brinqa

CUSTOMER SUCCESS STORY

Leading International Bank Achieves Complete 3rd Party Risk Visibility with Brinqa Vendor Risk Management

OVERVIEW

The Brinqa customer profiled in this case study is one of the top 10 commercial banks in the world. With more than 100,000 employees in over 50 countries, the bank has a strong presence in Europe, the Americas and emerging markets and provides a range of products and services to business, commercial, corporate and institutional clients as well as to personal and private clients.

CHALLANGE

In the wake of the recent high profile breaches originating from vendors, senior management demanded greater oversight into the organizations' interactions with Third Parties. The Technology Risk Management (TRM) team was charged with collecting, analyzing and presenting this information.

SOLUTION

The bank implemented a robust vendor risk management program with Brinqa VRM as the core to go from unreliable and fractured vendor risk management to complete vendor utilization awareness in 30 days; vendor profiling, risk classification and risk assessment in 60 days; and gap identification, remediation planning, risk reporting and continuous monitoring in 90 days. During this time over 1700 vendors and over 5000 vendor service and product engagements were assessed for risk.

High-profile breaches across diverse industries have put a firm spotlight on vendor risk management as a key area of concern for information security organizations of all shapes and sizes. This has transpired as most significant changes in the security world do, as the result of a series of cybersecurity incidents originating from vendors, resulting in penalties and firings, all under great scrutiny from the national and international media.

These breaches shine the light on what most security professionals have known for a while: That vendors are an integral part of an organization's day-to-day business, an extension of the enterprise entity. And while most organizations are getting better at developing and implementing internal information security policies and controls, the measures to extend these policies to vendors are grossly inadequate or simply do not exist.

Forward-thinking, risk-aware security organizations have begun mobilizing towards vendor risk management programs designed to provide answers to questions that really matter, in contrast to the false sense of security engendered by most compliance-oriented vendor management programs. One such organization, a leading international commercial bank, is profiled in this case study.

Like most successful financial services organizations, the bank recognizes that risk management and information security are a vital part of its growth and of its very existence. Where the bank showed great insight was in realizing that while compliance initiatives may keep auditors at bay, true confidence in one's information security measures requires a risk based approach that provides answers to questions that auditors will be asking tomorrow, and not just the ones they are asking today. The task of building and delivering this confidence fell to the Technology Risk Management (TRM) team.

With Brinqa VRM, within 90 days the bank established an authoritative vendor and engagement repository, assigned vendor risk classifications and completed an entire cycle of risk assessments for over 1,700 vendors and 5,000 vendor engagements.

The benefits realized in this first phase of deployment include:

- Authoritative vendor and service engagement repository
- Visibility into the organization's vendor dependence and utilization patterns
- 70% reduction in time to complete vendor risk assessments
- 30% reduction in assessment content generated for vendors

The need for comprehensive vendor risk assessment and reporting

The bank's existing vendor management program had been sufficient to satisfy auditors for years, and yet, when the program was evaluated for its effectiveness to provide answers to introspective questions aimed at getting a better understanding of the organization's vendor risk posture, it fell spectacularly short. Lets examine the reasons for this failure and compare them to desired program characteristics.

Limited vendor risk program scope

The existing vendor risk management program was put in place by external consultants with the primary goal of meeting compliance and audit mandates. As such, the program goals were fairly limited in scope. Vendors were assessed once upon being included in the program and then once a year when the vendor management team conducted their annual reviews. The program made no attempts to factor in how a vendor was actually being utilized by the business. As long as vendors were included in the program, they would be evaluated at the predestined frequency regardless of whether they were being engaged extensively for delivery of critical business goals or not at all.

Disjointed & cumbersome processes

Even within the narrow program scope there were serious points of friction resulting in suboptimal processes and lack of efficacy. The annual review was a beast of a process, occupying the entire vendor risk management team for a good portion of half of the calendar year. The assessments were conducted using a survey tool that sent out questionnaires but the data collected was eventually exported out to spreadsheets (through heavily customized ETL) to run the complex risk scoring and rating calculations desired. Similarly, gaps identified through the questionnaire-based data collection process were managed as tickets in an internal ticketing application. Further, reporting to stakeholders was managed through yet another tool that required another round of data transfer after risk rating and gap analysis. It was no surprise that the TRM team spent a good chunk of their 6-month risk assessment cycle simply managing and validating data transfer. In the lack of a single comprehensive solution to manage all the pieces of the program, the team found themselves falling to the familiar but highly inefficient model of managing the missing pieces through spreadsheets and email.

Vague vendor classification criteria

The program made some attempts to qualify the level of detail at which a vendor is evaluated. This is important since vendors form a wide range in terms of their relevance and importance to the organization and the types of services and products they provision. In an ideal world the vendor assessment process should reflect a vendor's relative position in the organization's information architecture. Vendors should be evaluated for controls that address risks relevant to the nature of services and products they deliver. While the program regulated risk assessment granularity based on vendor classification, the process to establish these classifications was ambiguous. Risk classifications were set arbitrarily, often driven by the perceptions of vendor sponsors, many of which turned out to be incorrect on detailed analysis.

Incomplete & incorrect risk assessments

The existing program never aimed to deliver very detailed risk representation, with vendors only being evaluated at the overall entity level and no provisions for expounding risk ratings into underlying dimensions. However, upon further analysis, this goal was seen to not be met either. Vendor information in the organization existed within different departments. Procurement and legal typically maintained their own repositories of vendor information. IT maintained further information about vendors delivering certain products and services. Upon analysis of a sample risk assessment cycle, it was seen that some vendors were represented multiple times, in different forms, depending on the source of the information. This resulted in duplication of effort as well as incorrect risk ratings for the vendors in question. There were also incidents where vendor classifications had been updated in response to changing relationships but the vendors were not evaluated again to reflect the updated state.

Lack of analytical insights

The level of detail captured and represented by the program was found to be insufficient to answer even very rudimentary questions that might be posed of the program

- What is the organization's dependence on a particular vendor?
- Which critical business functions, processes or initiatives have dependencies on vendor services or products?
- For comparable services and products, which vendor is the best/worst choice from a risk point of view?
- For vendors that provide comparable services and products are we rewarding secure vendors and penalizing vendors that are putting us at risk?
- Which gaps must a vendor address to fit within the norms of acceptable risk?

For stakeholders not directly involved, the black-box spreadsheet-based risk calculation methodology resulted in magic numbers and ratings that brooked no further analysis.

The blueprint for a comprehensive vendor risk management program

Working with Brinqa, the TRM team drew up the blueprint for a comprehensive vendor risk management program and set about putting it in place.

Establish a centeral authoritative vendor repository

Establishing an authoritative vendor repository is key to the effectiveness of a vendor management program. As with most organizations, vendor information at the bank was fragmented among different departments and business units that dealt with third parties. The TRM team drove an initiative to build consensus within the bank and utilized the Brinqa connector framework to create an authoritative repository of vendors by collating data from different parts of the bank like procurement, IT, strategic alliances etc. Gaps, redundancies and inconsistencies in vendor information were identified and remedied.

Define accurate and intelligent risk classification

Accurate vendor risk assessment requires that intelligent vendor classifications be established and that vendors be evaluated in accordance with these classifications. A formal vendor due diligence process was put in place and enforced with mandatory profile assessments designed to evaluate a vendor along inherent risk dimensions like country rating, credit rating and financial ratings as well as operational risk dimensions like continuity risk, integrity risk, organizational risk and strategy risk. Complete vendor profiles also take into account the criticality and impact of ongoing vendor engagements. The bank chose a tiered nomenclature, from a configurable set of classifications, with 'Tier I' for the most critical vendors to 'Tier III' for trivial vendors supporting ancillary functions.

Adopt a granular risk representation

Evaluating a vendor for security controls and policies without first understanding how the vendor is being utilized by business and without identifying the relevant risks is counter-productive and inefficient. The Brinqa VRM risk model utilizes 'engagements' (sometime referred as 'contracts') to capture every relationship between the organization and its vendors. Engagements capture important utilization information such as duration, budget, ownership, data location, access requirements, etc. If a vendor provides a particular service to several different departments within the organization, each of these engagements is identified and assessed independently for risk.

Include all vendor relationships

Often vendor management programs only consider service providers and ignore third parties that deliver products. This results in a skewed representation of the organization's external dependencies. The new program included vendor products as well as services to ensure that all external dependencies were factored in. The program leveraged existing investments in application security assessment tools to evaluate the risks associated with external software products.

Conduct engagement risk assessment

Engagement risk assessments leverage the Brinqa Integrated Compliance Framework (ICF) to serve two crucial functions in the vendor risk management process.

Quantify risk impact — takes into account the criticality of the business function being supported, the level of access being granted to the vendor, the sensitivity of the information being exposed etc. Risk impact is a quantitative representation of the organization's dependence on a particular vendor engagement and informs the level of scrutiny that the vendor must be placed under. Vendor risk classifications are updated to take into account engagement risk impacts.

Assess required mitigating controls – identify the risks assumed by the organization due to the nature, scope and criticality of vendor engagement. By correlating with the Brinqa ICF, they highlight the controls that the vendor must be evaluated for to ensure risk mitigation. It is irrelevant and counter-productive to test a vendor for data security controls if the vendor does not have access to the organization's data. .

Conduct context-aware vendor control assessments

Control assessments are conducted to evaluate the effectiveness of a vendor's security measures in dealing with the risks assumed by the business in its engagement with the vendor. Using a combination of vendor risk classifications and engagement risk identification to drive the content and assessment of vendor control effectiveness, the program achieved significant reduction in time and labor costs while simultaneously improving the quality of vendor responses. TRM considered different options available for control assessment content including SIG, SIG Lite, etc. before deciding on the proprietary Brinqa ICF questionnaires. Issue identification rules automatically capture gaps in a vendor's information security controls and provide a seamless path to risk treatment.

Use predictive models for remediation planning

Issue remediation tracking is traditionally a time and effort intensive task. In the absence of a mechanism to establish quantitative risk remediation goals, vendors were asked to fix all identified issues and gaps that met an arbitrary, static criterion (usually based on severity or other risk attributes). In reality, the organization was willing to accept a certain amount of risk. With a quantitative risk model, the organization was able to define acceptable risk thresholds. The TRM team was now able to utilize 'What If Analysis', a predictive risk remediation-planning tool, to clearly define a compliance path for the vendor. Vendors were now given precise instruction regarding which issues and gaps they must fix, and to what extent, to be within the acceptable levels of risk defined by the organization. This resulted in more than 50% reduction in time and effort required to plan and track remediation.

Establish continuous monitoring

Vendor risk management is only effective when it is enforced automatically and continuously. The program enforces vendor due diligence for all existing and new vendors and only vendors that successfully completed the process were allowed to be engaged in the delivery of products or services to business. As long as vendors are part of the program, they are evaluated at a frequency determined by their risk classification, regardless of whether they are being engaged by the business or not. Changes in engagement profile and risk classifications automatically trigger vendor assessments to ensure control measures commensurate with the latest ratings.

Prvoide comprehensive reporting

The TRM team leveraged Brinqa dashboard and report builder to add on to the out-of-the-box reports and developed a comprehensive catalog comprised of more than 20 distinct reports. Reports were designed to communicate program state and business and monetary impact to senior management. A distinct set of reports were developed for and made available to auditors providing detailed information about vendor coverage and assessment as well as risk identification and mitigation. Risk metrics are represented and tracked in reports and used by the team extensively to monitor the state of the program and vendor performance.

A "quick win" backed by solid results

Vendor Risk Management is a complex, involved task and when done right can build great trust and reliability in an organization's ability to monitor and manage external threats. Utilizing Brinqa Vendor Risk Management a top commercial bank was able to reign in the risks involved in its third party interactions and deliver tangible value and confidence in a short amount of time. On conclusion of the first phase of the initiative the organization had obtained a much clearer picture of its dependence on third parties. The organization was able to identify crucial vendors engaged in the delivery of mission critical goals and was able to ensure that steps were taken to protect the organization against all perceivable risks.

Brinqa Risk Analytics Solutions

Brinqa is helping organizations discover, understand and manage risk across diverse technology and compliance areas. Brinqa solutions (IT Risk Management, Security Risk Analytics, Vendor Risk Management, Compliance Risk Management) deliver a fresh approach to solving key risk problems affecting enterprises today.

Brinqa Risk Analytics Platform (RAP), the engine that drives Brinqa risk analytics solutions, delivers streamlined, uniform interactions to define risk models, incorporate data from a variety of sources, conduct risk assessments, identify and plan mitigation of gaps, define relevant risk metrics and indicators, and create reports and dashboards to take the heavy lifting out of risk management, letting you focus on the discovery, analysis, and remediation of risk.

Brinqa solutions combine comprehensive risk modeling, exhaustive data collection capabilities, risk-oriented analytics, and end-to-end risk management to create and implement sophisticated risk models. The solutions identify and evaluate key metrics and indicators to deliver immediate, accurate insight into an organization's risk posture. Brinqa solutions leverage existing investments in security technology using a vendor-agnostic connector framework and augment risk data by conducting context-rich assessments to allow risk professionals to discover relationships between disparate types of risk data previously hidden in siloed products and processes. All Brinqa solutions are available as cloud services, delivering powerful risk analytics with minimal administrative overhead.

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.