters	Evidence to keep	What to look for in a supporting solution	Status
Require unique user access for everyone, including seasonal, remote, outsourced, and offshore staff.	Shared credentials make it difficult to prove who accessed what and increase the risk of password exposure.	User list, access assignments, shared-login exception list	Look for a solution that supports unique user access and reduces the need for shared passwords.	☐ Not started ☐ In progress ☐ In place
Use multi-factor authentication for systems that touch client data.	MFA is a core expectation across security and compliance frameworks, including the FTC Safeguards	MFA enforcement report, covered system inventory, exception list, admin account review	Look for a solution that can help enforce MFA consistently across the applications staff use most.	☐ Not started ☐ In progress ☐ In place

Checklist item	Why it matters	Evidence to keep	What to look for in a supporting solution	Status
Apply least-privilege access so users only reach the applications and client information they need for their role.	Limiting access reduces exposure and makes access decisions easier to explain during reviews.	Role-based access matrix, access review notes, policy approvals	Look for a solution that supports role-based access, app-level access policies, and easier review of permissions.	☐ Not started ☐ In progress ☐ In place
Remove access promptly when someone leaves, changes roles, or no longer supports a client.	Offboarding gaps are common, especially after tax season, staffing changes, or temporary engagements.	Offboarding timestamps, deactivation records, user access review	Look for a solution that makes it easier to disable access quickly and keep a record of what changed.	☐ Not started ☐ In progress ☐ In place
Review access periodically, especially before tax season, after tax season, and after staffing changes.	Access that was appropriate six months ago may no longer match the firm's current client work.	Quarterly or seasonal access review, reviewer sign-off, remediation notes	Look for a solution that provides visibility into users, applications, and access activity so reviews are easier to complete.	☐ Not started ☐ In progress ☐ In place

Section 3: Turn Security Practices Into Proof

Being secure is important. Being able to prove what is in place is what helps a firm respond confidently when a client, insurer, regulator, or leadership team asks for evidence. The goal is not to create paperwork for its own sake. The goal is to make the firm's real security practices visible, current, and defensible.

Checklist item	Why it matters	Evidence to keep	Status
Maintain a Written Information Security Plan that reflects how the firm actually operates today and is appropriate for the firm's size, complexity, and activities.	Covered firms are expected to maintain a WISP containing administrative, technical, and physical safeguards appropriate to the firm. A WISP should be a living document, not a template that no longer matches the business.	Current WISP, review history, approved updates	☐ Not started ☐ In progress ☐ In place

Checklist item	Why it matters	Evidence to keep	Status
Complete and document a risk assessment that identifies internal and external risks and how those are addressed.	A WISP should be based on a risk assessment. Risk assessments help connect policies and controls to the firm's actual environment.	Risk assessment, mitigation plan, accepted-risk notes	☐ Not started ☐ In progress ☐ In place
Keep access logs and user activity records for systems that contain client or taxpayer data.	Covered firms are expected to maintain policies, procedures, and controls to monitor user activity and detect unauthorized access. Logs can help demonstrate who accessed what, when, and from where.	Access logs, SSO reports, login activity, retention policy	☐ Not started ☐ In progress ☐ In place
Provide staff with security awareness training, and document training completion and policy acknowledgements.	Covered firms are expected to provide security awareness training. Training records show that policies were communicated and practiced, not just written.	Training roster, completion reports, signed acknowledgements	☐ Not started ☐ In progress ☐ In place
Select and retain vendors capable of maintaining appropriate safeguards, periodically assess vendors based on risk, and retain supporting due diligence records.	Covered firms are expected to select reasonable vendors, ensure contractual safeguards, and periodically assess vendor risk.	Vendor inventory, risk classification, diligence materials such as SOC 2 reports where applicable, contract security terms, review cadence	☐ Not started ☐ In progress ☐ In place

Section 4: Strengthen the Everyday Security Baseline

Checklist item	Why it matters	Evidence to keep	Status
Maintain antivirus or anti-malware protection on devices that access client data.	Endpoint protection is a basic safeguard for systems that store or reach sensitive information.	Endpoint protection report, device inventory, alert review notes	☐ Not started ☐ In progress ☐ In place
Use firewalls and secure network configurations.	Network safeguards help reduce unauthorized access to systems and client data.	Firewall configuration, network diagram, review records	☐ Not started ☐ In progress ☐ In place

Checklist item	Why it matters	Evidence to keep	Status
Encrypt client data at rest and in transit over external networks.	Covered firms are expected to encrypt client data at rest and in transit. Encryption helps protect data if a device, backup, or account is compromised.	Encryption status report, data flow and device inventory, backup configuration	☐ Not started ☐ In progress ☐ In place
Back up critical data and test recovery on a defined cadence.	Backups support continuity and ransomware resilience, but only if they can be restored.	Backup report, restore test results, backup retention policy	☐ Not started ☐ In progress ☐ In place
Use secure remote access practices for staff working outside the office.	Remote work, outsourced support, and seasonal staffing can create access risk if not managed consistently.	Remote access policy, MFA report, VPN or secure access configuration	☐ Not started ☐ In progress ☐ In place

Section 5: Prepare Before Someone Asks

Compliance readiness is easier to manage when evidence is gathered before a request arrives. A proactive firm does not need to have every answer memorized. It needs to know where records live, who owns the response, and how to show the steps it has taken to protect client data.

Checklist item	Why it matters	Evidence to keep	Status
Name an owner responsible for coordinating the security and compliance readiness program, and ensure internal oversight for an external owner.	Clear ownership by a designated individual is expected of covered firms and helps the firm keep documentation current and respond faster when questions come up.	Owner assignment, responsibilities, service-provider oversight if applicable, annual review notes where required	☐ Not started ☐ In progress ☐ In place
Create a simple evidence folder or compliance binder for key records.	Centralizing evidence makes client, insurer, regulator, or leadership requests easier to handle.	Evidence index, folder structure, record owners	☐ Not started ☐ In progress ☐ In place

Checklist item	Why it matters	Evidence to keep	Status
Maintain a written incident response plan with named roles, internal processes, communications, remediation, documentation, and post-event review steps.	Covered firms are expected to maintain an incident response plan and notify the FTC no later than 30 days after discovery of certain events. When timing matters, firms should not be deciding roles and responsibilities for the first time.	Incident response plan where required, contact list, notification records, tabletop exercise notes	☐ Not started ☐ In progress ☐ In place
Review cyber insurance requirements before renewal.	Insurance questionnaires often ask about MFA, backups, encryption, WISP status, and evidence.	Insurance questionnaire, attestation support, control evidence	☐ Not started ☐ In progress ☐ In place
Schedule a recurring compliance readiness review.	A light recurring review keeps the checklist manageable and helps prevent last-minute cleanup.	Review calendar, meeting notes, updated action list	☐ Not started ☐ In progress ☐ In place

Quick-Win Action Plan

If you only have...	Why it matters	Evidence to keep
30 minutes	List the top 10 applications that store or access client data.	Application inventory with data owner and access owner
1 hour	Review current users in your most sensitive client-data systems.	User access export, removed-user list, follow-up notes
1 day	Confirm MFA, offboarding, and access review practices across core systems.	MFA report, offboarding record, access review checklist
1 week	Create a simple evidence folder for your WISP, risk assessment, training records, access logs, vendor reviews, retention and disposal records, and incident response plan.	Evidence index and owner list
1 month	Run a full access and evidence review before busy season or renewal season.	Completed checklist, remediation log, leadership summary

Choosing a Supporting Solution

Firms do not need to solve every compliance challenge with one tool, and no single solution establishes compliance or replaces a broader security program, legal guidance, a WISP, risk assessment, staff training, vendor oversight, incident response planning, or ongoing review. But if access control is a priority, a supporting solution may help produce practical, day-to-day proof points: who has access, how access is protected, what applications are in scope, and how access is removed when it is no longer needed.

- Access control: Help manage who can reach client-data applications and under what conditions.
- Single sign-on and MFA support: Reduce password risk and support stronger authentication practices.
- User and application visibility: See which users and applications are in scope for review.
- Offboarding support: Make it easier to remove access when staff, roles, seasons, or client assignments change.
- Evidence readiness: Maintain access records and activity visibility that can support client, insurer, regulator, or leadership due diligence conversations.

For firms looking for this type of support, Cloud Protect is one example of a solution designed to help centralize access, strengthen authentication, improve visibility, and support access-related evidence. If you would like to learn more, connect with Rightworks to see whether it is a fit for your firm's compliance readiness goals.

Bottom line: Compliance readiness is not about panic. It is about building a practical, repeatable way to protect client data and prove the firm is taking reasonable steps to manage risk. Start with access. Keep evidence as you go. Review regularly. Improve over time.