COMPASS
CYBER SECURITY

THIRD-PARTY VENDOR DUE DILIGENCE

An organization's level of cyber security is only as strong as the security of its vendors, creating a weakest link dependency. Is your organization preforming the proper due diligence on third-party vendors? COMPASS provides comprehensive questions to ask when engaging with these third-party vendors as their risk should be incorporated into your cyber security program.

QUESTIONS TO ASK THIRD-PARTY VENDORS

Who is accountable for safeguarding your data?

Even when your data is being hosted by a 3rd party, you are likely still responsible for keeping it secure. Ask your vendor for a list of responsibilities of the vendor and the customer so it is clear what each party must do to safeguard your data.

What safeguards does your vendor have in place to protect your data?

Ask your vendor if they perform security best practices such as IT Vulnerability scans, employee training, security monitoring, etc.

Does your vendor host your information internally or through another third-party?

Many vendors rely on additional service providers to host their data. It's important to know where your information will be stored and who is responsible for safe-guarding it.

Does your vendor have a security risk management plan?

Your vendor should be willing to provide a SOC Type 1 or SOC Type 2 report that outlines what they do to protect your data. Some vendors even provide executive summary reports with the findings from their security tests.

Does your vendor allow routine check-ins?

Protect your institution's interests with a strong contract that specifies key performance measures, service-level agreements, and benchmarks. This should include the right to conduct on-site visits to the third-party vendor and the right to audit, accept or reject the work product. Require remediation if there are deficiencies.

THIRD-PARTY VENDOR STATISTICS

- 75% of Senior Executives and Board Members believe third-party risk is serious.
- 63% of breaches were traced to third-party vendors.
- Only 29% of organizations indicate they have a formal third-party risk management program in place.
- Only 26% of respondents believe that their organization's third-party risk assessment of controls is effective.

For more information, please contact info@compasscyber.com or 667-401-5108.

VOSB

MEMBER OF NBOA

COMPASSCYBER.COM