BBH SOLUTIONS

What Goes Into a Vendor's SOC 2 Audit?

AN OVERVIEW FOR REGIONAL BANKS

SOC-2, or Service Organization Control 2, is a measure of your service organization's controls as related to security, confidentiality and processing integrity of information. It is considered one of the baselines in security compliance for financial institutions' vendors and third parties.

To understand what goes into a SOC-2 audit, it's important to understand some of the requirements service providers must follow to obtain and maintain SOC-2 certification. Keep reading to learn more about the requirements for certification, why your vendors should be SOC-2 compliant and what is reviewed during a SOC-2 audit.

01

What Is SOC-2 Compliance, and How Is It Maintained?

To become SOC-2 compliant, a service provider must be measured by an auditing agency on the effectiveness of well-documented security policies and standard operating procedures. These must be in place related to the **5 Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy.** These categories comprise the five pillars of SOC regulations.

To stay SOC-2 compliant, the service provider must develop a baseline of how they expect their support systems – and, if applicable – cloud environment to function daily with reporting capabilities that measure anomalies within the baseline. These anomalies can range from inappropriate access of data by under-privileged internal resources to phishing attempts from outside the organization.

Continuous security monitoring platforms are the easiest way to detect when abnormalities occur. Your service provider's reporting solution should be set up to administer alerts as soon as an out-of-spec issue is detected. Exposure or modification of data, controls, or configurations within the environment, file transfers, and abnormal user account access are all examples of alerting triggers. Part of any financial institution's responsibility is performing a Due Diligence effort on each vendor. Having a SOC-2 compliant service provider makes that Due Diligence process much simpler.

02

Why Your Vendors Should be SOC-2 Compliant

Financial institutions themselves are not required to be SOC-2 compliant, but are responsible for ensuring their service providers meet criteria that align with SOC-2 standards, according to the Federal Financial Institutions Examination Council (FFIEC). Service providers that support a financial institution or store the business data of a financial institution in the cloud are not required to be SOC-2 compliant. However, retaining a compliant service provider goes a long way with regulatory entities and speeds up the vendor due diligence process.

According to **FFIEC guidelines**, there are certain standards all financial institutions are required to adhere to, including the following:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

This, by proxy, also applies to any vendor responsible for hosting or maintaining the business data of a financial institution, i.e., managed service providers. These providers must be held to similar standards in order for financial institutions leveraging them to adhere to the regulations set forth by the FFIEC and the **Consumer Financial Protection Bureau (CFPB)** relative to federal consumer financial law. The best way to ensure that service providers are abiding by these regulations is to obtain and review their SOC-2 report.

03

What Goes Into a SOC-2 Audit

Service providers are responsible for selecting the Trust Services Criteria that pertain to their particular business. A provider does not need to adhere to all five; however, it is recommended that a provider supporting a financial institution adhere to at least the security and confidentiality criteria.

The audit itself is conducted by an accredited **AICPA** auditing firm experienced in SOC compliance. They review the Service Description and controls of each service provider and determine whether their control measures fit the criteria of SOC compliance. They will take into consideration all Trust Services Criteria the vendor reports and measure it against their stringent guidelines.

Data Management

One of the most heavily weighted aspects of a SOC review for service providers representing financial institutions is data management.

There are three categories that the auditor will focus on during the evaluation:

1. The preservation of electronic records.
2. The retention period for which this information is stored.
3. Tracking of changes to the system.

The remainder of the audit will address:

- The security of the systems housing the data.
- Confirmation that information is readily available to clients when they expect it to be.
- How confidential information is protected.
- Verification that the information intended to be kept confidential is kept that way.
- Verification that data is processed in the agreed-upon ways, with incident control measures, access policies, etc.

04 Final Thoughts

Because many financial institutions are outsourcing data storage, data management and IT services, the vendors they use are essential to ensuring that they remain compliant with all federal banking regulations. Partnering with a SOC-2 compliant service provider will allow you to focus on your core business initiatives, rather than spending time continuously verifying that all of your business data systems meet industry standards and going through lengthy and potentially questionable due diligence verification of non-SOC compliance vendors.

About BBH Solutions

BBH Solutions is a New York City-based managed service provider that specializes in Security and compliance support for regional banks in the Tri-State area and beyond. We offer compliance support either as a stand-alone service or as a part of our complete managed services offering.

Our team of experts is committed to providing best-in-class support while keeping all of your critical business data and applications secure. Our cloud offerings put security first, so you can rest assured knowing that, when it comes time for an audit, your IT systems are covered.

If you are approaching an audit or have areas of concern regarding your audit-readiness test results, download our IT Audit Remediation Plan for Regional Banks.

Get the IT Audit Remediation Plan

If you're interested in learning more, **contact us** to speak with one of our specialists today.