Tax Software Compliance Features:

What to Validate Before Filing Season

INTUIT
professional tax solutions

Compliance failures don't announce themselves during quiet periods. They surface under pressure when volume is high, deadlines are tight, and your attention is split across hundreds of returns.

A client's Social Security number appears in an access log you can't review. A return gets modified without documentation of who changed what. An unauthorized user accesses sensitive data because the permission controls weren't configured correctly. By the time you discover these gaps at the start of a new season, you're managing compliance risk while maintaining production throughput.

Pre-peak season is your validation window. You have time to test, find gaps, and fix them before filing season creates consequences. By the new year, you're either working from a validated compliance infrastructure or discovering problems while processing client returns.

Here's what to validate and why it matters.

What Workflow Features Actually Do

Compliance features protect client data and reduce firm liability. They work two ways.

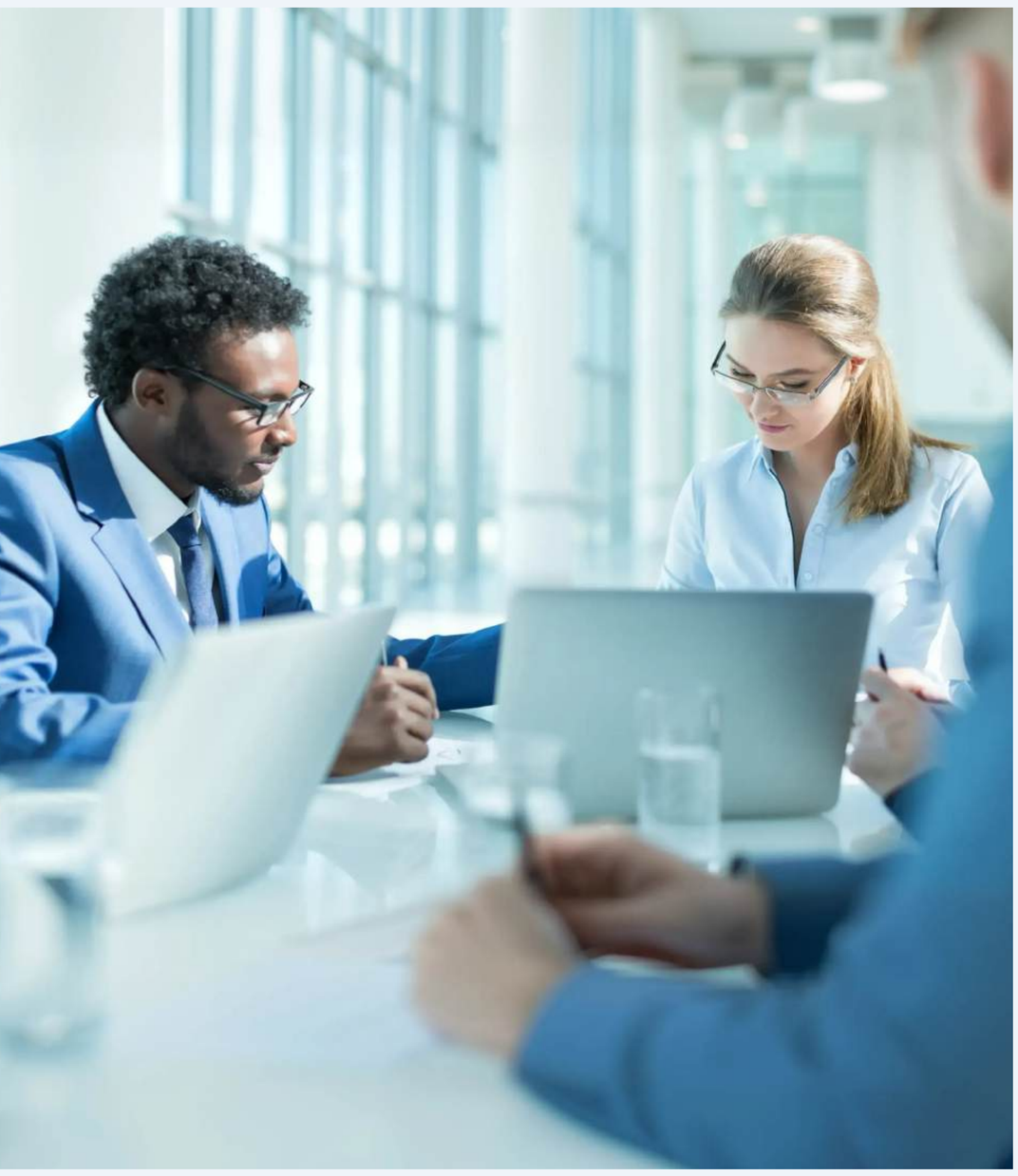
PREVENTION FEATURES

stop unauthorized actions before they happen. Access controls prevent users from viewing returns they shouldn't see. Permission levels stop inappropriate modifications. Session timeouts lock inactive accounts.

DOCUMENTATION FEATURES

show what happened after actions occur. Modification history captures who changed what and when. Deletion records prove document handling. Secure transmission logs confirm encrypted connections.

Five Core Compliance Features to Validate



01 Role-Based Access Controls

User-level permissions define who accesses which returns and what actions they can perform.

WHY THIS MATTERS:

Access accumulates over time. Former employees still have active accounts. Contractors have broader access than their current role requires. One firm found seven inactive accounts that had been sitting dormant for months.

TO VALIDATE

Time investment: 2 hours

1. Document all user roles in your firm.
2. Assign appropriate permission levels based on actual responsibilities.
3. Test whether users access only assigned returns.
4. Verify lower-privilege users can't override controls.
5. Confirm session timeouts lock accounts after 15-30 minutes of inactivity.

BENEFIT

Protects client data and reduces the risk of breaches.

Multi-Factor Authentication

02

Secondary verification beyond passwords includes SMS codes, authenticator apps, or biometric verification. Required at login and for sensitive operations.

WHY THIS MATTERS:

MFA reduces the risk of unauthorized access by roughly 99% compared to password-only systems. If someone gets your password through a phishing email or data breach, MFA stops them at the second verification step.

TO VALIDATE

Time investment: 1.5 hours

1. Enable MFA for all users.
2. Test the authentication flow across devices your team uses.
3. Verify backup methods exist for device loss scenarios.
4. Document your MFA policy in security procedures.

REAL-WORLD EXAMPLE:

Firms that enable MFA during pre-peak validation can block credential stuffing attacks when peak season begins. Audit logs often show dozens of failed login attempts stopped at the MFA layer during the busy season.

BENEFIT

Critical protection for remote work environments.

03

Data Encryption Standards

Encryption of data at rest and in transit uses AES-256 standards for stored data and SSL/TLS protocols for transfers.

WHY THIS MATTERS:

Encryption is table stakes for IRS compliance. You need to verify it's actually working, not assume it exists.

TO VALIDATE

Time investment: 1 hour

1. Confirm encryption meets IRS Publication 4557 requirements through vendor documentation.
2. Verify web-based platforms use secure connections by looking for "https" in your address bar, not "http."
3. Check certificate validity by clicking the lock icon in your browser.
4. Test that client portal communications show encrypted connections when clients access their information.

COMMON MISTAKE:

Firms assume their platform is encrypted because it's cloud-based. During validation, you discover your client portal is using an expired security certificate.

BENEFIT

Protects client personally identifiable information and ensures regulatory compliance.

Return Locking 04

Once a return is filed, locking prevents accidental or unauthorized modifications. When a filed return is changed and transferred to next year's filing, those incorrect changes carry forward into new returns.

WHY THIS MATTERS:

Returns get updated for amended filings. Staff make unintended modifications. Return locking creates a clear barrier between what's filed and what's being worked on.

TO VALIDATE

Time investment: 1 hour

1. Confirm return locking is enabled for filed returns.
2. Test that locked returns can't be edited without explicit override.
3. Verify that override attempts create documentation showing who made the change and when.
4. Document your firm's override procedures.

REAL-WORLD SCENARIO:

One firm discovered its return modification history was incomplete. Returns were updated after filing, but the changes didn't show who made the modifications or when they occurred. Return locking prevents this by creating an explicit "this return is filed" checkpoint.

BENEFITS

Prevents data corruption and creates a clear trail for filed work.

INTUIT ProConnect™ Tax

05

Document Management and Retention

Centralized storage for client documents with automated retention policy enforcement and version control.

WHY THIS MATTERS:

IRS requires three years minimum from filing date. Professional standards recommend seven years. Most firms need manual enforcement to work, and that fails at scale.

TO VALIDATE

Time investment: 1.5 hours

1. Upload test documents and verify storage location.
2. Confirm retention policies apply automatically.
3. Test version control.
4. Verify archived documents remain accessible throughout the retention period without degradation.
5. Document your retention policy in writing.

COMMON GAP:

Retention policies exist in procedures but aren't applied automatically by the system. Staff are manually deciding what to keep and what to delete. Enforcement becomes inconsistent, and some client files develop gaps.

BENEFIT

Eliminates manual tracking and ensures audit readiness throughout required preservation periods.

Pre-Peak Season Validation Approach

You don't need a month-long project. About 8-10 hours spread over three to four weeks tests core features without disrupting current operations.

Early in the validation window:

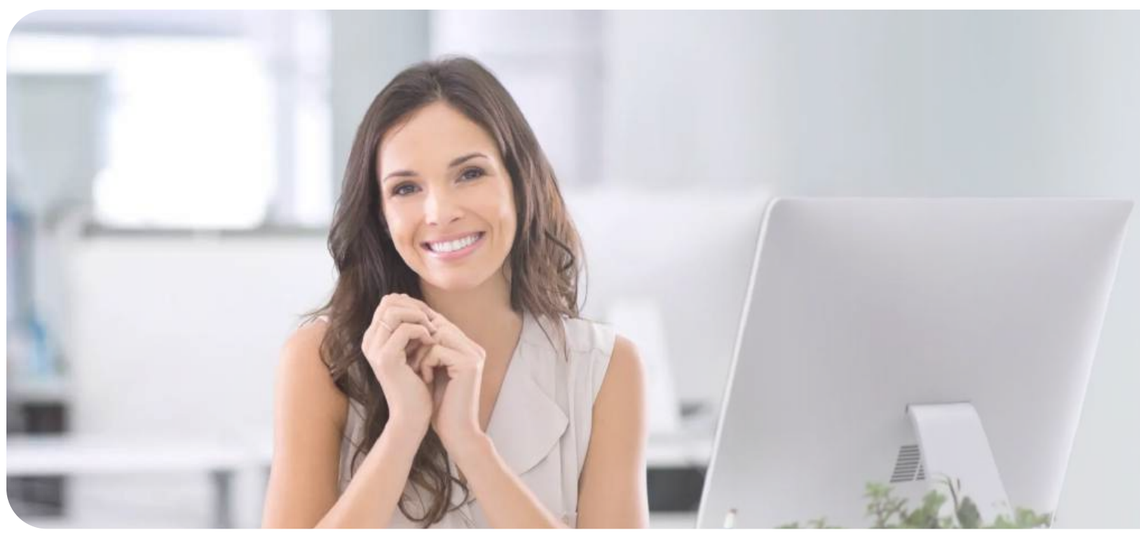
Review your current user list and update permission levels based on actual roles. Enable MFA for all users. Test session timeouts. Verify encryption certificates are current. Document who has what access and why.

Mid-validation:

Test return locking on sample filings. Process five to ten test returns through your complete workflow from prep to filing. Review modification documentation for completeness. Verify retention periods meet minimums for your jurisdiction.

Late validation:

Run a complete end-to-end test with sample returns across your actual workflow. Verify all systems are operational. Confirm staff training is complete.



RETURN

Validated compliance posture before peak season creates risk exposure.

Documentation Best Practices

Documentation proves your compliance controls work when regulators ask, clients dispute preparation decisions, or malpractice claims arise.

WHAT TO DOCUMENT:

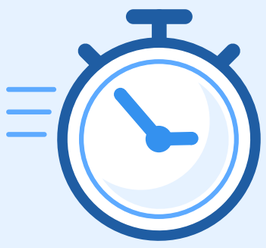
- Configuration records: current user list with permission levels, MFA enrollment status, encryption standards in use, retention policies applied
- Validation evidence: dated screenshots of security settings, test results from pre-peak validation, sample documentation of modifications showing who changed what
- Policies and procedures: your access control policy, incident response plan, data retention schedule, quarterly review schedule

STORAGE APPROACH

Keep compliance documentation separate from client files in secure, backed-up locations. Update documentation annually or whenever systems change significantly. Make documentation accessible to partners and compliance officers during audits or regulatory inquiries.

What This Means for Your Firm

Tax software compliance features protect firms from regulatory risk, data breaches, and liability exposure when properly configured and validated. Configuration determines effectiveness.



You have roughly **8-10 hours of validation work** ahead if you haven't tested these features recently. That's a small investment compared to discovering compliance gaps at the start of tax season while processing client returns under deadline pressure.

How ProConnect Tax Supports Compliance Validation

ProConnect Tax includes all six compliance features as core platform capabilities, designed specifically to support the validation approach outlined in this guide.

01 **Role-based** security architecture provides granular permission controls by user. During pre-peak validation, you assign permission levels matching your firm's structure: preparers, reviewers, partners, administrators. The system enforces those boundaries automatically and logs access attempts.

02 **Multi-factor authentication** integrates directly into the login process. Enable MFA for all users, and the platform handles authentication through SMS codes or authenticator apps. Your validation confirms authentication works across devices and backup methods exist for recovery scenarios.

03 **Encryption** meets IRS Publication 4557 requirements for both storage and transmission. Data at rest uses AES-256 encryption. Data in transit uses TLS protocols. During validation, you verify SSL certificates are current and connections show as encrypted.

04 **Return locking** prevents modifications to filed returns without explicit documentation. Once you mark a return as filed, the system creates a clear checkpoint. Any override attempts are logged with complete modification history showing who made changes and when.

05 **Document management** centralizes client files with automated retention policy enforcement. Set retention rules once, and the system applies them automatically based on document type and date. Version control maintains complete document history without manual tracking.

Configuration determines effectiveness. ProConnect provides the compliance infrastructure, but strategic firms validate that permissions are assigned correctly, users are trained on available features, and documentation proves controls work as intended.