SOLUTION BRIEF

Brinqa Vendor Risk Management

A unified solution for continuous vendor risk monitoring through granular, context-aware risk assessment, treatment and communication.

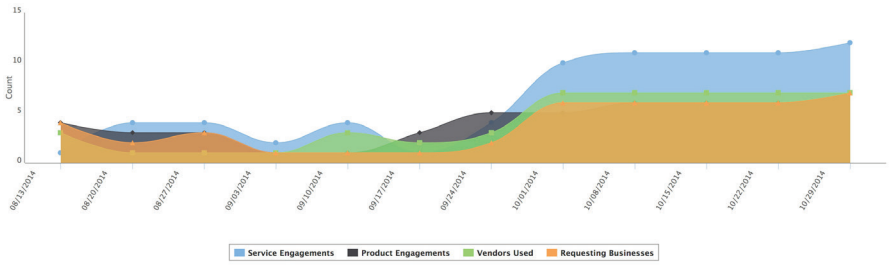
Highlights

- Centralized and standard vendor risk repository
- Comprehensive vendor risk profiles : leverage commercial risk ratings and exposure
- Intelligent vendor classification : consider changes in relationship, scope, and financial and operational footprint
- Granular risk assessment : Evaluate vendor relationship, services provisioned and products delivered
- Continuous vendor evaluation : evaluate frequently based on governance levels
- Assess what matters : Identify risks and evaluate mitigating controls
- Leverage technology security tools to evaluate risk associated with vendor products
- Quantitative and predictive risk remediation planning
- Limited vendor portal (for delivery of documents, assessment response and issue remediation)
- 4th Party Risk Assessment: Evaluate a vendor's security dependencies
- Supports SIG (all versions) and OCIL 2.0

Vendors comprise an important and often overlooked or misrepresented part of an organization's risk ecosystem. Organizations depend on vendors and third parties for execution of key business-critical IT functions and processes. Vendors have access to an organization's applications, infrastructure and important business and personnel information through use of provisioned products and services. In recent times, enterprises across diverse industries like financial services, high-tech and retail have suffered data breaches as a result of lacking vendor risk management processes, resulting in significant losses to financial and brand value.

Vendor risk affects several aspects of a business like service availability, business continuity, controls for information security and privacy, and compliance with regulations, among others. A growing dependence on vendors for specialized technology and IT services, along with the growing incidence and cost of breaches originating from vendors, places an immediate emphasis on ensuring that vendors are considered in initiatives for regulatory compliance, continuity planning and information security best practices.

Vendor Risk Program Trend



Highest Risk Vendors

Provisional Data Services
BRQ Consulting
Addison Search, LLC
AC Financial Recruitment Ltd.
A & J Recruitment Limited
Acme Packet, Inc.
ABN AMRO Bank N.V.
Accounting Principals Inc

Key Risk Indicators

Challenges

Organizations struggle to maintain an accurate representation of all third parties and their impact on business objectives. Third parties form a wide range, from strategic vendors crucial to achieving a business's central goals to trivial vendors that enable ancillary processes. Vendor services and products support a wide variety of functions at different levels of the organizational hierarchy. Risk organizations are charged with the unenviable task of ensuring that all risk aspects of a vendor's utilization are assessed, analyzed, and clearly communicated and understood by business. This must be done as seamlessly as possible and all efforts must be made to avoid additional work or noise for the business.

Static, unintelligent processes to monitor and manage the risks associated with third parties are no longer sufficient to meet the requirements of auditors and security teams. Risk analysts should be able to tell at a glance how many vendors exist in their organization, how these vendors are being used by businesses and departments, the risk classification of these vendors, and if the vendors have undergone all the appropriate risk evaluations dictated by established risk classification.

Vendor risk management systems should capture and track details of how different parts of the organization leverage a vendor's services and products. Organizations should have immediate insight into how a particular vendor performs compared to other vendors that provide similar services or products. Changes in a vendor's financial and operational footprint in the organization's environment should be factored into vendor risk evaluation processes.

Brinqa Solution

Brinqa Vendor Risk Management implements a holistic approach with an emphasis on accuracy of risk identification and representation, to ensure all vendors and associated products and services are accounted for in context of their relationship with the organization and in context of their engagement impact and scope. Existing investments in Information security as well as commercial risk rating and exposure agencies are utilized to present a complete picture of the organization's vendor risk.

Flexible, context-aware vendor assessments are conducted to quantify relevant risk dimensions as well as to identify risks and assess the applicable mitigating controls. Vendor risk classifications are established and utilized to ensure all vendors are evaluated periodically based on their relevance and importance to the organization.

Develop Vendor Risk Profiles and Classifications

The first step in conducting a successful vendor risk management program is to ensure that all vendors are identified and accurate risk profiles and classifications are established. The solution establishes an authoritative vendor repository by integrating with existing databases, information management and procurement systems or by creating the inventory directly in the application. A vendor's risk profile should take into account inherent factors that reflect how the vendor's organization is structured, how it does business, its perceived image in the public domain etc. For this purpose the solution provides out-of-the-box integrations with specialized organizations like commercial risk rating agencies. In the absence of this information from external sources, the application automatically conducts risk assessments to evaluate these risk dimensions.

A crucial factor in establishing risk profile and classification is the scope and impact of a vendor's ongoing engagements within the organization. Vendors being engaged for the delivery of highly sensitive, costly or mission-critical business objectives are rated higher that those being utilized for non-essential ancillary functions. The solution also allows for strategic vendors to be flagged and handled with greater scrutiny.

A robust vendor risk profile development process ensures that relevant risk information is obtained, gaps identified and classifications established that inform the level of detail required when evaluating the risk incurred by interactions with the vendor.

Engage Vendors for Services and Products

The solution provides an interactive, risk-centric vendor engagement process for provisioning services or products from third parties. It takes historical vendor performance into account to provide suggestions during the vendor engagement process to help businesses make the best decisions when provisioning services and products from vendors.

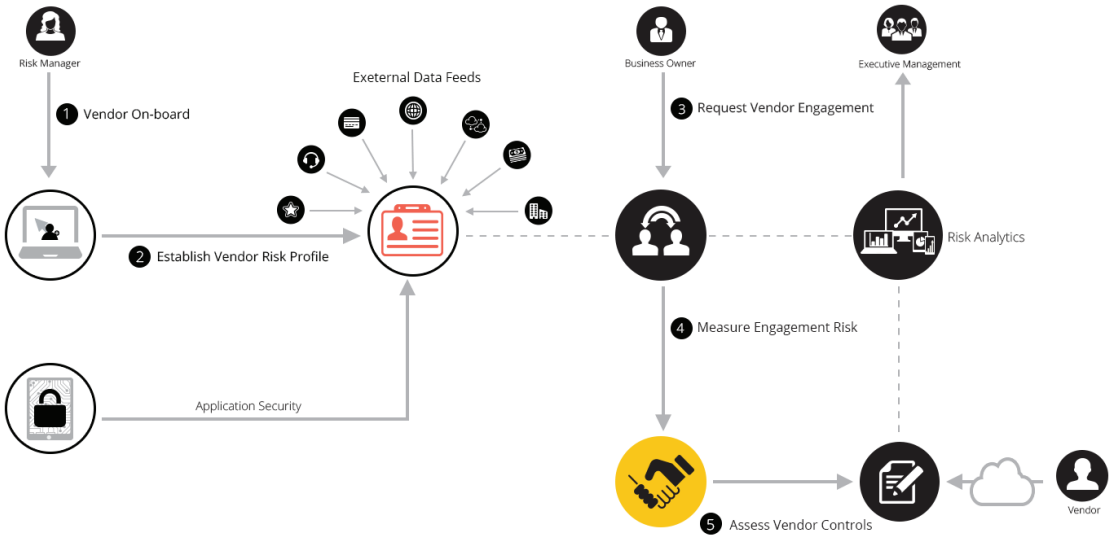
Similarly, the solution can prevent business from engaging vendors that have not completed their on-boarding requirements, or vendors that have high, unresolved risks associated with them as a result of current engagements.

Evaluate Granular Risks

To create true representation of the risks associated with a vendor, in addition to evaluating the overall vendor relationship, the solution also quantifies the risks associated with each distinct vendor engagement within the organization.

By evaluating individual vendor engagements for risks and corresponding mitigating controls, the solution provides complete transparency and visibility into the organization's interactions with a vendor and ensures that vendors do not accidentally get access to information or infrastructure that they are not cleared for.

Detailed control assessments, conducted to identify the gaps and issues that must be addressed by a vendor, are tailored specifically to how the vendor is being used by different businesses and departments within the organization and thus very accurate in its representation of the risks associated with doing business with the vendor.



Brinqa Vendor Risk Management employs a wide variety of integrations available in the Risk Analytics Platform to evaluate the application security risks associated with a vendor's software products. Findings from static code analysis, dynamic code analysis, application penetration testing and open source vulnerability deliver valuable information that is used for evaluating risks associated with the use of a vendor's software products and help businesses make better decisions when selecting comparable products or versions.

Conduct Relevant, Contextual Risk Assessment

Granular vendor engagements are quantified using automated risk assessments. Engagement risk assessment evaluates how businesses intend to use the vendor, what level of access will be granted to the vendor, If any data will reside on vendor's network, whether sensitive business information will be exposed etc. It establishes the risk classification of the engagement, and by identifying imminent risks and leveraging the comprehensive Brinqa Compliance Framework, it clearly outlines the controls that the vendor must have in place to support the organization's risk and compliance goals.

Identify Issues and Plan for Remediation

Gaps and findings identified by risk assessments or application security testing tools should be vetted, assigned and targeted for risk treatment. The solution provides a comprehensive workflow engine to track the ongoing mitigation, remediation, exception management and risk acceptance of identified issues. Closed loop remediation ensures that gap resolution is reflected in a vendor's risk profile in real time. Organizations spend significant time and human resource to remediate issues without clear knowledge of how mitigating or fixing a particular problem affects their risk posture.

Brinqa Vendor Risk Management takes the guess-work out of remediation planning using quantitative and predictive mechanisms like the "What If Analysis" that allow risk professionals to analyze groups of issues together, giving them an unambiguous answer to the question 'How does fixing these issues, in this manner, help me reduce risk on these entities and to what numeric extent?' This enables organizations to give a clear mandate to vendors about what risks need to be addressed and to what extent to ensure a relationship within acceptable levels of incurred risk.

Understand and Communicate Risk

The solution provides a comprehensive library of metrics, reports and dashboards that give risk analysts and business owners a complete oversight on the vendor risk management process. Overview dashboards give a clear indication of how many vendors have completed the on-boarding requirements, how many critical risks and issues have been identified, which vendors, services and products have the highest risks associated with them etc.

Multi-dimensional perspectives of risk are established at every step of the risk assessment process to provide detailed performance metrics on several risk dimensions. Granular risk evaluation allows risk professionals to see at a glance how different vendors are performing in delivery of the same service, thereby enabling better procurement decisions. Dynamic risk reports deliver complete visibility into vendor relationships by providing the ability to splice risk data across and to drill down into details, risk and control performance metrics for root cause analysis. Risk trends across relevant risk areas promote understanding of the organization's exposure and vendor behavior that impact it. Risk reports highlight businesses and processes that are most at-risk due to their vendor dependencies as well as predict potential problem areas.

Continuously Monitor and Track

Many organizations do a fair job of ensuring that vendors are evaluated when they are first introduced into the organization's risk environment. However, there is very little oversight to track the vendor as its relationship with the organization changes and evolves. Often, vendors are never assessed again after their initial on-boarding process. This can result in a false perception that implies compliance based on evaluation of irrelevant or insufficient controls dictated by an outdated risk classification of the vendor.

Brinqa Vendor Risk Management factors in the scope and impact of ongoing vendor engagements to reflect the overall vendor risk profile and classification continuously. Risk profiles and classifications are used to establish the frequency and level of vendor risk evaluation required to ensure continuous monitoring and management of vendor risk.

Identified risks are quantified against regulatory and organizational mandates on a temporal scale that rewards complete and quick resolution and penalizes partial or delayed remediation. Informed, efficient, closed-loop remediation planning is promoted through predictive measures and granular remediation plans.

Conclusion

Vendor Risk Management is a complex, involved task and doing it right has never been more relevant. Automate your data collection, risk assessments and risk remediation workflows while gaining the ability to work closely with business partners and optimizing time and flexibility to focus on critical risk mitigation. Eliminate duplication and utilize your existing investments in information security and governance to address vendor risk in a holistic manner with the Brinqa Vendor Risk Management solution. Visit www.brinqa.com or email sales@brinqa.com for more information.

About Brinqa

Brinqa is a leading provider of unified risk management – enabling stakeholders, governance organizations, and infrastructure and security teams to effectively manage technology risk at the speed of business. Brinqa software and cloud services leverage an organization's existing investment in systems, security, and governance programs to identify, measure, manage and monitor risk. With Brinqa, organizations are reducing response time to emerging threats, impact to business, and technology risk and compliance costs by over 50% through real-time risk analytics, automated risk assessments, prioritized remediation, actionable insights and improved communication.