rightworks

2026 US Accounting Regulatory and Security & Compliance Map

A comprehensive map of cybersecurity obligations for accounting and bookkeeping firms

Regulations, professional standards, and industry-standard security frameworks covered

- GLBA / FTC Safeguards Rule (16 CFR Part 314)
- State privacy laws and state breach-notification laws
- IRS Publication 4557 + Written Information Security Plan (WISP)
- AICPA Code of Professional Conduct / State Boards of Accountancy
- NIST Cybersecurity Framework / ISO 27001
- HIPAA, SOX / PCAOB, FISMA / IRS Publication 1075 (if in scope)
- SOC 2 / AICPA Trust Services Criteria
- Circular 230 professional conduct obligations

May 13, 2024	30 days	Every 6 months	At least annually
FTC Safeguards breach notification requirement in effect	FTC notice deadline after discovery of a 500+ consumer event	Vulnerability assessments unless continuous monitoring applies	QI report and annual pen test, unless continuous monitoring applies

How to use this map

Each row includes a Compliance timing / deadline column. Some items have firm dates or cadences, including FTC's 30-day breach notification, annual reporting, annual penetration testing, six-month vulnerability assessments, and two-year secure disposal. Under 16 CFR 314.6, financial institutions maintaining customer information concerning fewer than 5,000 consumers are exempt from the formal written risk assessment, testing regime, written incident response plan, and annual report requirements in 16 CFR 314.4(b)(1), (d)(2), (h), and (i). Other obligations are scope-triggered, contract-triggered, event-triggered, or periodically reviewed rather than tied to a fixed calendar date.

IRS publications, NIST CSF, ISO 27001, SOC 2, professional standards, insurance underwriting criteria, and client requirements should be distinguished from binding statutes and regulations. Product mappings identify controls or evidence that may support compliance, subject to product configuration, licensing, and firm procedures. Product use does not by itself establish compliance.

This compliance map also highlights where Rightworks Cloud Protect and Cloud Protect Plus can help firms strengthen their compliance readiness.

Compact compliance map:

Federal baseline, assurance, and state layer

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
FEDERAL BASELINE	GLBA / FTC Safeguards Rule	Risk assessment and security program — document risks, assign accountable ownership, and maintain safeguards for client financial data.	**MANDATORY if in scope**	At least annually for Qualified Individual report; periodic risk reassessment; program updates after material operational, threat, or testing changes.	Risk assessment; named Qualified Individual; controls that address identified risks; written risk assessment and annual reporting where required, subject to under-5,000 consumer exceptions.	Cloud Protect centralizes identity, access, MFA, offboarding, SSO, and app-access audit history across systems holding client data.	Cloud Protect Plus adds endpoint and email-layer controls that reduce phishing, malware, ransomware, and device exposure.	WISP/security program; risk assessment; QI assignment; MFA report; access logs; offboarding records; annual report record.
FEDERAL BASELINE	GLBA / FTC Safeguards Rule; IRS Pub 4557	Written Information Security Plan required by GLBA/ FTC Safeguards Rule; IRS Pub 4557 and Security Six provide implementation guidance for protecting taxpayer data.	**MANDATORY**	WISP requirement applies if handling taxpayer data; PTIN holders certify WISP awareness at PTIN renewal; IRS/ security-summit are guidance and should be checked for current updates.	WISP; antivirus/ anti-malware; firewalls; MFA; backups; drive encryption; VPN for remote access.	Cloud Protect supports centralized MFA, SSO, app access policy, unique credentials, secure remote access governance, and offboarding evidence.	Cloud Protect Plus adds endpoint protection, email protection, backup/ recovery support, and managed device controls.	WISP; MFA logs; access policy records; backup recovery reports; endpoint status; training records.
FEDERAL BASELINE	FTC Safeguards testing and monitoring	Regularly test or monitor safeguards and identify vulnerabilities in customer-information systems.	**MANDATORY if in scope**	Annual penetration test and vulnerability assessments at least every six months and after material changes, unless effective continuous monitoring is in place.	Continuous monitoring or annual penetration testing plus vulnerability assessments every six months; retest after material changes. Subject to under-5,000 consumer exceptions.	Cloud Protect provides access visibility and policy evidence that supports audit and remediation follow-through.	Cloud Protect Plus adds endpoint, email, and backup signals that support testing evidence and remediation tracking.	Pen test report; vulnerability scan results; remediation log; change review; access and endpoint evidence.

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
FEDERAL BASELINE	FTC breach notification	Notify the FTC after discovery of a breach involving unauthorized acquisition of unencrypted customer information for 500+ consumers.	**MANDATORY if threshold met**	No later than 30 days after discovery of a notification event affecting at least 500 consumers; FTC notification requirement effective May 13, 2024. Separate state notification requirements may also apply.	Incident response process; breach scope assessment; evidence of accounts, systems, and data affected.	Cloud Protect access logs help establish who accessed which systems, when, and from where for scope assessment.	Cloud Protect Plus adds email and endpoint alerts plus backup/recovery evidence for incident triage.	IR plan; breach review record; access/event logs; email/endpoint alert records; notification decision log.
FEDERAL BASELINE	Secure disposal under FTC Safeguards	Dispose of customer information securely when no longer needed, subject to legal or business-retention exceptions.	**MANDATORY**	No later than two years after the last use of the customer information to serve the customer, unless an exception applies; retention policy reviewed periodically.	Retention and disposal procedures; business/legal retention exceptions; periodic data-retention review.	Cloud Protect helps control and evidence access to retained customer-data systems.	Cloud Protect Plus adds endpoint and backup controls to reduce exposure of retained data.	Retention schedule; disposal record; access logs; backup retention evidence; exception log.
ASSURANCE	SOC 2 / vendor due diligence	Enterprise clients may ask for assurance, and firms must evaluate vendors as part of service-provider oversight.	**MANDATORY / Contract-driven**	No universal fixed date for SOC 2 reports; may be contract/client renewal driven. FTC Safeguards Rule requires contractual safeguards and risk-based periodic assessment of service providers.	Vendor inventory; SOC 2 Type II collection where applicable; security terms; periodic reassessment.	Cloud Protect helps document which staff and apps access client data, with control evidence for client/vendor conversations.	Cloud Protect Plus adds email, device, endpoint, and backup evidence that broadens demonstrable security posture.	Vendor inventory; SOC 2 records; service-provider review log; MFA/access evidence; endpoint/backup reports.

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
ASSURANCE	AICPA Code / State Boards	A breach involving confidentiality violations, gross negligence, or failure to follow applicable professional standards may result in an AICPA or state-board inquiry.	**MANDATORY**	No single federal calendar date; event-driven after breach or board inquiry; continuing obligations depend on state board rules.	Documented controls; professional accountability; governance over confidential client data.	Cloud Protect provides policy-driven access, MFA enforcement, offboarding, and audit-ready access records.	Cloud Protect Plus adds layered defenses showing active steps to reduce compromise and preserve recoverability.	Control library; access audit log; MFA report; offboarding record; IR plan; endpoint/ email evidence.
ASSURANCE	Circular 230	Circular 230 governs practitioner duties such as accuracy, due diligence, competence, returning client records, and firm compliance procedures.	**MANDATORY for IRS practice**	No fixed calendar deadline; applicable duties arise whenever practicing before the IRS.	Policies and controls for protecting client matters, communications, and taxpayer information.	Cloud Protect helps enforce access control and unique credentials for tax systems and client-data applications.	Cloud Protect Plus adds email protection and endpoint controls around client communications and tax data touchpoints.	Access audit trail; MFA enforcement; tax-system access policy; email threats; offboarding evidence.
STATE LAYER	Comprehensive state privacy laws	Client residence can trigger state privacy obligations, even when the firm is located elsewhere.	**MANDATORY if in scope**	State-specific; 19 comprehensive privacy laws in force as of January 1, 2026; obligations attach based on jurisdictional, revenue, or data-processing thresholds. GLBA exemptions vary by state.	Data inventory; policy transparency; data-subject response process; reasonable security controls. Requirements vary by state statute.	Cloud Protect supports centralized access control, access logs, and user/app visibility for consistent handling of personal information.	Cloud Protect Plus adds endpoint, email, and backup controls that reduce breach probability and support resilience.	Data inventory; access logs; privacy/security policy records; DSAR evidence where applicable; backup/endpoint reports.

Compact compliance map:

State layer, specialized obligations, and security baseline

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
STATE LAYER	State breach notification laws	All 50 states have breach-notification laws that may stack on top of federal FTC notifications.	**MANDATORY if breach occurs**	Where a state law includes a consumer-notice period, it is typically 30-60 days, in addition to the FTC's 30-day notification requirement. Separate attorney-general notification requirements may apply.	Incident response; rapid scope assessment; state-by-state notification decision records.	Cloud Protect access logs and offboarding records help assess affected accounts, data systems, and access paths.	Cloud Protect Plus provides email/ endpoint alert evidence and backup/recovery reporting for breach analysis and continuity.	IR plan; notification matrix; scope assessment; access logs; email/endpoint alerts; recovery documentation.
STATE LAYER	Cyber insurance requirements	Carriers commonly require MFA, backups, encryption, documentation, and accurate security attestations.	**Market Practice / Contract-driven**	Renewal/ application driven; commonly annual with policy renewal, plus event-driven production of evidence after an incident or claim.	Evidence-backed security posture matching policy attestations.	Cloud Protect provides MFA and access evidence to support insurance applications and renewals.	Cloud Protect Plus adds endpoint, email, and backup posture evidence commonly expected by cyber insurers.	MFA report; backup status; endpoint protection report; WISP; questionnaire evidence; IR plan.

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
SPECIALIZED	HIPAA	Firms handling PHI, such as bookkeeping/ payroll for medical practices or health-plan work with access to patient billing, claims, diagnosis, or similar PHI, may become business associates.	**MANDATORY if in scope**	A BAA must be in place before PHI is disclosed to the firm. Breaches must be disclosed no later than 60 days after discovery or as set out in the BAA. Timing of other obligations may depend on the BAA.	BAA; administrative and physical safeguards; technical safeguards including access controls, audit controls, authentication, and transmission security.	Cloud Protect supports user identity, least privilege, SSO, MFA, and access audit trails for PHI-touching systems.	Cloud Protect Plus adds email filtering, endpoint protection, and backup controls around PHI access points and communications.	BAA; access logs; MFA report; PHI system access review; email/ endpoint reports; backup evidence.
SPECIALIZED	SOX / PCAOB	Firms auditing public companies may need to evaluate issuer ITGCs relevant to financial reporting under applicable SOX and PCAOB requirements.	**MANDATORY if in scope**	Audit-cycle and client-engagement driven; evidence is obtained during issuer control testing and audit work. SOX 404(b) auditor attestation does not apply to accelerated filers or emerging growth companies.	Issuer ITGC evidence evaluated by the auditor: access controls, change management, privileged access, and system integrity.	Cloud Protect supports access reviews, role-based access control, privileged access visibility, and offboarding evidence.	Cloud Protect Plus adds device posture, endpoint policy, and backup evidence supporting broader ITGC and resilience narratives.	Access recertification; privilege inventory; offboarding timestamps; endpoint reports; backup evidence.
SPECIALIZED	FISMA / IRS Pub 1075	Firms handling federal tax information from government agencies or federal contract work face stricter control expectations.	**MANDATORY if in scope**	IRS Pub 1075 requirements apply before handling federal tax information. For FISMA-related work, cadence depends on the agreement and control baseline.	For Pub 1075: IRS-tailored NIST control baseline, access control, logging, encryption; incident response, service-provider oversight. For FISMA-related contracts: the agency-assigned NIST control baseline and contractual security requirements.	Cloud Protect helps centralize access governance, MFA, logging, and account revocation for systems touching federal tax information.	Cloud Protect Plus adds endpoint/ email control evidence and recoverability for stricter control expectations.	System access logs; MFA report; account review; IR plan; endpoint/ email reports; backup evidence.

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
SECURITY BASELINE	MFA everywhere	The FTC Safeguards Rule requires MFA for every system touching client data. IRS guidance also identifies MFA as a baseline safeguard.	**MANDATORY baseline**	In place before access is granted; reviewed periodically; alternatives require written approval and must be equivalent controls under the FTC Safeguards Rule.	MFA across tax software, email, cloud storage, portal, IRS e-Services, and admin accounts.	Cloud Protect enforces MFA through SSO and centralized policies across integrated apps and client-data systems.	Cloud Protect Plus adds email defenses that reduce MFA bypass and credential theft attempts.	MFA enforcement report; SSO log; exception list; admin account review.
SECURITY BASELINE	Offboarding / least privilege	Access for departed seasonal or offshore staff must be revoked quickly based on the firm's documented procedures.	**MANDATORY baseline**	Access should be removed at termination/ offboarding; access controls should be periodically reviewed under FTC Safeguards.	Unique users; no shared logins; least privilege; last-day revocation; periodic access review.	Cloud Protect enables one-click lockout, access policy management, unique credentials, and access reviews.	Cloud Protect Plus adds device controls and mailbox/device risk reduction after personnel changes.	Offboarding timestamps; user access review; app access report; policy configuration records.
SECURITY BASELINE	Backups / ransomware resilience	IRS Pub 4557 names backups within the Security Six. Backups and recovery controls should be maintained based on the firm's risk assessment, contractual commitments, and resilience requirements.	**IRS-recommended baseline**	No single fixed cadence in IRS Pub 4557; maintain and test/review backup and recovery controls on a documented, risk-based firm cadence and after material changes.	Encrypted offsite backups; restoration testing; recoverability documentation.	Cloud Protect supports access control around cloud repositories and backup admin access.	Cloud Protect Plus adds Microsoft 365 backup/recovery support and endpoint security to reduce ransomware impact.	Backup policy; restoration tests; backup recovery report; endpoint ransomware alert evidence.

Category	Regulatory Body & Obligation	Specific Obligation	Status	Compliance Timing / Deadline	Required Control	Cloud Protect	Cloud Protect Plus	Evidence Available
SECURITY BASELINE	Security awareness training	FTC program requirements include personnel training and specialized training for security staff.	**MANDATORY**	Updated as necessary to reflect risks identified by risk assessment; many firms operationalize as annual plus new-hire/seasonal refreshers.	Training program; completion records; role-specific security procedures.	Cloud Protect evidence and policy workflows support training around secure access, MFA, SSO, and offboarding procedures.	Cloud Protect Plus adds phishing/ email-security context and endpoint hygiene into the training baseline.	Training completion; policy acknowledgements; phishing/email report; security staff training record.

Can you produce the evidence required if the FTC, IRS, a state board, insurer, or enterprise client asked tomorrow? Cloud Protect supports the access-and-identity evidence layer; Cloud Protect Plus adds the email, endpoint and backup protection needed for a stronger compliance posture.

Learn more