preston@hardpointcompliance.com
hardpointcompliance.com

How a Microsoft 365 security assessment lines up with ALTA Best Practices 5.0

For real estate closing law firms and title agencies. ALTA's Title Insurance and Settlement Company Best Practices, Version 5.0, took effect October 8, 2026. A firm that follows them needs evidence for each item. This page shows which items an HPC assessment gives evidence for, and which it does not touch.

What the assessment gives evidence for

ALTA 5.0 item	What ALTA asks	What the assessment checks in Microsoft 365	What the firm gets
Pillar 3, A.1	Multi-factor authentication for systems holding client information	Which mailboxes and admin accounts require MFA, which sign-in methods are allowed, and whether any account can still sign in without it	A list of accounts and their MFA status, gaps named
Pillar 3, A.2	A password plan: unique logins and minimum standards	Password and sign-in policy, shared or generic accounts, idle sign-out settings	Current settings set against ALTA's list (see note)
Pillar 3, A.5	Network and cloud security for client information	Admin roles, access rules by location and device, SharePoint and OneDrive sharing, third-party app access	Findings ranked by risk, each with its fix
Pillar 3, A.7	Encryption in transit and at rest, where feasible	Whether email encryption is available and on, and how files are shared outside the firm	Current state and what is missing
Pillar 3, A.8	Reasonable monitoring for unauthorized access	Whether audit logging is on, whether sign-in and mailbox alerts exist, and who receives them	Yes or no for each, with the fix
Pillar 3, B.3	Periodic review of security controls	The assessment itself, dated, with an optional quarterly recheck	A dated report the firm can file as its review
Pillar 2, G.1 (email side)	Verify outgoing wire instructions independently; procedures should include MFA	The mailbox controls wire fraud relies on: hidden forwarding rules, mailbox access by other accounts, protection against spoofed senders (SPF, DKIM, DMARC)	Evidence the firm's email is hard to read or impersonate

Note on A.2: ALTA still lists password expiry, which current Microsoft and NIST guidance no longer recommends. The report shows the firm's setting and leaves that choice to the firm.

What the assessment does not cover

- Writing the information security plan (WISP) or the privacy plan
- The wire verification procedure itself, or a wire verification service (Pillar 2, G and J)
- Incident response and business continuity plans, and testing them; staff security training
- The title production system and any system outside Microsoft 365; software updates on the firm's computers (Pillar 3, A.3)
- Physical security, background checks, escrow accounting and reconciliation

Plainly

- ALTA's Best Practices are voluntary. An underwriter or lender may still ask how a firm handles them.
- The assessment gives evidence for the items above. It does not make a firm "ALTA compliant", and we never say it does.
- We would be a vendor under Pillar 7. A firm following the framework may ask us for our own security policy and insurance.
- Whether a federal or state rule applies to a given firm is a question for the firm's own counsel.

Fixed price. Assessments start at $1,000. Details and a sample report at hardpointcompliance.com.