SOLUTION BRIEF

Brinqa Information Technology Risk Management

Unified solution for assessment, monitoring, reporting and treatment of IT risk.

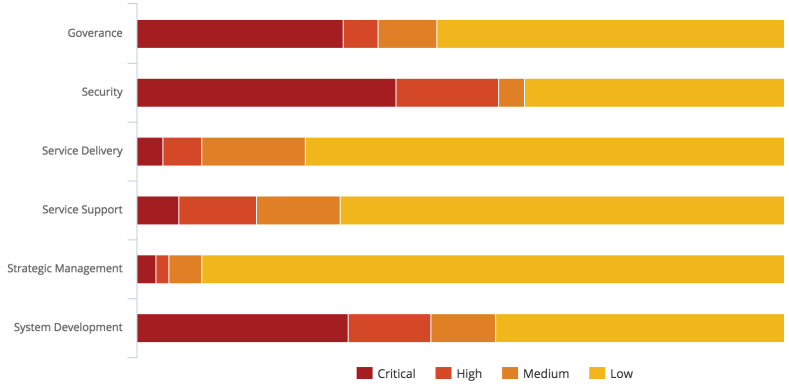
Highlights

- Adaptive Risk Models
- Business-context aware risk evaluation
- Authoritative asset inventory
- Dynamic & consistent risk assessments
- Configurable risk thresholds & tolerances
- Risk dependency and flow visualization
- Multi-dimensional risk perspective
- Continuous risk monitoring
- Risk metrics and indicators
- Uniform issue and remediation tracking
- Advanced data querying and dashboard builder
- Dedicated reports portal
- Industry-leading, standards-driven risk and control framework
- NoSQL indexing and storage
- Scalable and secure

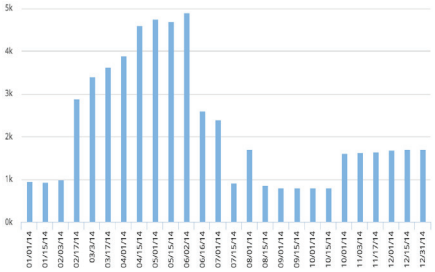
Information Technology has quickly transformed from a supporting function to a tool for innovation and a competitive advantage in the modern enterprise. Increasingly distributed and decentralized environments are driving how individuals and enterprises work together. Data driven analytical approaches are transforming how diverse business functions like marketing, sales, research, etc. function and organize to help an enterprise support growth initiatives, remain competitive and constantly innovate. At the center of it all is a ubiquitous IT organization as diverse and distributed as the functions it serves and supports. The rise of mobile phones, BYOD, virtualization and cloud services in the corporate environment have served to push the scope of IT organizations further beyond the physical walls of the enterprise.

With the increased strategic importance of IT, IT Risk Management is firmly in the spotlight for CIROs, CISOs and executive boards alike. ITRM is a distinct and crucial function in modern enterprises tasked with providing security professionals as well

Asset Risk By Control Domain



Count of issues



Key Risk Indicators

1,074 critical open issues

24% of the assets have been assessed more than once in last year

36% of assets are not compliant

as business users with a clear visibility into the risk posture of the organization. ITRM presents a holistic risk-view of the organization, mapping crucial business entities and processes to relevant components of the IT infrastructure. It provides the framework to leverage security systems at the disposal of an organization to monitor, interpret and evaluate risks associated with any IT component and their impact to business - highlighting the critical gaps and risks that must be addressed to meet organizational security goals. ITRM translates gap and threat information as reported by security tools into contextual and actionable data at the speed and in the language of business. It defines risk thresholds for different business entities and presents roadmaps for remediation and mitigation of identified risks. ITRM translates corporate and regulatory mandates into security controls that must be implemented to meet key confidentiality, integrity and availability requirements. And it does all this with minimal impact to the organization's core business.

Challenges

Gaining true insight into an organization's technology risk posture is a daunting task. To be able to do so, an organization needs deep understanding and self-awareness of how its different technology and infrastructure components are also potential sources of risk. Every level of an organization's hierarchy is affected by risks of greatly varying nature and significance. To get a complete picture of risk, the organization must be able to represent how different types of risks affect functions and processes at every level. This involves identifying all the potential sources of risk for a business function or component and their associated impact. In its ideal form, this exercise is at once highly detail-oriented and ultimately comprehensive. The smaller level of granularity that this exercise is undertaken at, the more accurate is the final representation of risk.

A large variety of security tools are available to monitor and protect different IT components. As an organization expands the coverage and scope of its technology controls and corresponding monitoring systems, it runs the risk of losing critical information in the vast magnitude of security data being reported. Investments in security tools are of limited benefit in the absence of a framework to interpret, analyze and prioritize the gathered data. A unifying structure is required to normalize data from distinct security tools into a uniform language and scale and to contextualize this information according to the mandates and priorities of the supported business functions. The highly complex, dynamic and interconnected nature of security data also means that it is no longer sufficient to observe and report, a framework that delivers real results must be able to analyze the available data and gain true insights. Incidents like breaches resulting from the Heartbleed vulnerability have highlighted how ill prepared traditional approaches to ITRM are for dealing with the ever-evolving threat landscape. Security organizations scrambled and struggled to locate and patch all applications using the vulnerable version of the affected library. The seemingly rudimentary ability to easily search and locate specific types of assets was missing from most existing ITRM programs resulting in many organizations not being react fast enough to prevent breaches.

Granular representation of risk at individual business function or component levels is of limited use unless it is viewed holistically against the organization's overall risk goals. This problem gets compounded by the fact that each organization is unique and while organizational risk models can be suggested based on industry, size, geographical location etc., to truly capture an organization's (ever evolving) priorities, biases and tolerance to different types of risk, the representative model must be highly flexible and open to change.

Brinqa Solution

Brinqa ITRM takes a data-driven and analytics-powered approach to the challenges posed by today's security and threat landscape. The effectiveness of a risk management program is directly driven from its accuracy in identifying all entities in scope for risk measurement, factors that affect and influence risk and the underlying relationships. An advanced risk model designed using the Brinqa Risk Analytics Platform lays the groundwork for definition and determination of risks, identification and monitoring of relevant entities in the ecosystem, definition and representation of conditions that impact risk and evaluation of quantitative risk impact. Optimized data collection features like contextual assessments and automated data connectors serve to fortify the risk model with security information from all sources available in the organization's IT ecosystem. The integrated Brinqa Risk and Control Framework forms the context for data collection, risk evaluation and gap identification – providing a reliable and proven basis for all actions and plans aimed at improving the organization's risk posture. Graph analytics driven exploratory, diagnostic and predictive features place powerful tools at the hands of risk professionals to promote a true understanding of risk.

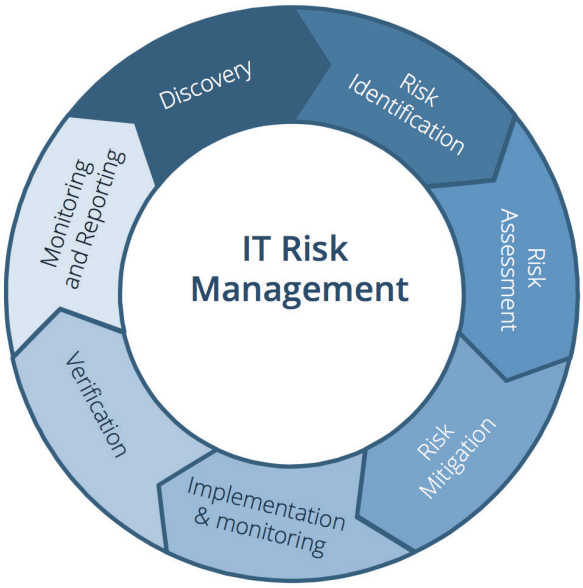
Build an Authoritative Asset Repository

A common challenge for most ITRM programs is establishing and maintaining an accurate asset inventory. Asset identity resides in several different tools in a typical IT infrastructure — Application details may be maintained in CMDB or disparate databases, network entities may be represented by network mapping or asset discovery tools, business processes and entities may reside in databases managed by teams outside of IT. While a daunting task, it is a crucial ITRM task to maintain a single repository of all assets for which risk needs to be evaluated and monitored.

Brinqa ITRM addresses this challenge by providing a dynamic inventory template representing most assets typically required to be monitored by an ITRM program. Built on the Brinqa Risk Analytics Platform, the advanced data modeling capabilities make it very easy for risk professionals to grow the asset inventory as required by managing different asset types.

Utilize Business Hierarchy and Risk Modeling

An ITRM program is effective only when it provides a holistic risk-view of the business. To be able to present this view, a thorough understanding of the different entities being monitored and their relationship to each other is required. It is equally important to establish business ownership and risk flows to enable accurate risk evaluation and reporting. At the core of the Brinqa ITRM solution is a risk model that represents relationships between the entities being monitored, the computational strategies for normalizing and contextualizing security data, the events and triggers that effect the overall risk posture and the governance and lifecycle management features required for entities. The Brinqa solution is unique in delivering a risk model that is truly dynamic and that evolves as the scope of the ITRM program changes and evolves.



Perform Comprehensive Risk Assessments

Long recognized as a vital tool by private and government research organizations, risk assessments are a severely under-valued and under-utilized weapon in the arsenal of most risk and security organizations. Risk assessments are an invaluable tool for testing the coverage of an ITRM program, evaluating the inherent nature, criticality and impact of business and IT assets and as a basis for identifying relevant controls and policies. Brinqa ITRM provides detailed content options and a simplified flow for conducting risk assessment of assets as a means of providing decision makers with information required to understand factors impacting different components of the risk model.

The assessment framework supports intelligent assessments that evolve with changing scope and state of analysis to reduce responder fatigue and ensure the highest quality of manual data collection possible. Assessments make extensive use of Brinqa Risk and Control Framework to go beyond static data collection and provide powerful control evaluation and gap identification. A standardized inherent risk and control risk evaluation model is available out of the box to perform detailed risk evaluation of any assets in scope. Collaboration features ensure that all relevant stakeholders are engaged in every step of the risk assessment process.

Advance to Data Driven Assessments

The lifeblood of an ITRM program is the security data it consumes, interprets and analyzes. The processes employed — to extract relevant security data from different tools and parts of the IT infrastructure, transform it into a common risk language and interpret it according to the needs and priorities of business — govern to a large extent whether an ITRM program will be successful or not.

Brinqa ITRM simplifies this crucial step through centralized connector management, providing a single interface in which to configure the extraction, normalization and contextualization of security data, utilizing more than a 100 purpose-built, out-of-the-box connectors available for a wide variety of security tools. The

interface also enables automation and monitoring, making one of the most cumbersome parts of an ITRM program almost effortless through complete management.

Implement a Comprehensive Controls Framework

While it is crucial to identify and monitor risks, it is equally imperative for an effective ITRM program to provide risk professionals with the roadmap and guidelines for remediating and mitigating these risks. Brinqa Controls Framework, developed in collaboration with our technology and solution partners, and based on our years of experience helping large organizations navigate the complex ITRM landscape provides risk professionals with a comprehensive framework. It provides granular control implementation definitions and correspondingly granular remediation options for identified risks. Brinqa controls framework provides mapping to common industry standards and frameworks like ISO, COBIT, NIST, etc.

Identify Issues and Plan for Remediation

Gaps and threats identified through any security tools employed by the organization may be converted into issues to be tracked for remediation. Brinqa ITRM enables automatic issue creation and consolidation based on rules as well as manual issue creation on an ad hoc basis. Brinqa Risk Matrices enable predictive remediation planning by simulating remediation of selected issues and analyzing the corresponding quantitative risk impact. The integrated Brinqa Risk and Control Framework provides clear guidelines to security professionals about the actions that may be taken to remediate a problem. The controls framework also enables program owners to demonstrate compliance with industry standards and regulations such as PCI, SOX, FISMA etc. through defined mappings.

Analyze and Report

Brinqa ITRM solution comes with a wide variety of technology and business hierarchy based reports targeted for a diverse audience ranging from C-level executives to engineering managers. Line-of-business and other organizational or reporting hierarchy based reports provide a clear view into which parts of the organization are most at risk. Technology oriented reports highlight the most critical and exploited threats and guide security teams towards remediation plans that deliver the most benefit to the organization.

Advanced filtering and searching features make it easy for business users, risk professionals and administrators to analyze and correlate asset and risk data across their domains. Diagnostic analytics allow for in-depth investigation of the root-causes, patterns and impact associated with identified gaps and threats. Risk-model-graph exploration enables security professionals to identify at-risk assets and resources based on information flow and access patterns and help them implement effective precautionary measures and policies.

Conclusion

Address the challenges of the constantly evolving technology risk landscape with a solution designed from the ground-up to adapt to changes in scope, scale and mandates. Brinqa ITRM leverages powerful and dynamic risk modeling, optimized contextual data collection, state-of-the-art risk and control framework, comprehensive governance and lifecycle management, advanced graph analytics and detailed risk reporting to deliver a complete framework for assessment, monitoring, reporting and treatment of technology risk.

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.