1847Financial | HTK

A SOC 2 report is a useful report to understand the control environment of a vendor or service provider. This reference guide is designed to provide a brief overview when reading a SOC2 report.

What is a SOC2 report?

A SOC 2 (System and Organization Controls 2) report is a comprehensive document that provides detailed information about a service organization's (vendor's) controls and processes related to security, availability, processing integrity, confidentiality, and privacy. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA).

The SOC 2 report is often requested to assess the effectiveness of a service organization's internal controls and security measures. It is typically prepared by an independent third-party auditor who evaluates the organization's systems, policies, and procedures to ensure they meet the defined criteria.

The report includes detailed descriptions of the organization's control environment, risk management processes, and the effectiveness of controls in place to safeguard customer data and ensure the reliability of services. It provides assurance to stakeholders that the organization has implemented adequate controls to protect their interests and meet regulatory requirements. SOC 2 reports are valuable tools for demonstrating transparency, accountability, and trustworthiness in service organizations.

To learn more: https://www.venminder.com/blog/when-request-vendor-soc-1-vs-soc-2-report

Some questions you can ask if a SOC2 report is not available:

When a SOC 2 report is not available, there are several key questions you can ask to gather information about the vendor's security practices and controls:

1. Security Policies and Procedures:
   - Can you provide documentation outlining your security policies and procedures?
   - How do you protect sensitive data from unauthorized access or disclosure?
2. Data Protection Measures:
   - What measures do you have in place to secure customer data?
   - How do you ensure the confidentiality and integrity of data stored on your systems?
3. Availability and Disaster Recovery:
   - How do you ensure the availability of your services?
   - Do you have a disaster recovery plan in place, and if so, how is it tested and maintained?
4. Processing Integrity:
   - How do you ensure the accuracy and completeness of data processing?
   - Are there controls in place to detect and prevent errors or irregularities in data processing?
5. Confidentiality and Privacy:
   - How do you protect the confidentiality of customer information?
   - What measures do you take to comply with privacy regulations, such as GDPR or HIPAA?
6. Third-Party Security Assessments:
   - Have you undergone any independent security assessments or audits?
   - Can you provide evidence of compliance with industry standards or regulations?
7. Incident Response and Breach Notification:
   - What procedures do you have in place to respond to security incidents or data breaches?
   - How do you notify customers and stakeholders in the event of a security incident?

HTK

By asking these questions, you can gain insights into the service organization's security practices, risk management processes, and commitment to protecting customer data, even in the absence of a SOC 2 report.