Best Practices:
Review of 2023 Framework (v 4.0) Changes

OVERVIEW

- Overview: 2023 ALTA Best Practices v 4.0 Revisions
- What Objectives have Changed?
- Which Content has Changed?
- Which Best Practices Resources Have Changed?
- How Do You Certify – and When?
- Process and Timing
- How Can You Prepare?

Overview

2023 ALTA Best Practices v 4.0 Revisions

2023 Best Practices v 4.0 Revisions: Overview

- The World has Changed:
  - New threats: Fraud, Theft
  - Business Has Advanced: RON, Outsourced/Remote workers, more technology
  - Laws Have Changed
- Best Practices Updates Have Focused Primarily on Three Pillars:
  - Pillar 2: Procedures and Controls of Escrow
  - Pillar 3: Written Information Security Plan to Protect NPI
  - Pillar 4: Standard Real Estate Settlement Policies and Procedures
- ALTA is now highly focused on ensuring operational improvements for Agencies

Changes in Objectives

2023 ALTA Best Practices Revisions

First: Why Is Best Practices Important?

- By following Best Practices, including identifying and remediating any deficiencies, Agents are taking active steps to protect the parties and processes of Settlement, which include:
  - Consumers
  - Banks
  - Title Insurers
  - Real Estate Brokers and Agents
  - Their Own Business

Changes to Best Practices Objectives

- Prior versions of Best Practices have focused on compliance certification being provided to Lenders
- Revisions for 2023:
  - Continued Agent Certification to 3rd parties, including Lenders and Title Insurers.
  - New major focus is on continual improvement to operations:
    - Safety
    - Customer Experience
    - Efficiency

Best Practices Framework: Specific Changes

Updates in the "Definitions" Section

Various "Defined Terms" have been updated
to clarify their intent within Best Practices

Escrow: A transaction in which an impartial third-party acts in a fiduciary capacity for all or some of the parties (including the Consumer, or lender) in performing Settlement services according to local practice and custom.

Escrow Trust Account: An account at a Federally Insured Financial Institution utilized to hold funds in trust for a real estate transaction. These funds are held in the account holder's fiduciary capacity as established by written instructions.

Licenses: The various business and professional licenses which are required to conduct the business of title and Settlement services including, but not limited to, Title Agency or producer licenses or registration, escrow/settlement licenses, a license to practice law, and local business operating licenses.

Three-Way Reconciliation: A method for determining whether the three main components of the Escrow Trust Account are in agreement at a regular interval (e.g., monthly, weekly, daily). This process is also used for discovering shortages (whether incidental or intentional), charges that must be reimbursed, or any type of errors or omissions that must be corrected in relation to an Escrow Trust Account. This process requires a comparison of: (1) the Trial Balance, (2) the book balance, and (3) the reconciled bank balance. If all three parts do not agree, the difference must be investigated and corrected.

New Definitions in Definitions Section

Additional “Defined Terms” have been created to clarify intent within Best Practices

Consumer: Buyer(s), borrower(s), or seller(s) in a real estate transaction

Title Agency: Any person, company or entity which is authorized by a Title Insurer to issue title insurance policies. A Title Agency may also perform one or more of the following functions outside of their relationship with the Title Insurer: (1) collect and/or disburse premiums, escrows, security deposits or other funds, (2) handle escrow, Settlement or closings, (3) solicit or negotiate title insurance business, and (4) record documents.

Title Insurer: Any person, company or entity that is licensed to issue and insure title insurance policies

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 “Purpose” section is updated to note that

the loss of funds may fall outside of E&O Coverage, and could fall to the Agency

~~to~~risk of loss of ~~client~~ funds. Loss of funds may not be covered by the Title Agency's Errors and Omissions (“E&O”) insurance or the contract with its Title Insurer. Such losses would then become the responsibility of the Title Agency. Settlement companies may engage outside contractors to

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to address the handling of non-settled funds and avoidance of undue risk (aka, “Wiring off of the float”)

In making disbursements from Escrow Trust Accounts, and subject to state law requirements, Company should ensure that undue risk is not being undertaken for escrow deposits that are not fully settled or that could be reversible.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to address the guidelines for handling Escrow Account Disbursements

Follow state good funds law and Title Insurer requirements/guidelines for Escrow Trust Account individual transaction disbursements.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to control the use of "Fintech" applications

Positive Pay or Reverse Positive Pay are utilized, if available for the payment type, and have policies and procedures in place that prohibit or control the use of Automated Clearing House transactions, international wire transfers, and electronic/digital receipt of funds from web based fintech applications.

… and require that third-party earnest money platforms meet Good Funds law requirements and are not subject to the EFTA

When utilizing a third-party earnest money deposit or disbursement platform that facilitates the digital transfer of Escrow Trust Account receipts and disbursements, ensure that the platform meets any good funds law requirements and is not subject to the Electronic Funds Transfer Act (EFTA) which allows for reversal of consumer payments.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to specify that Wire Transfer Procedures should include Multi-Factor Authentication and follow ALTA's published guidance

For outgoing wire transfers, this includes documented procedures to verify wire transfer instructions independent of the initial communication. Such procedures should include the use of multi-factor authentication and should be similar in nature to those currently cited by ALTA in the Outgoing Wire Preparation Checklist.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to extend the background check refreshes not only to those employees having access to client funds, but to all employees

Background Checks are ~~completed in~~obtained and reviewed during the hiring process. ~~At~~Thereafter, at least every three years, ~~obtain~~updated Background Checks going back five years are obtained and reviewed for all employees ~~who have access to customer funds~~.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to require the review and manager approval of aging Escrow file balances

Outstanding Escrow Trust Account file balances are documented and reviewed from time to time to determine appropriate status or action. Balances older than six months require management approval of activity.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to recommend the use of Wire Verification Services

If available, efficient, and economical, make use of wire transfer verification service providers. Such service providers should be vetted to understand any risk of use, security protocols, and the providers' protection of Consumer data.

Content Changes in Pillar 2 – Escrow Accounting

Pillar 2 Procedures are updated to require that the daily reconciliation process identify and investigate any discrepancies using either electronic or manual processes

On at least a daily basis, reconcile the Escrow Trust Account activities in the bank's records to the activities in the Escrow Trust Account books, identifying and investigating any discrepancies. This activity may be performed electronically or manually depending on volume of items clearing the bank.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 Purpose is updated to include a defined term of “WISP”

3. **Best Practice: Adopt and maintain a written information security plan (“WISP”) and a written privacy ~~and information security program~~plan to protect ~~Non-public Personal Information~~ NPI as required by local, state, and federal law.**

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to protect NPI and Company systems by requiring specific security measures: MFA, Password Management, and Software Updates

Establish ~~a written information security plan~~ and implement a WISP designed to protect ~~to protect nonpublic information in~~ the security and confidentiality of NPI and the security of the Company's ~~possession and detect loss of nonpublic information based on the size and complexity of the Company's operations~~information systems. The WISP should include:

- Multi-factor authentication, if available, that requires multiple credentials (factors) for access to systems containing NPI.
- Password management plan that requires unique login names and system passwords to access systems containing NPI. System passwords must meet minimum standards which include:
  - re-entry of the password after system idling;
  - passwords that expire after a certain period of time;
  - difficult-to-guess passwords that include a combination of uppercase letters, lowercase letters, special characters, with a minimum length of eight total characters.
- Timely software updates that require routine updates to systems, software, and code that, when left outdated, can result in data breaches, cyberattacks, exploits, ransomware attacks and other exposure of NPI.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to require background checks for not only employees with access to NPI, but also to anyone with access to NPI or information systems - including service providers

Physical security ~~of Non-public Personal Information.~~

- Restrict access to ~~Non-public Personal Information to~~the Company's information systems to only authorized employees and authorized service providers who have undergone Background Checks ~~at hiring~~.

- Control physical access to NPI in physical forms, including cabinets, desks, storage, or other areas where NPI exists in any physical or electronic format to authorized employees and authorized service providers who have undergone Background Checks.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to extend network security requirements to the use of cloud systems, virtual equipment, data centers, and 3rd party hosting

Network and cloud security ~~of Non-public Personal Information.~~to protect NPI.

- Maintain and secure access to Company information technology software applications and data stored on physical or virtual equipment at Company location(s), in a data center, in the cloud, or hosted by third-party vendors.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to specifically include in the DR/BC plan instances where there is a compromise of systems or facilities

Establish and periodically test, a written ~~Establish a written disaster management and~~ business continuity and disaster recovery plan outlining procedures to recover and maintain information ~~and~~, business functions~~-~~, and business processes in the event of a disruption or compromise of systems or facilities,

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to include in the DR/BC plan procedures for the continuing of operations for Consumer Settlement and notification of any delays

Establish and periodically test, a written ~~Establish a written disaster management and~~ business continuity and disaster recovery plan outlining procedures to recover and maintain information ~~and~~, business functions ...

...

including continuity of operation for Consumer Settlements, and timely notification of parties in case of any delays.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to require the written response plan to address *any* cybersecurity incident, not just those involving NPI; include periodically testing and follow the recommendations of the ALTA Cybersecurity Incident Response Plan

- Establish, and periodically test, a written incident response plan designed to promptly respond to, and recover from, a ~~breach that compromises the confidentiality, integrity, or availability of Non-public Personal Information in the Company's possession.~~
  - ~~Establish internal and service provider processes for determining the size, nature and scope of any~~ cybersecurity incident~~.~~, which includes all the recommendations of the ALTA Cybersecurity Incident Response Plan template.

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to specify that service provider policies are to be consistent with the Company WISP – including: IT Consultants, outsourcing company employees, and third-party software employees

~~Utilize multifactor authentication for all remotely hosted or accessible~~Select service providers and third-party systems ~~storing, transmitting or transferring non-public personal~~ whose information~~.~~

~~Post~~ security policies are consistent with Company's WISP, including but not limited to:

- Independent contractors and service provider employees who have access to NPI in the course of their work. This group of people may include signing professionals, IT consultant employees, outsourcing company employees, and third-party software provider employees.
- ~~Software tools and resources which may have access to NPI or store records~~

Content Changes in Pillar 3 – Written Information Security Plan

Pillar 3 is updated to specify that software tools and resources are to be consistent with the Company WISP – including: 3rd party software / systems; automated processes; APIs; software add/plug-ins

~~Utilize multifactor authentication for all remotely hosted or accessible~~Select service providers and third-party systems ~~storing, transmitting or transferring non-public personal~~ whose information~~.~~

~~Post~~ security policies are consistent with Company's WISP, including but not limited to:

- Software tools and resources which may have access to NPI or store records containing NPI as part of their setup or operation. These software tools and resources might include third-party software or systems; automated processes for order entry, search, or production; automated or artificial intelligence processes that integrate with other internal or external systems; automated status or communication processes; API data integrations; and software add-ins or plug-ins.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 Description is updated to point to the importance of contractual obligations in the Settlement process

4. **Best Practice: Adopt standard real estate ~~settlement~~ Settlement policies and procedures ~~and policies~~ that help ensure compliance with ~~Federal and State Consumer Financial Laws~~: (i) federal and state consumer financial protection laws and regulations, and (ii) contractual obligations as applicable to the Settlement process.**

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to include “consumer objectives” in the training of staff

~~Review legal and contractual~~ Train staff to provide a framework which will:

- Minimize errors in completing the Settlement.
- Enable a timely response to concerns raised by any of the parties following the Settlement, including addressing Consumer complaints in compliance with the requirements ~~to determine Company obligations to record documents~~of ALTA Best Practices.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to require the disclosure of affiliated business relationships

~~Maintain~~Disclose Affiliated Business Arrangements.

- In compliance with state and federal laws and regulations, establish and implement procedures requiring proper disclosure of any affiliated business arrangements in which Company participates.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to require written procedures related to closing documents

Prepare and execute documents accurately.

- Establish and implement written procedures regarding the preparation and proper execution of Settlement documents. These procedures must comply with state law, federal law, contractual obligations with the Title Insurer, and as contractually agreed to ~~help ensure that third-party signing professionals, including notaries public, engaged~~ by the ~~Company~~ Consumer or lender, and/or as directed by the Consumer or lender.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to expand Best Practice requirements to monitor and verify that signing professionals have state and contractually required licensing and insurance to notarize documents, conduct the settlement, and safeguard NPI

Oversee Signing professionals

- Establish and implement written procedures to monitor and verify that all signing professionals possess the appropriate ~~qualifications, professionalism, and knowledge, including the standards described below.~~state licensing and insurance to notarize documents (both in person and remotely, if applicable), conduct the Settlement (if applicable), and safeguard NPI. These requirements are determined by a mix of legal and contractual obligations, including state regulations and Title Insurer requirements and restrictions.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to address the need to perform Background Checks for signing professionals employed by the Company who either conduct Settlements, or may have access to either Settlement documents or funds

~~Require that third party~~For signing professionals who are employed by Company, establish and implement written procedures to perform Background Check(s) for employees who conduct Settlements or who have access to Settlement documents and funds.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to require third party signing professionals to have the required professional designation, insurance, and bond as required by state law and/or the title insurer

- For signing professionals~~:~~

~~Furnish~~ who are third parties, require demonstrable evidence of their current: state licensure, where required, or ~~evidence if they have attained~~ a recognized and verifiable industry designation, ~~and,~~ E&O insurance and Notary surety bond, if required by state law and/or the Title Insurer.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to address that when a vendor is used to provide a third-party signing professional, the Best Practices obligations may be assumed by that vendor

Company may engage a vendor who may assume the obligations to monitor and verify that the third-party signing professional complies with ALTA Best Practices requirements.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to provide guidance in utilizing Remote Notarization Platforms for employee signing professionals and by third party signing professionals

Selecting Remote Notarization Platforms.

- If Company employees will be notarizing Settlement documents via remote notarization, select a remote notarization platform authorized by the state in which the notary public is located and that is approved by the Title Insurer, as applicable. Ensure that the software platform is capable of meeting the minimum requirements of the state, including retention of the video and safeguarding of NPI.
- Implement procedures to charge fees as authorized by the state regulations.
- 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 is located has a process to approve remote notarization platforms, then the selected software platform must be approved by the state, and the Title Insurer, as applicable.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to provide guidance for the additional procedures to follow when using an e-recording vendor

- If Company will be submitting documents for recording through an e-recording vendor, ensure Company complies with local laws and requirements, and has a contract or agreement in place with the e-recording vendor.

Content Changes in Pillar 4 – Settlement Processes

Pillar 4 is updated to provide guidance in the payment of fees or tax for Escrow Trust Accounts

- Comply with written procedures and controls for Escrow Trust Accounts, including e-recording accounts, containing recording fees and/or any applicable tax that may be imposed by the state or municipality on the recording of documents.

Content Changes in Pillar 6 – Insurance and Fidelity Coverage

Pillar 6 is updated to require that Cyber, Crime, and E&O Coverage limits and exceptions should be reviewed at least yearly

Insurance coverage limits and exceptions, particularly E&O insurance, cyber liability insurance, and crime coverage, change frequently and should be thoroughly reviewed with the Company's insurance broker/agent at least on an annual basis.

Content Changes in Pillar 5 and Pillar 7

No Significant changes to either Pillar

Forms that Have Changed

2023 ALTA Best Practices Revisions

Best Practices Resources that have Changed

- Best Practice Framework: Provides the standards for Best Practices
- Best Practices Assessment Procedures: Testing Requirements
- Best Practices Certification Reports
  - There are now two Certification Reports available:
    - Best Practices Third-Party Assessment Report
    - Best Practices Internal Assessment Report and Letter *(fka "Self-Assessment")*
  - These replace the BP 3.0 Forms: (1) Compliance Management Report, (2) Maturity Model, and (3) Assessment Readiness Guide
- Other Forms
  - Assessment Guide and FAQ Resources
  - Policy and Procedures Creation Guidance
  - Sample Outline / Table of Contents
  - Template for Best Practices Policies and Procedures

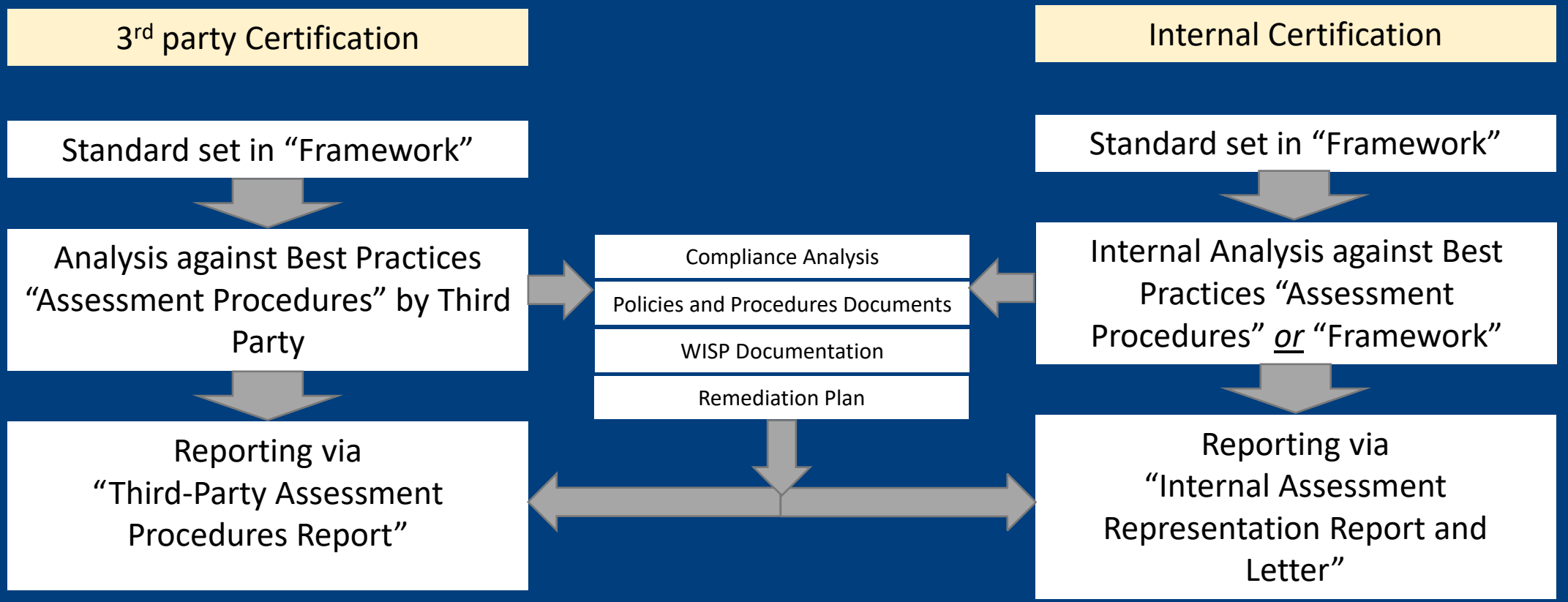
How Do You Certify?

2023 ALTA Best Practices Revisions

Basic Information on Certification

- Best Practices Framework sets the standards for evaluation
- Best Practices provides other documents to assist with the evaluation:
  - Assessment Procedures: Tool for evaluating compliance with the standards
  - Assessment Compliance Reports: Frameworks for evaluating against the Assessment Procedures. Different forms are available for 3rd party and internal assessments.
    - Third-Party Assessment Report: For those Companies certifying via a third-party assessment, this form will be used to provide an analysis against the "Assessment Procedures", providing a certification letter, summary of exceptions, and a list of exceptions with a remediation plan.
    - Best Practices Internal Assessment Report and Letter *(fka "Self-Assessment")*: This form will be used for Internal Assessments to provide an analysis against either the "Framework" or the "Assessment Procedures" providing a certification letter, and a list of exceptions with a remediation plan.
  - Various Policies and Procedures templates
  - ALTA Website for standards used in Best Practices:
    - https://www.alta.org/business-tools/information-security

Basic Information on Certification



How Do You Certify?

- The *"ALTA Best Practices Framework: Title Insurance and Settlement Company Best Practices"* remains the standard
  - Additional ALTA Best Practices documents provide frameworks for analysis and reporting
- ALTA Best Practices Certification of Best Practice Compliance requires:
  1. Analysis against the Best Practices Framework or Assessment Procedures using either one of the Assessment Compliance Reports* or other method, so long as the written report contains an analysis of requirements against the following attributes:
     i. Current status of compliance for each Framework or Assessment Procedures requirement
     ii. Whether compliance is documented for the requirement
     iii. Whether remediation needs to occur for the requirement
     iv. Plan for remediation to achieve the requirement
     v. Who completed it / Third-party vs internal assessment

     * *Multiple previously available reporting documents are being consolidated to two documents – one for internal assessments and another for 3rd party assessments/certifications.*
  2. Documentation of Policies and Procedures, including WISP. These documents may be requested by entities requesting Best Practices Compliance information.
  3. Certification by Company of compliance status.

Process and Timing

2023 ALTA Best Practices Revisions

Process and Timing

- Publication of 2023 Best Practices 4.0 Revisions: January 23, 2023
  - Announced in Title News Online, and at: https://www.alta.org/best-practices/
  - Site will contain revised Framework and Assessment Procedures, along with other documents
  - Questions may be submitted to: bestpractices@alta.org
  - FAQs will be updated as questions are submitted
- Effective Date of 2023 Best Practices Revisions: May 23, 2023
  - Provides time for analysis, updates, and process changes before standards take effect
  - But Companies may utilize Best Practices 4.0 at any time after Publication on January 23, 2023
- Certification timeline:
  - Entities performing Best Practices certification are current for 24 months from certification
    - Example: Certification in June 2022 on 3.0 standard is thus certified until June 2024
  - *However*… Best Practices 4.0 (2023) is designed to improve operations, and should be used as the guide even prior to official certification on 4.0.

How Do You Prepare?

2023 ALTA Best Practices Revisions

How Do You Prepare

- Assign primary responsibility for certification
  - Information Collection – What has changed; how do we align to the standards
  - Use the ALTA Best Practices FAQs to resolve questions
- Determine your method for certification – internal vs. third-party
- Determine mandatory certification timeline: 24 months from prior certification
  - But it is recommended to work toward the new standard ASAP
  - Doing it now helps you safeguard and improve your operations
- Use resources: title insurer, webinars, Best Practices documentation
- Assume that Best Practices is an ongoing process which needs to be periodically reviewed and processes updated

Thank you for all of your work…

- The Best Practices Executive Committee has spent the past year (plus) intensively working to update the ALTA Best Practices standards to provide the revised structure for improved title operations.
- Other ALTA groups, including the Best Practices Work Group, the Internal Audit Council, the Data Privacy Work Group, and the providers of industry comments, have all contributed to provide their feedback and expertise.
- This large investment of time, effort, and thought has been in addition to their “day jobs”… and we would like to say:

THANK YOU!

Questions?

Submit Questions to:

BestPractices@alta.org

Updates to Information:

https://www.alta.org/best-practices