CANOE

CHECKLIST FOR ALTERNATIVE INVESTORS

8 Critical Considerations for Prioritizing Data Security in a Vendor Evaluation

www.canoeintelligence.com

Checklist: 8 Critical Considerations for Prioritizing Data Security in a Vendor Evaluation

As an alternative investor, the strength of a cybersecurity program is especially crucial as you are typically dealing with sensitive, confidential documents and data. Without proper security measures in place, there is a risk of data or documents being lost, accidentally deleted, or shared with unauthorized parties. The fallout can be significant, leading to larger challenges, including permanent data loss, interrupted business operations, and reputational damage.

This checklist identifies the types of security vulnerabilities alternative investors deal with when working with technology vendors and how to properly manage these risks.

1. Access Controls

- **What controls does the vendor have in place to limit who can access data?**
- **Do these include multi-factor authentication and role-based access controls?**

This can help prevent data leaks or insider threats, where employees intentionally or unintentionally misuse or leak sensitive information.

2. Authentication

- **How many layers of authentication are in place to protect unauthorized access to your data?**

Vendors that do not implement multi-factor authentication increase the risk of unauthorized access to client accounts, resulting in financial loss, data breaches, and reputational damage to the company.

3. Compliance with Security Standards

- **Has the vendor detailed their governance strategy and compliance with industry-standard security certifications?**

A vendor's compliance with industry-standard security certifications, such as SOC2, ISO 27001, or PCI-DSS, indicate that they have undergone rigorous security assessments and are following best practices for protecting data.

4. Encryption

- **What encryption methods does the vendor have in place to protect data in transit and at rest?**
- **Do these encryption methods include data in storage and during transmission over networks?**

If a vendor has weak encryption or no encryption at all, hackers can potentially intercept sensitive data, such as passwords or financial statement data. This can lead to financial fraud or other forms of cybercrime.

5. Regular Security Assessments

- **How often does the vendor undergo security assessments?**
- **How comprehensive is their testing and review process?**

Vendors should undergo regular security assessments to identify and address any vulnerabilities in their systems and processes. This includes regular penetration testing, vulnerability scanning, and security audits.

6. Contractual Agreements

- **What does your contract state regarding the vendor's responsibilities to you in terms of data protection and security incident response?**

In your contract, vendors should outline their responsibilities for protecting data and response to a breach or other security incident. These agreements should also include provisions for regular security audits and assessments.

7. Logging, Monitoring, and Alerting

- **What proactive steps does the vendor take to monitor and manage suspicious activity?**

Security information and event management (SIEM) tools are recommended to collect and consolidate alerts from security tools and critical infrastructure into manageable and actionable information. Without log retention and access, the vendor is at risk of losing logged information in the case of a security event.

8. Incident Response

- **How will the vendor plan to respond to a security incident or data loss?**

A well-defined security incident response plan should outline the steps the vendor will take to discover, contain, investigate, and remediate a security or data loss incident. Vendors that lack rigorous monitoring and auditing procedures may not be able to detect or prevent suspicious activity on their platform, leading to cyber attacks, data breaches, and other forms of security incidents that can damage client trust.

Next Steps

The merits and consequences of implementing or not implementing a strong security infrastructure are clear. In summary, poor security standards can have serious consequences for both financial technology companies and their clients, including financial losses, data breaches, reputational damage, and legal liability. It's extremely important for companies in this space to prioritize security and take all necessary measures to protect their clients' sensitive information. Document and data management applications need to prioritize the protection of sensitive information, control access to their data, and comply with relevant regulations.

How Does Canoe Stack Up?

Our philosophy is that client data in the Canoe should be even more secure than it would be in the client's ecosystem. Canoe has over 200 clients that trust us with their sensitive information. We take that responsibility very seriously and, thus, have implemented multiple layers of protection to ensure the safety and privacy of that data.

Canoe's Technology Leadership Team (TLT) consists of six experienced individuals who also frequently consult with expert industry advisors. The technology organization is designed to promote collaboration while balancing separate concerns, enabling Canoe to deliver a thoughtfully-designed, secure, and useful product to our customers.

1

Access Controls

- **Principle of Least Privilege:** Canoe deploys the principle of least privilege access for our client-facing platform, and we review that access on a periodic basis.
- **Role Permissions:** Our cybersecurity measures ensure that only authorized individuals have access to data, and authorization permissions can be defined on a role-by-role basis.

2

Authentication

- **Secure Encryption via HTTPS:** To protect our client-facing SaaS platform, users can only access it over HTTPS.
- **Multi-Factor Authentication (MFA):** We leverage industry-standard security measures, such as MFA, authentication/authorization modules, password complexity enforcement, IP filtering, identity federation, and user access groups for controlling feature and data access.
- **Session Timeouts:** User sessions timeout after 30 minutes of inactivity, and the session ID is not part of the application URL.
- **Credentials:** Our clients are required to provide a username and password, as well as an MFA code, in order to access their accounts.

3

Compliance with Security Standards

- **Systematic Reviews:** Canoe systematically reviews the state of our technology with the help of external parties. Like most financial firms, we undergo an annual SOC2 type 2 audit to validate the controls we have in place to safeguard customer data, such as periodic internal testing.

4

Encryption

- **Advanced Encryption Algorithm:** Canoe uses advanced encryption technology to protect all data transmission between our servers and our clients' devices. This means that any data transmitted over the internet, including login credentials and financial statement data, is protected from hackers and other cyber threats. Canoe encrypts data in transit and at rest via an encryption algorithm.
- **Application-Only Access:** Canoe does not make documents or sensitive data available in email notifications because email is not always secure or encrypted. We only allow access to sensitive data or documents in the application itself, where we can control their security.

How Does Canoe Stack Up?

5

Regular Security Assessments

- **Testing and Assessments:** Canoe employs industry-leading tools for cloud infrastructure vulnerability scanning, annual security testing, network penetration testing, web application penetration testing, and AWS security configuration assessments.
- **Cybersecurity Programs:** Canoe participates in Blackstone's portfolio company Cyber Security program and meets with their portfolio cybersecurity team on a monthly basis to review our security posture.
- **Due Diligence Processes:** For other clients and prospects, we have gone through very stringent tech and security diligence processes. These clients and prospects happen to be among the most sophisticated cybersecurity-focused firms within the financial industry.

6

Contractual Agreements

- **Provider and Supplier Requirements:** Canoe requires our third-party suppliers to follow industry standard compliance and regulatory strategies and certifications. As a provider, Canoe supplies SOC2 certification and outlines protection, privacy, and incident response requirements

7

Incident Response

- **Security Incident Response Plans:** Canoe has a well-defined security incident response plan in place to ensure preparedness in the event of a security breach or other data loss incident.
- **Monitoring and Auditing Procedures:** We have implemented rigorous monitoring and auditing procedures to detect and prevent any suspicious activity on the platform. This includes real-time monitoring of user behavior, as well as regular security audits to ensure that our systems are up-to-date and secure.

8

Logging, Monitoring, and Alerting

- **Proactive Detection:** Canoe uses world-class tools to proactively detect and address issues before customers are impacted.
- **Comprehensive Audit Trail:** All actions by authenticated users are logged, ensuring you have a complete historical audit trail.
- **Cybersecurity-Focused AWS Configurations:** Our AWS instance is configured to ensure cloud configuration drift is prevented, and we employ a number of different tools to support logging, monitoring, and alerting, including those for detecting and troubleshooting application errors, infrastructure logging and monitoring, analyzing application and infrastructure logs, and intrusion detection and prevention.

Powering Alternative Investment Intelligence

While document and data management is vital, it does not drive scale, boost performance, or differentiate your firm. Automating these tasks does. With Canoe, you can separate your firm from the rest and immediately drive client value. Free your team from alternatives document collection, data extraction, and data delivery. Gain deeper access to data. Generate investment insights with more confidence.

200+ Alternative Investors are Fortifying Their Firms with Canoe

By introducing automation to alternatives document collection and data management workflows, institutional investors, wealth managers, and general partners are seeing dramatic improvements in data accuracy and access, team efficiency, and client satisfaction.

94%

ROI on time spent collecting documents, from 18 hours to 1 hour per month

20x

increase in the number of funds processed by each employee

100+

technical integrations for downstream reporting and analytics workflows

98%

reduction in time spent reconciling administrator documents, from 13 hours to 15 minutes

How Does Canoe Intelligence Work?

Canoe automates the collection and categorization of alternative investment documents from 250+ GP and administrator portals, extracts and validates the relevant data elements from those documents using shared intelligence from 25,000+ funds, and ultimately delivers clean, actionable data to our clients' downstream systems.

Why Leading Alternative Investors Choose Canoe

Achieve Operational Efficiency. Serve Clients More Confidently. Scale Business Growth.

Pioneers in Alternatives Technology

Canoe is purpose-built for industry experts by industry experts. Our experience and know-how drives our ability to successfully automate every manual task related to alternatives document and data management.

Shared Intelligence

When clients use Canoe to automate their alternatives data management, they are actively contributing to a stronger and more connected industry. The data within every new fund document introduced is mapped, speeding onboarding and improving data extraction accuracy.

The Alternatives Ecosystem

Whether it be connecting with GPs and portal providers to automate document collection or integrating seamlessly with reporting systems to streamline analysis, Canoe's ecosystem elevates the practice of alternative investing for all.

Backed by Innovators

From clients to investors to partners, our network is full of industry changemakers who are united in advancing the state of alternative investments and trust Canoe to power the evolution.

Automate your alternatives document and data work with Canoe.

SEE CANOE IN ACTION