ALTA BEST PRACTICES GUIDANCE – VETTING A VENDOR

VERSION: 01.00
PUBLISHED 08-19-2025

ALTA Best Practices Executive Committee
And Workgroup

Contents

Summary – Purpose of this Guidance

As the use of vendors offering both "best of breed" and integrated technology and service solutions that provide operational efficiencies and safety has become an important part of title operations, the process of selecting the vendors is a critical, but often overlooked aspect of business operations and is not without risks:

- Will the vendor solution actually fulfill the needs? Sales promises can differ from operational delivery, and analysis of what is actually provided and having that reflected in the terms of the agreement is important.
- The stability of a vendor solution can be an operational risk – if the system is not available, that may significantly impact the business. The stability of the vendor and well-designed systems with failover availability can be critical aspects for systems that are operationally important.
- Data is often being entrusted to the third party – and proper analysis of the permitted disclosures and risks of exposure becomes important. Don't overlook the risks of disclosure of data through the use of AI and accidental inclusion in the underlying data model.
- Outside of awareness of payment terms, the contractual terms are often not fully apparent until things go wrong: the contractual terms are an important part of where you manage risks. We all know the payment terms for our vendor relationships, but if the vendor relationship sours or a breach of responsibility occurs, it's important to know, among other things:
    - the term of the agreement and renewal provisions,
    - delivery and performance guarantees,
    - early termination triggers and provisions,
    - liability provisions,
    - handling and ownership of sensitive data,
    - how disputes are handled, and
    - whether there is vendor insurance coverage to provide recovery in case things go significantly wrong.

ALTA Best Practices has continued to implement and update the requirements to address risks and threats to the real estate industry. In support of these changes, ALTA is providing this document to support an in-depth analysis of third-party vendors so a Company can manage risk. ALTA understands that no document or approach will eliminate all vendor risk, but continued efforts to mitigate risk are critical to assure the continued operation of your Company.

This Guidance outlines some of the approaches that can be utilized but does not set a minimum standard or requirement for what analysis to utilize. In addition to your own due diligence, we recommend guidance from technology experts and attorneys to ensure your selection process and the contractual terms are well suited to the requirements and complete. The amount of investigation that your Company decides to perform on a vendor will vary depending on the role the vendor will play, the criticality of the product or service, any exchange of information or data between your Company and vendor, and the

proprietary nature of the information. Your Company will need to determine the nature of vendor relationship and the amount of vetting that is appropriate.

Topics of Inquiry:

1. Vendor Qualifications and Experience

a. Industry Experience: Evaluate how long the vendor has been in business and their track record within the industry. Confirm that they have successfully served clients with similar needs or in similar sectors.
b. References and Reviews:

- Consider obtaining references from previous or existing clients to understand their experiences, focusing on service quality, responsiveness, and overall satisfaction.
- Use third-party review platforms and services like the Better Business Bureau to gather additional insights.
- Conduct online searches to uncover any news articles or mentions that could indicate the vendor's reliability or any past issues. This includes checking for negative reviews or complaints.
- Check for any CFPB complaints or other locations for civil or criminal action against the vendor.

Goal: Gain comfort knowing this vendor has a strong reputation for supporting other companies in the industry or similar sectors.

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: 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.

   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.

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.

3. Financial Stability

a. Assess the financial strength of the company by evaluating length of time in operation, business growth, and financial reports, if available, and request a Dunn and Bradstreet number. If financial reports are not available, request proof of stability to mitigate risk associated with vendor solvency.

Goal: Make sure this vendor has the financial stability to support you and won't end up causing business disruptions due to inadequate finances.

4. Service Quality and Reliability

a. Performance Standards: Assess whether the vendor can meet the scope/functionality, scale, and timeline of requirements. Work internally first to determine your needs and requirements before asking a vendor to assess the fit of their product or service to your needs.
b. Understand the onboarding process, the expenses associated, and what will be required from your team. If changes are needed, what will that cost and how will it be delivered?
c. Request SLAs (Service Level Agreement(s)) to define performance standards, response times, and penalties for non-conformance.
d. Problem Resolution: Ask how the vendor handles disputes or challenges that may arise during a transaction.

Goal: Gathering these details upfront can help you set expectations contractually to ensure you get the service required to support your business.

5. Technology and Innovation

a. Evaluate the vendor's use of technology, tools, and platforms to ensure that they align with your needs, and that the technologies employed are up to date.
b. Ensure that the vendors and any sub-vendors employ secure systems to protect data and privacy, especially if handling sensitive, NPI, PII, or proprietary data.
c. Determine if the vendor updates their products, services, and processes to adapt to industry trends, customer needs, and security protocols, and whether they have a commitment to innovation, continual improvements, and adherence to security guidelines, and security of sensitive, NPI, PII, and proprietary data.

Goal: When you select a vendor, consider the impact they may have on your business for many years to come. How they are managing their business and security today is a good indication of how they will manage it moving forward.

6. Data Security & Privacy

a. What security certifications do they hold (e.g., SOC 2 Type I / Type II, ISO 27001)?
b. How do they protect NPPI?
c. What is their data breach notification procedure?
d. Security Penetration Testing – request evidence that regular network/system venerability and penetration testing is occurring.
e. Confirm that the vendor has disaster recovery and business continuity plans and, as appropriate, request additional details to ensure that the vendor can promptly recover and maintain operations during unforeseen events.
f. If the vendor uses subcontractors, services, or technology providers for any of their services, confirm that the vendor vets their subcontractors and providers to the same compliance and quality standards as the vendor applies to their own to data security, system stability, compliance, and operational continuity standards.

Goal: Security and privacy have never been more important. Confirm vendors maintain safe data security and privacy practices and protocols to keep your business safe.

7. Wire Fraud Prevention (where applicable)

a. What specific controls do they have to prevent wire fraud?
   (1) Confirm process for verifying authenticity of wire instructions, including but not limited to independent call back verification.
   (2) Review policies and procedures for validating wire instruction changes including verification protocols.
   (3) Verify whether all changes are confirmed using a secure and documented method.
   (4) Confirm whether they are using AI-based advanced fraud detection or pattern recognition.
   (5) Document vendor's staff training on fraud prevention
   (6) Describe frequency of training and whether scope includes both ongoing and emerging threats.
   (7) Determine whether training covers responding to wire fraud incidents, and whether it includes simulated fraud attempts.
b. Have they experienced any wire fraud incidents? Is there insurance coverage if there is an incident?

Goal: Wire fraud is one of the leading causes of loss of funds. Ensuring that not only are your operations taking the necessary steps to prevent wire fraud, but that your vendors are providing adequate protection and coverage(s) is critical to your business.

8. Contractual Considerations

a. Contract Terms: Review contract terms carefully and engage counsel as needed to ensure the contract includes sufficient clauses related to (among others) indemnification, termination rights, confidentiality, compliance with industry standards, and that such protections extend to the actions or inactions of subcontractors. Sales statements do not equate to contractual guarantees.
b. Ensure that vendor requirements for performance and data protection are also reflected in contractual terms. Again, sales statements do not equate to contractual guarantees.

Goals: Vendors may promise a lot during the sales process, so make sure those promises are included in the contract and that you have the right to terminate, litigate, and/or recover if they aren't met.

9. AI Inquiries

There are multiple forms of AI, the most discussed and utilized recently being Generative AI. However, this questioning should not be limited to Generative AI, as other forms of AI can also use inputs to their modeling. These might be machine learning or neural networks, among others. Some considerations may include:

a. Is the vendor providing or using Generative AI as part of their process? For what purposes?

b. Is the vendor using your company data within their AI process?

c. Is the vendor using your data for training the Generative AI models?

d. Is the AI being used for decisioning or pricing?

e. Does the vendor share your data with any form of Generative AI?

f. What other forms of AI or model building is the vendor utilizing? Is your data used in any of those models?

g. Do the privacy policies and standards utilized in the use of the AI align with your Company's privacy policy standards?

Goals: Vendors may be putting your data at risk by their use or provision of AI tools or third-party services. It is important to understand how your data is being utilized and exposed so you can determine whether a solution introduces risks of disclosure.

Red Flags to Consider

1. Reluctance to provide documentation and clear, written procedures regarding wire fraud prevention or incident response handling
2. Inadequate or lapsed insurance coverage(s)
3. Poor or no references
4. Unclear pricing structures
5. Weak security protocols
6. Limited disaster recovery capabilities
7. High staff turnover
8. Outdated technology or lack of commitment to continual improvement
9. Unresponsive customer service or limited support hours
10. Limited industry experience
11. Lack of security certifications
12. No multi-factor authentication
13. Weak wire fraud controls (where applicable)
14. No regular security assessments
15. Lack of alignment of the proposed contract to the delivery and protections promised during the sales process

Additional Resources

Forbes - https://www.forbes.com/councils/forbestechcouncil/2023/04/04/16-key-considerations-when-vetting-a-new-tech-vendor-or-partner/

Kirkpatrick Price - https://kirkpatrickprice.com/blog/vendor-due-diligence-checklist/#

ALTA Webinar: Let's Go Shopping For Tech: https://www.youtube.com/watch?v=SPBDqnRfJvg

CFPB Complaints Search: https://www.consumerfinance.gov/data-research/consumer-complaints/search