MANAGING 3RD PARTY RISK

A company can outsource activities, but it cannot outsource its risk

A company can outsource activities, but it cannot outsource its risk

Companies are increasingly leveraging external vendors to tap into the expertise and cost economies for certain roles. While this provides capacity for internal resources to focus on more strategic priorities, companies cannot understate the importance of selecting and partnering with secure vendors. We have all heard the horror stories of company breaches caused by vulnerabilities in third-party environments. These vulnerabilities can provide an opportunity for threat actors to interrupt business operations or steal critical company and customer information. Partnering with insecure vendors can easily result in lost revenue and the ability to conduct business, especially in highly regulated industries. After all, customers will hold a company accountable even if a breach occurred because of a vendor.

The sophistication of threat agents continues to increase with the adoption of new technologies and innovative attacks. One cannot over emphasize the importance of risk mitigation, especially when considering the proliferation of vulnerable end points caused by an expanding remote workforce, internet of things (IOT) integrations, and the increased number of external partners. Companies must continue to bolster their security to stay in front of the changing landscape, regardless of whether the threat comes from a foreign sponsored actor, a small-scale hacker, or people working within your organization.

Cybersecurity will never be perfect. Understanding risk and mitigating it through industry proven practices and risk-based decision making remains the most effective way to balance business needs with securing a company's environment. Utilizing robust third-party risk management practices provides a foundation for companies in this environment to reduce residual risk. For this reason, companies demand their partners have mature cybersecurity practices in place. These are "table stakes" for vendors wanting to provide goods and services, particularly in highly regulated industries like healthcare.

About Guidacent

Since 2012, Guidacent has worked with clients in various industries to successfully execute hundreds of projects that meet their business objectives. The team of seasoned professionals work with business and technical stakeholders to "get in, get the job done, and get out."

Guidacent helps companies establish IT Compliance Programs, manage audits and assessments, remediate known vulnerabilities, and execute their cybersecurity roadmaps. This includes managing vendor selection, onboarding of services and solutions, and maturing the control environments of clients and their vendors. Guidacent helps to identify the appropriate control frameworks, establish efficient tools and processes, and trains client staff to continue maturing the program after the engagement.

Program Examples

Strengthening Vendor Management Practices

> ***Client Feedback: Guidacent enabled us to meet our aggressive deadlines and implement changes to achieve the highest eligible score in the Third-Party Assurance Domain.***

Our client engaged us to implement controls aimed at strengthening its vendor management processes and achieve HITRUST certification. This included revising policies, procedures, and templates used for identifying and working with third parties. We also managed the change management process across the contracting team and business relationship owners. The client received the highest eligible score in the Third-Party Assurance Domain during the HITRUST validated assessment.

Managing Third-Party Maturity Assessment

> ***Feedback from Assessment Firm Manager: It was a pleasure working with Guidacent. They made our job easy and enabled us to deliver a quality product on time.***

Guidacent coordinated a third-party maturity assessment for a multi-billion-dollar client. The client engaged Guidacent to manage the assessor, ensuring the timely deliverable of the assessment report. We identified stakeholders, scheduled interviews, and ensured all necessary documentation was provided in a timely manner to the assessor. Guidacent coordinated the review and acceptance of the report and worked with the client to determine next steps for addressing recommendations.

Onboarding Managed Security Service Provider (MSSP) – Vendor Risk Management

> ***Feedback from MSSP Manager: We made great progress onboarding with the client because of Guidacent's assistance.***

A large client in the healthcare sector needed our help onboarding a new MSSP for vendor risk management. We worked with client staff and the MSSP to establish key workflows, identify and execute operational efficiencies, and negotiate an expanded scope of work to manage vendor remediation activities. This enabled the client to transition all third-party assessments to the expert MSSP, which freed up internal resources to focus on other strategic activities. Leveraging the MSSP for this work also reduced the amount of time required to complete assessments, resulting in a reduction in the amount of time required to approve new vendors.

Onboarding of New Auditor (SOC1 / SOC2)

Our client recently engaged a new firm to conduct SOC1 and SOC2 audits. Guidacent managed the onboarding of the auditor and worked with the client team to understand the new audit approach. We worked with the auditors to finalize the audit schedule and

communicate it to key stakeholders, ensuring the timely completion of interviews and provision of requested information.

Maturing Client's Compliance Program to Achieve ISO Certifications

A cloud computing software client engaged Guidacent to establish continued compliance across eight of its products. We managed client certification activities on both new and mature products against ISO and SOC frameworks. Guidacent also implemented a GRC tool to increase program operational effectiveness and sustainability. We further developed whitepapers to educate the sales team on the compliance standards to which their products adhere.