How to vet technology providers

Introduction

Milou Lammers, J.D.

- UR Law Class of 2015
- Compliance Manager, iland Cloud

Context

My team answers between 500 - 1,000 due diligence questions per month from customers about our compliance & security measures as a technology provider. I'd like to share questions you should considering asking & what to look for next time you are conducting vendor due diligence on a technology provider.

Topic Areas to Focus On

- Compliance Program
- Compliance Documentation
- Business Continuity & Disaster Recovery
- Incident Management
- Vendor Management

Questions to Ask:

Compliance Program

- Do you have a dedicated compliance program?
- How do I reach the compliance program if I have a question?
- How large is your compliance department?
- Does your organization have an individual responsible for information security? If so, who?
- How many team members support your organization’s compliance & security requirements?

Documentation to Ask For:

Information Security Compliance Documentation

- AICPA SSAE 18 SOC 2 Type II Report
- ISO 27001 Certificate
- Cloud Security Alliance STAR CAIQ
- Penetration Test Results Summary
- Information Security Policy, Data Destruction Policy, Third-Party Management Policy
- Industry specific documentation (HIPAA compliance (HITRUST report), NIST 800-171 self-assessment, CJIS report, etc.)

Questions to Ask:

Business Continuity & Disaster Recovery

- Request a copy of the vendor’s Business Continuity Response Plan (BCP)
- How frequently is your BCP tested? When was it last tested?
- Do you have a summary or report we can view of your most recent BCP?
- What Disaster Recovery (DR) strategies does your organization have in place?
- Does the BCP meet your SLA requirements such as RTO and RPO?

Questions to Ask:

Incident Management

- Ask about the vendor's incident management program
- Is the incident management program is tested at least once a year?
- Under what circumstances will our organization be notified in the case of a breach? What is the definition of a breach?
- Who will be contacted in the case of a breach & how?
- How soon will we be contacted in the case of a breach?
- Can this breach timeline be contractually determined?

Questions to Ask:

Third-Party Vendor Management

- Ask about the vendor's third-party vendor management program
- What vendors they utilize generally and which ones may have access to your organization's data
- Ask how about their vendor due diligence processes & vendor risk assessments

Questions to Ask:

Third-Party Vendor Management

- Confirm that they have contractual agreements in place with their critical vendors including confidentiality agreements
- Ask to review their critical vendors' compliance documentation (such as a SOC 2 or ISO 27001 certificate)
- Ask how & when they will notify your organization if they have a material change in vendor that impacts your service

Reviewing a Privacy Policy

- When was the Privacy Policy last reviewed?
- Whose contact information do they provide? (Save this contact information)
- What information do they collect and/or process?
- Who do they share this information with?
- What cross-border data transfer mechanism do they rely upon?

Analyzing a SOC 2 report

1. Review the trust services criteria - which ones did this vendor audit against?

2. Review the limitations noted by the auditor in the service auditor’s report

3. Distinguish which text was written by the auditor and which was provided by the vendor in the overview

Analyzing a SOC 2 report

4. Review the testing results & ask for additional evidence to show that any deviations to the standard were properly addressed (if any deviations raised)

5. Review the length of the reporting period

6. If the reporting period has passed, request & review the vendor’s bridge letter

Resources

- CSA STAR Registry
- International Association of Privacy Professionals
- NIST Special Publications

Questions?