

Best Practices v. 5.0 – Release Notes

Publication Date: October 8, 2026

Updated Content:

- Best Practices v 5.0
 - Best Practices Assessment Procedures v 5.0
 - Updated “Vetting a Vendor” Guidance v 1.01
-

Overview:

After the ALTA Best Practices were significantly updated in 2023 with the release of version 4.0, the Best Practices Executive Committee decided that a yearly review and recommendations for revisions as needed will better achieve the objective of having Best Practices respond to the changing requirements and needs of the industry, laws, and regulations. Each year since, ALTA has issued a revised version of the ALTA Best Practices. This year, we are moving the versioning to 5.0 to align with the significant changes being implemented in Pillar 7 to focus on vendor management.

Changes to Best Practices in version 5.0

The changes being implemented in the update from ALTA Best Practices v 4.2 to v 5.0 are as follows:

1. Conversion of the Best Practices guidelines to an outline format to support the reference to specific Best Practices sections, which replaces the use of bullets in prior versions of Best Practices.
2. Require in Pillar 1 documentation of the ALTA Policy Forms License compliance for inclusion in the certification package.

Procedures to meet this best practice:

- A. Establish and maintain for the Company and individuals, as needed:
 1. Applicable business License(s); compliance with the Licensing, registration, and business requirements of the applicable state regulatory [authority](#).
 2. Confirmed compliance with [ALTA's Policy Forms Licensing \(PFL\) requirement with proof of licensure*](#) attached to certification package.
(Licensure compliance certificate may be downloaded from: <https://alta.org/PFL-certificate/>)*
 3. A confirmed listing in the [ALTA Registry](#) (subject to those business entity types supported by the ALTA Registry).

3. Replacement of Pillar 7 to provide Vendor Management guidance, with the Complaint Handling of the prior Pillar 7 materials now included within Pillar 4. This expands on the Vendor Management Guidance document provided in 2025 by including Vendor Management as a Pillar within Best Practices.

Purpose: The use of a Vendor is often an appropriate business decision for a Company to perform certain functions, to develop and market additional products or services, or rely on expertise from Vendors that would not otherwise be available without significant investment. However, the fact that a Company enters into a business relationship with a Vendor does not absolve the Company of responsibility to avoid harm to the Consumer and other parties to the transaction. Thus, the Company should identify, evaluate and minimize the risk to funds, NPI, and legal and contractual obligations that may exist when utilizing Vendor software and/or services.

Procedures to meet this best practice:

- A. In selecting a Vendor for software, services or other matters, Company should:
 1. Evaluate whether the Vendor will have access to NPI or any funds held by Company.
 2. Identify risks posed to the Company from use of the Vendor that may impact the Company's responsibility for safekeeping funds, NPI, or other legal or contractual obligations.
 3. Depending upon the amount of NPI, funds or other information that the Vendor may impact or have access to, and which could cause harm to Consumer or other parties to the transaction, perform the following functions:
 - i. Conduct due diligence to verify that the Vendor understands and is capable of complying with the legal and financial responsibilities to the Consumer and other parties to the transaction.
 - ii. Request confirmation from the Vendor that the Vendor conducts appropriate training and oversight of employees that have Consumer contact or compliance responsibilities; and
 - iii. Include in the contract with the Vendor clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities which may cause harm to the Consumer or other parties to the transaction.
 - iv. Perform due diligence of Vendors to understand the risks posed by their use of sub-vendors, and determine whether sufficient information and

contractual protections have been provided to evaluate the sub-vendor risks:

- a. Whether the Vendor applies equivalent security controls to their vendors
 - b. Whether the Vendor notifies you of breaches involving sub-vendors
 - c. Whether the Vendor is liable for the actions or inactions of their sub-vendors to the same extent that the Vendor would be liable if they were providing the service(s)
- B. Periodically review and confirm that the vendor is meeting the expectations as set forth above.

(For additional guidance on selecting a vendor, please refer to ALTA's Best Practices Guidance - Vetting a Vendor: <https://www.alta.org/policies-and-standards/best-practices/>. Also note the requirements when engaging vendors as found within Pillars 2, 3 and 4 of these Best Practices, including analyzing the vendor's use of Artificial Intelligence (AI) and the associated risks.)

4. Defined Term for “Vendor”: With Pillar 7 now being utilized for Vendor Management, it became important to provide sufficient context to determine whether a vendor evaluation should be completed.

Vendor: An entity that sells or provides goods, services, or resources to the Company, with or without a contract or compensation. A Vendor also includes:

1. Third-party providers that offer specialized services, technology solutions, or outsourced operations that support the Company's functions without being directly involved in the core production or delivery process, such as those that process data and host content.
2. AI agents, chatbots, virtual assistants and similar artificial intelligence products even if the Company engages a provider by merely sharing Company data or information, and
3. Social media platforms if utilized for business operations, advertising, data processing, or if the Company is providing the social media platform with PII.

5. Defined Term for “Multi-Factor Authentication”: As this term is utilized in both Pillars 2 and 3, and it was recommended to add additional clarity to understand the requirement.

Multi-factor Authentication: authentication through verification of at least two of the following types of authentication factors:

- (1) knowledge factors, such as a password;
- (2) possession factors, such as a token; or
- (3) inherent factors, such as a biometric characteristic.

6. Include additional requirements in Pillar 3.A. for the planning and implementation of the WISP:

7. Encryption. To the extent feasible, protect by encryption all NPI held or transmitted by the Company both in transit over external networks and at rest.
8. Reasonable monitoring of systems to detect unauthorized use of or access to NPI.

7. Include in Pillar 3.B.4 additional elements of “Preparedness and Training for Threats” within Pillar 3:

4. Establish a training program to guide management and employee compliance with Company’s WISP and awareness of current and developing cybersecurity threats. The program should include annual cybersecurity awareness training and cover social engineering for all personnel.

8. Clarify in Pillar 4.F.3. the responsibility of the Company to vet third-party vendors who monitor and verify third part signing parties

- iv. Company may engage a vendor who assumes the obligation to monitor and verify that the third-party signing professional complies with ALTA Best Practices requirements. Such service providers should be vetted, including the requirements for Vendor Management as described in Pillar 7, to understand any risk of use, security protocols, and the providers’ protection of Consumer data.

9. Clarifying in Pillar 4.G. that for RON transactions, the selection of the platform can require considerations of requirements in the location of both the notary and the property.

- 0.3. If Company will engage a third-party to notarize documents via remote notarization, oversee the selection of the platform in compliance with ALTA Best Practices. If the state in which the property and/or notary public is located has a process and/or requirement to approve remote notarization platforms for the transaction, the selected software platform must be approved by the state(s) as required, and by the Title Insurer, as applicable.

Secondary Document Updates

ALTA Best Practices Assessment Procedures: In addition to the updates to ALTA Best Practices v. 5.0, update to the ALTA Best Practices Assessment Procedures (v. 5.0) were made to align to Best Practices 5.0.

ALTA “Vetting a Vendor” Guidance: There have also been updates made to the ALTA “Vetting a Vendor” Best Practices Guidance (v. 1.01) to specify that a Company should consider being added to the Vendor’s insurance as an additional insured, and to determine whether Company’s own insurance will provide coverage for the actions of a Company’s Vendor.

2. Compliance and Insurance

- a. Obtain assurance from the vendor, and to the extent practical, confirm that the vendor adheres to all applicable laws, regulations, and industry specific requirements such as data privacy laws (e.g., CPRA), consumer protection and cybersecurity frameworks (e.g., GLBA, CFPB), and state specific laws and regulations.

- b. Insurance Coverage:

Vendors: Confirm that the vendor holds adequate insurance coverage, including errors and omissions insurance, crime, cyber insurance, and general liability coverage, as appropriate for the industry and risk presented. **Consideration should be given to being added to vendor’s insurance as an Additional Insured.**

Suggested documents to request and review, as appropriate:

- Certificate of Insurance for errors and omissions, general liability, crime, and cyber security.
- Proof of compliance with industry standards, such as ISO certifications and SOC-2 compliance.
- Any other certificates or licenses that they have.
- Proof that they are authorized to operate in your state, if licensing is required.

Company: Review your Company insurance coverage to address claims that may arise due to actions of the Company’s vendors.

Goal: Ensure that the vendor you select is compliant and that if something were to go wrong, the vendor has the necessary coverage to support their customers.