PRIORITIZING INFORMATION SECURITY &
THIRD-PARTY RISK MANAGEMENT

40 Questions to Ask During **Vendor Due Diligence**

omega systems
technology managed

@omegasystemsMSP
www.**omegasystems**corp.com

40 Questions to Ask During **Vendor Due Diligence**

The benefits of outsourcing or co-sourcing can be invaluable to your organization. From network administration and human resources to payroll and sales support, third-party vendors and service providers can streamline critical areas of your business operations and help you expedite growth and success.

But with reward, of course, comes risk. And inviting managed services providers and other outsourced vendors into your operational enterprise introduces potential vulnerabilities into your environment if you don't keep a close eye on data access controls and overall security practices.

Completing careful and comprehensive vendor risk assessments to ensure your sensitive information is controlled and secured before, during and after third-party vendor engagements is essential to maintaining your operational integrity and satisfying growing requirements from various stakeholders, investors, boards of directors, and industry regulators.

Be sure your vendor due diligence checklist includes careful examination of the following areas and requires complementary documentation and evidence to support all vendors' completed questionnaires:

- *Governance & Oversight*
- *Risk Assessments & Security Policies*
- *Advanced Threat Protection*
- *Access Control*
- *Employee Security Training*
- *Incident Response & Recovery*
- *Third-Party Risk Management*
- *Regulatory Compliance*

40 Questions to Ask During **Vendor Due Diligence**

Governance & Oversight

- [ ] Is there a team or person responsible for your cybersecurity controls, practices, and overall program?
- [ ] What are their daily responsibilities?
- [ ] What relevant cybersecurity or IT credentials do they hold?
- [ ] How often are the company's controls, practices, and cybersecurity program reviewed and updated by those responsible?
- [ ] Do you outsource any IT or security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?
- [ ] Can you provide a current SOC 2 report that addresses your existing security controls?

Risk Assessments & Security Policies

- [ ] When was your most recent cybersecurity risk assessment and/or network vulnerability assessment?
- [ ] What were the results of that assessment?
- [ ] Has action been taken to remediate any of the risks or gaps identified in the most recent assessment?
- [ ] Do you perform penetration testing? If so, how often? What were the most recent results?
- [ ] Do you have a physical security policy that protects your office location(s)? What is the screening process for allowing visitors, contractors and other employees to access your site?

Advanced Threat Protection

- [ ] What tools or technologies are used for proactive threat monitoring?
- [ ] Do you have a dedicated individual or team (e.g. Security Operations Center) tasked with monitoring and alerting?
- [ ] Do you employ advanced tools for endpoint security?
- [ ] Do you employ encryption or other methods to protect data in transit between your organization and customers?
- [ ] What is your patch management policy/schedule?
- [ ] Describe any other technologies or processes you have in place to prevent unauthorized intrusion to your network.

Access Control

- [ ] Do you maintain an inventory of authorized and unauthorized devices and software?
- [ ] Do you maintain an access control policy? How frequently is it updated?
- [ ] Do you employ a 'principle of least privilege' to limit access to sensitive data or information?
- [ ] Do you perform background checks for personnel who are entrusted with sensitive information or granted access to sensitive systems?
- [ ] Describe your physical security practices that protect the safety and security of information on-site.

Access Control *continued*

- [ ] Do you require multi-factor authentication or employ a zero trust program to prevent unauthorized users from accessing your network and data?
- [ ] What processes do you have in place to secure remote access to your corporate network?
- [ ] Do you have a removable media policy to limit data access or theft via USB or other devices?

Employee Security Training

- [ ] Are your company's employees required to complete annual information security awareness training?
- [ ] In addition to an annual assessment, are employees trained or educated on security threats in other ways (e.g. managed phishing tests)? If so, please describe.

Third-Party Risk Management

- [ ] Do you (as a vendor yourself) utilize third-party vendors who have access to your organization or customers' data?
- [ ] Do you perform third-party due diligence on all vendors, contractors, and other partners?
- [ ] How do you monitor third-party service providers?

Regulatory Compliance

- [ ] Does your organization require compliance under any specific regulatory frameworks? (e.g. PCI DSS, GLBA, SEC, CMMC, etc.)
- [ ] How do you address customers' regulatory compliance requirements?
- [ ] Has your firm been audited by its regulator in the last 18 months? If yes, what was the outcome of that audit?

Next Steps

Vendor risk management is just one component of an effective cyber risk management program. And this list of due diligence questions should be further customized to incorporate specifics relative to your business model, industry, regulatory compliance requirements, locations and other potential risk factors.

To ensure your business is properly structured to withstand modern cybersecurity threats, be sure to carefully evaluate all vendors and third parties who interact with your company using a comprehensive vendor risk management assessment. This includes vetting and authorizing what systems and data they have access to within your environment.

If you're looking for an MSP or managed security service provider (MSSP) that will take your organization's data security priorities seriously, Omega Systems can meet your third-party risk management needs while delivering a premier IT service that drives your business' success.

Get in touch with our team to learn more.