Cybersecurity Compliance Audit Guide

Appropriately vetting vendors before selection and then overseeing the vendors during the course of their service to monitor their privacy and security practices is an important component of an organization's security program. Vendors often state that they have implemented certain security measures to obtain your business, but how would your organization know if this was true before it was too late? Organizations should consider including certain provisions in vendor contracts that would require the establishment of written information security policies, implementation of certain technical security measures, and the right to audit to verify compliance. Specifically, we recommend that you think through the following when discussing the information security programs and measures required of your vendors.

1. **Vendor Information Security Programs** – Your organization may consider requiring a vendor to establish a written Information Security Program that can be measured against a standard that your organization is comfortable and familiar with. This can be done by requiring a vendor to comply with a recognized information security standard or a standard established by your organization. Depending on the relationship with the vendor, your organization may consider reviewing the vendor's written program prior to or during the engagement. Below are some security standards to consider when evaluating a vendor's Information Security Program:

   a. NIST Cyber Security Framework – General standards, guidelines, and best practices to manage cybersecurity- related risk.
   b. NIST Small Business Information Security: The Fundamentals – Information Security guide tailored to small businesses with developing security postures.
   c. COBIT 5 – Suitable to evaluate a vendor's Information Security Program at a point in time.
   d. ISO 27001 – Requires yearly certifications and evaluation. Best for mature programs.

2. **Technical Requirements** – As part of the vendor's Information Security program, your organization may consider requiring vendors implement certain technical features to protect your data. You may want to consider requiring the following measures depending on the vendor's size and role with your data:

   a. Intrusion Detection/Prevention Systems – Network monitoring for malicious/suspicious activity.
   b. Data Loss Prevention Systems – Detect and prevent data exfiltration through real-time monitoring.
   c. Security Information & Event Management System – Real-time analysis of security alerts generated by network applications and devices.
   d. Encryption of data in transit & at rest – Best practice for transmission and storage of data.
   e. Multi-Factor Authentication – Protect remote access and email accounts in the event of a compromised password.
   f. Anti-Virus/Malware Deployment – Protect systems from known viruses and malware.
   g. Patch Management System – Ensure all systems receive critical updates to patch vulnerabilities.
   h. Cloud configuration – Ensure permission settings for any cloud services that are used are securely configured.

3. **Audit Rights** – Certain considerations need to be taken when demanding or conducting a vendor information security audit. Some of those considerations for your organization are as follows:

a. Will the audit be conducted by the vendor, a third-party, or resources at your organization?
b. What will be within the scope of the audit?
    i. Physical and/or technical audit?
    ii. Certain network segments that deal with your organization's data?
    iii. Perimeter or internal security?
c. Outside of a full audit of a vendor's Information Security Program, will the vendor be required to conduct periodic risk assessments or penetration testing?
d. For vendors that access or process sensitive data, will your organization require a third-party to certify compliance with recognized standards (e.g., PCI DSS, ISO 27001 or SOC 2, Type 2)? If so, require the vendor to provide you with evidence of compliance annually.