

DATA SHEET:

Vendor Risk Assessment

Identify Your Risk of a Third-Party Breach

Customized Questionnaire Development

Using industry standard frameworks, our security experts develop customized questionnaires designed to measure vendor risk unique to your business environment.

Rapid Third-Party Data Collection

Alleviating resource constraints, our security experts conduct third-party data collection on your behalf accelerating the evaluation process and ensuring response accuracy.

Comprehensive Evaluation Of Vendor Risk Profiles

Illuminating areas of greatest risk, our security experts perform careful examination of responses and corrective actions against your organization's level of risk tolerance.



44% revealed that they had experienced a Third-Party-related data breach in the last year¹

33% of organizations cited lack of internal resources as a challenge in evaluating Third-Party vendors¹

48% of organizations that experienced a third-party breach reported significant business consequences (reputational damage, discontinued business, financial loss)¹

As ever-expanding digital networks necessitate expansion of third-party and vendor access to sensitive data, the old adage that a chain is only as strong as its weakest link has never been more relevant from a security perspective. In an unfortunate tradeoff, business enablement from third parties and vendors in turn present business risk. Lack of visibility and end-to-end control of vendor security practices increase the potential attack surface for which organizations must account. Unfortunately the scale and expertise required to assess potential third-party risk presents challenges for most organizations with resource constraints.

Based on the eSentire Security Framework that is built on the foundations of NIST, eSentire Vendor Risk Assessment is designed to help resource constrained organizations:

- Determine risk identification and measurement criteria
- Categorize assessment data access against risk appetite
- Develop questionnaires for assessment
- Conduct comprehensive assessments
- Analyze data with comparisons against risk categorizations
- Define corrective actions for risky third parties and vendors
- Determine defensive adjustments to mitigate risk

¹eSentire/Spiceworks Third-Party Third-PartyRisk Research, January 2019

Factors Requiring a Vendor Risk Assessment:

- Exploration of acquisition or mergers
- Regulatory requirements
- Risk measurement of new partnerships, vendors or third parties
- Increased risk profile of existing vendors due to additional data access, public breach or Nth party access

What Does it Help You Answer?

- What should my criteria be for assessing my third party partners and vendors against?
- What questions do I ask to gather the right level of information?
- How do I categorize my third parties and vendors against their potential to disrupt business?
- Do my third party partners and vendors meet requisite security standards?
- How effective are my current third-party risk policies and controls to mitigate against risk?
- Who are my third party partners and vendors sharing my data with?
- What measures do I require my third party partners and vendors to put in place that is balanced with their risk profile?
- How do we track progress and improvement?
- What controls should we put in place based on the assessment?

How Does It Work?



Deliverables

- ✓ Measurement criteria and questionnaire development
- ✓ Execution of risk assessments on identified vendors and third parties
- ✓ All vendor interactions and necessary follow-ups handled by eSentire on behalf of the client
- ✓ Measurement of risk assessment data against client-specific risks, industry standards, and the eSentire Security Framework
- ✓ Assessments completed within a predictable 4-6 week timeframe
- ✓ Executive summary on findings
- ✓ Recommendations for programmatic improvement and progress measurement

Make The Case For An eSentire Vendor Risk Assessment:

- Comprehensive third-party and vendor risk visibility
- Risk identification and categorization criteria unique to your business operations
- Satisfies third-party risk compliance mandates
- Frees up time and resources from compliance, risk, IT, and cross-functional teams
- Tracks, measures, and holds your third parties and vendors accountable for the risk they pose
- Guidance for continued improvement in third-party and vendor risk mitigation strategy and controls

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit www.esentire.com and follow @eSentire.