brinqa

SOC 3 Report

System and Organization Controls Report on the Suitability of the Design and Operating Effectiveness of Controls

Description of the Brinqa Cyber Risk Management Platform for the period December 1, 2022, to November 30, 2023

Prepared in Accordance with the AICPA's SSAE No. 18

Table of Contents

Section I – Report of Independent Accountants 1
Section II – Assertion of Brinqa, Inc.'s Management 4
Attachment A – Brinqa's Description of the Boundaries of Its Brinqa Cyber Risk Management Platform 6
Company Background 6
Leadership 6
Brinqa Cyber Risk Management Platform 6
Infrastructure & Software 8
People 8
Data 8
Processes & Procedures 9
Complementary Subservice Organization Controls 9
Complementary User Entity Control Considerations 10
Attachment B – Principal Service Commitments & System Requirements 13

Section I

Independent Service Auditor's Report on a SOC 3 Examination

Section I – Report of Independent Accountants

risk3sixty Compliance, LLC
408 South Atlanta Street
Suite 180
Roswell, GA 30075

To: Brinqa, Inc.

Scope

We have examined Brinqa, Inc.'s ("Brinqa's" or "the Company's") accompanying assertion titled "Assertion of Brinqa, Inc. Management" (assertion) that the controls within the Brinqa Cyber Risk Management Platform (system) were effective throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *217 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Brinqa is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved. In Section II, Brinqa has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Brinqa is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Brinqa's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Brinqa's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Brinqa Cyber Risk Management Platform were effective throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

risk3sixty compliance, LLC

Roswell, Georgia
January 16, 2024

Section II

Assertion of Brinqa, Inc.'s Management

Section II – Assertion of Brinqa, Inc.'s Management

January 16, 2024
Brinqa, Inc.
3700 N Capital of Texas Hwy | Suite 350
Austin, TX 78746

We are responsible for designing, implementing, operating, and maintaining effective controls within the Brinqa Cyber Risk Management Platform (system) throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that Brinqa's service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *217 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Brinqa's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2022, to November 30, 2023, to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Brinqa's controls operated effectively throughout that period.

Attachment A

Description of the Brinqa Cyber Risk Management Platform

risk3sixty

Security | Privacy | Compliance

Attachment A – Brinqa's Description of the Boundaries of Its Brinqa Cyber Risk Management Platform

Company Background

Brinqa is a leading provider of knowledge-driven, risk-based cybersecurity solutions. Brinqa Cyber Risk Graph, the knowledge graph for cybersecurity, connects relevant security and business data, establishes common data ontology, and powers cybersecurity decisions and outcomes. Brinqa solutions apply this knowledge to uniquely inform risk management strategies, standardize data management and analysis, deliver actionable insights, and automate risk remediation. Brinqa delivers all the tools needed to implement risk-based cybersecurity packaged in a high-performance, enterprise-grade platform that addresses critical cybersecurity challenges such as Asset Management, Vulnerability Management, Application Security, and Cloud & Container Security. Brinqa solutions evolve with the business and provide a stable and robust cybersecurity foundation that supports and enables true digital transformation.

Brinqa was founded in 2008 by industry leaders in risk management with a proven track record in delivering cutting edge, innovative, and cost-effective solutions. Brinqa's award winning software and cloud services are trusted by Fortune 500 companies across risk disciplines such as asset management, vulnerability risk, and application security. Brinqa is headquartered in Austin, Texas and has a global presence.

Leadership

Brinqa's leadership team brings over 60 years of risk management and security software expertise that enables the Company to deliver effective, knowledge-driven cyber risk management solutions. The Company has organized their leadership and defined information security policies to ensure alignment with business objectives and to adequately serve their clients. Top management reviews the Company's organizational structure and security policies at least annually as part of strategic planning, and they have defined standards of conduct for their employees.

Brinqa Cyber Risk Management Platform

The Brinqa Cyber Risk Management Platform includes solutions such as Vulnerability Risk Service and Application Security Risk Service. Brinqa solutions are built for security; transforming IT, context, and threat data into knowledge-driven insights that empower organizations to own their cyber risk.

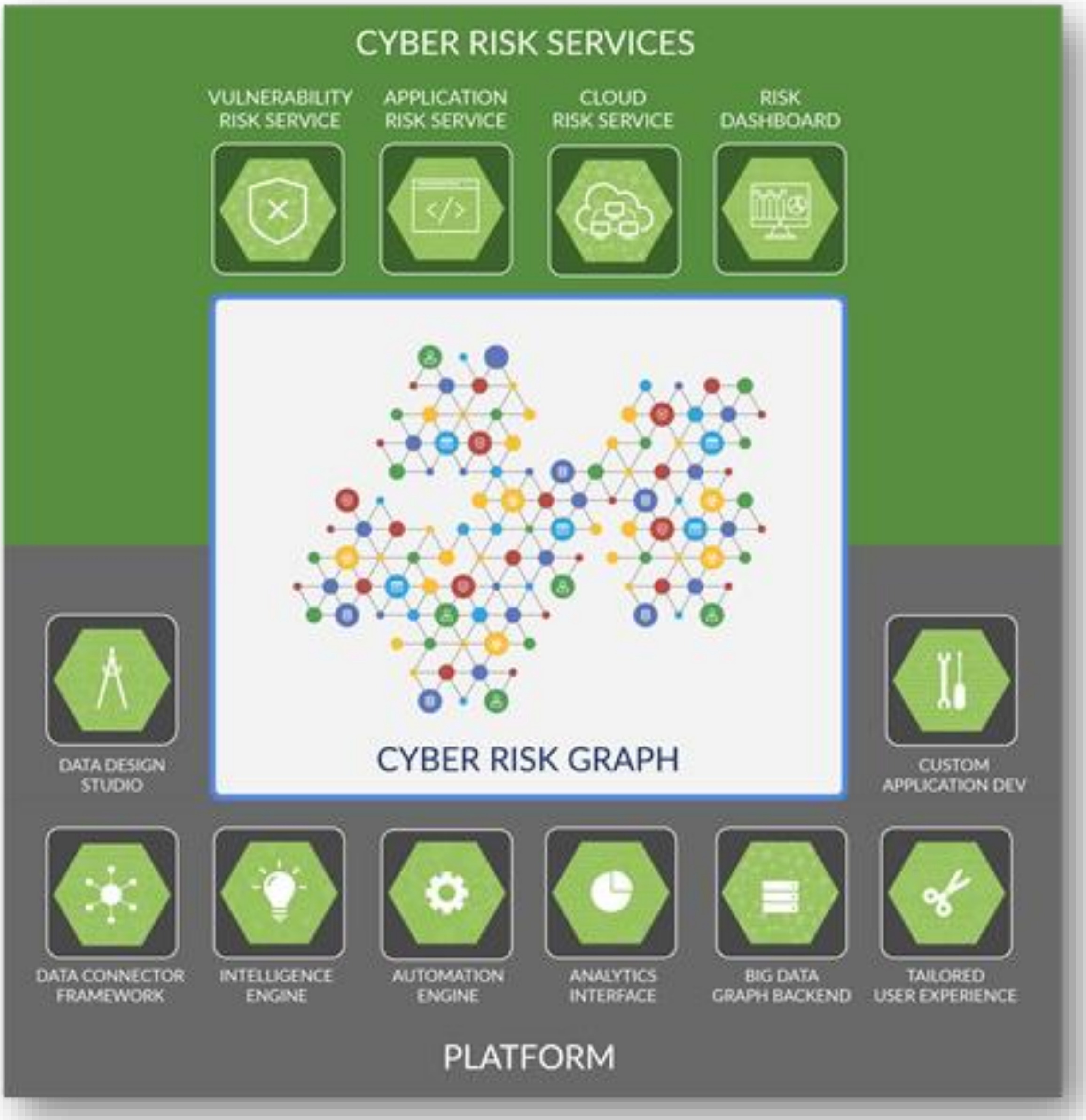
Vulnerability Risk Service

Brinqa Vulnerability Risk Service connects, models, and analyzes all relevant security, context, and threat data to deliver knowledge-driven insights for vulnerability prioritization, remediation, and reporting. The comprehensive solution delivers effective asset management; helps evaluate and visualize each asset's overall business context, impact, and value; enables users to accurately enumerate, prioritize, and address vulnerabilities; and facilitates continuous improvement of the vulnerability management practice.

Application Risk Service

Brinqa Application Risk Service brings together development and security systems and processes across every stage of the software development lifecycle (SDLC) to deliver a unified, risk-aware application security program. The comprehensive solution provides complete visibility into an organization's varied software assets; automates the process for prioritizing and fixing the most critical issues at all stages of the SDLC; and promotes developer-centric security across the software development environment.

System Diagram



Infrastructure & Software

The primary infrastructure and software used to provide Brinqa's Cyber Risk Management Platform service includes the following:

Primary Infrastructure & Software	
Platform	Purpose
Google Cloud Platform	Virtual machines running Linux operating systems; virtualized networking infrastructure; firewall services; snapshots and backups.
Jira	Change management workflow and ticketing
BigQuery	Log management
Vault	Secrets management
Datadog	Monitoring and security, Cloud SIEM
Brinqa	Cyber risk management

People

The Brinqa staff provides support for the above services in each of the following functional areas:

- Executive Management – Provides general oversight and strategic planning of operations.
- Research & Development Team – Responsible for delivering a responsive system that fully complies with the functional specifications.
- Quality Assurance Team – Verifies that the system complies with the functional specification through functional testing procedures.
- System Administrators – Responsible for effective provisioning, installation and configuration, operation, and maintenance of systems hardware and software relevant to the system.
- Customer Success – Serves customers by providing product and service information that includes resolving product and service issues.
- Professional Services – Serves customers by providing product and service deployments.
- Audit & Compliance – Performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements.
- People – Provides oversight of all areas from recruiting to exit of all human resources.
- Finance & Business Operations – Responsible for all aspects of finance, legal and overall fiduciary obligations for the business.
- Sales & Marketing – Responsible for the overall sales cycle.

Data

The client's production data is managed, processed, and stored in accordance with the relevant data and financial compliance requirements and other regulations. Several modules within the system work together to import vulnerabilities, issues, and findings from any integration point such as existing security tools, threat feeds, ticketing system, or database.

Processes & Procedures

Formal IT policies and procedures describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Brinqa policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any team member.

- Access, authentication, and authorization
- Risk management and incident response
- Change management
- Information security
- Business continuity
- Data Backup and disaster recovery
- System monitoring
- Vulnerability monitoring and management

Complementary Subservice Organization Controls

The Company utilizes subservice organizations to perform certain functions to improve operating and administrative effectiveness. The accompanying description includes only policies, procedures, and control activities at the Company and does not include policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditors did not extend to policies and procedures at these subservice organizations. The Company conducts regular assessments of its service providers (review of SOC reports, regular meetings, annual vendor questionnaires, etc.) in order to collect, track, and manage third party security controls based upon the risk presented to the business. The subservice organizations related to the scope of the system are shown below:

Service Provider	Description of Services	Relevant Criteria
Google Cloud Platform (GCP)	Platform-as-a-Service including infrastructure, data center hosting services, web application firewall services, and backup storage and encryption.	CC6.4*, CC7.2*, CC7.5*

**Subservice organization is complementary to the criteria*

Complementary subservice organization controls (CSOCs) are controls that Brinqa's management assumed, in the design of the system, would be implemented by their subservice organization and are necessary, in combination with controls at Brinqa, to provide reasonable assurance that Brinqa's service commitments and system requirements were achieved. The following subservice organization is responsible for the respective CSOCs and Brinqa's related service commitments and system requirements can be achieved only if the CSOCs are suitably designed and operating effectively during the period addressed by the description.

Complementary Subservice Organization Controls (CSOCs) – Google Cloud Services		
Category	**Criteria**	**Applicable Controls**
Security	CC6.4	GCP is responsible for implementing and maintaining physical access controls to data centers hosting Brinqa production infrastructure.
	CC7.2	GCP is responsible for monitoring the critical production servers for anomalies indicative of malicious acts, natural disasters, and errors.
	CC7.5	Critical system components are replicated across multiple Availability Zones and backups are maintained. GCP is responsible for ensuring that datacenters hosting Brinqa's production infrastructure are included in a disaster recovery plan.

Complementary User Entity Control Considerations

The processes of the Company were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve the Applicable Trust Services Criteria included in this report.

This section highlights those internal control responsibilities that the Company believes should be present for each user organization and has considered in developing its control policies and procedures described in this report. In order for users to rely on the control structure's policies and procedures reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place.

Furthermore, the following list of control policies and procedures is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user. Accordingly, this list does not allege to be, and is not, a complete listing of the control policies and procedures that provide a basis for management's assertions related to the Applicable Trust Services Criteria.

Complementary User Entity Controls (CUECs)		
Category	**Criteria**	**Applicable Controls**
Security	CC2.3	**Terms of Service:** The Customer is responsible for ensuring that their end-users abide by the same terms of service as those by which the customer is bound.
	CC6.1 CC6.2 CC6.6	**Access Control:** Users are provisioned administrative access to their Brinqa environment upon onboarding. End-users are responsible for provisioning and de-provisioning end-user access in their environment. The Customer is responsible for implementing compensating controls to satisfy their security requirements for application authentication (including controls to ensure that user passwords remain confidential).
	CC7.1	**API Access:** The Customer is responsible for restricting access to and monitoring the use of Application Programming Interfaces (APIs) available in the Brinqa environment.

Complementary User Entity Controls (CUECs)		
Category	Criteria	Applicable Controls
	CC2.3 CC7.5	**Reporting Issues:** Users are responsible for immediately notifying Brinqa management of any actual or suspected information security breaches, including compromised user accounts.
	CC8.1	**Change Notifications:** Users are notified of application updates in the Brinqa notification dashboard. Users are responsible for reviewing those notifications. The Customer is responsible for validating and testing their product release.

Attachment B

Principal Service Commitments & System Requirements

risk3sixty

Security | Privacy | Compliance

Attachment B – Principal Service Commitments & System Requirements

Brinqa designs its processes and procedures related to its information security and risk management software as a service solution to meet its objectives for its Brinqa Cyber Risk Management Platform. Those objectives are based on the service commitments that Brinqa makes to user entities; the laws and regulations that govern the provisioning of its services; and the financial, operational, and compliance requirements that Brinqa has established for the services.

Service commitments to user entities are documented and communicated in Customer Agreements and on the Legal page published on its public website. Service commitments are standardized and include, but are not limited to, the following:

Brinqa will protect the confidentiality and integrity of the Brinqa Cyber Risk Management Platform and all customer information.

- All data classified as potentially sensitive is encrypted at the database level while at rest.
- All data in transit is encrypted, including the following:
  - Information transmitted over the public internet (HTTPS)
  - Data transferred within system components (TLS)
- The network perimeter is controlled with firewalls configured to prevent access based on pre-defined access control lists. Firewalls monitor the network, and the network administrators receive notification of issues detected by the system based on pre-defined alert thresholds.
- The Company has implemented mobile device management (MDM) tools that enforce mobile device hardening (including laptops and mobile phones) and have the ability to remotely wipe devices, if needed. MDM tools are implemented on all devices that are used to store or access sensitive company data.

Brinqa will implement Security and Privacy principles within the fundamental structure of the platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

- The Company has logically segmented its network so that unrelated portions of the information system are isolated from each other.
- Administrative level access to the Company's critical systems (Network, Application, Source Code, and Databases) is limited to appropriate individuals based on job function and current employment with the Company.
- Management performs a periodic user access review of all in-scope systems (application, network, source code, databases) at least quarterly. Any issues identified are tracked to final remediation.

Brinqa will communicate all relevant information clearly with all internal and external stakeholders.

- Security events that may impact internal or external users, including breaches of sensitive information or loss of service, are communicated to the impacted parties in line with contract and regulatory requirements.
- The Company communicates relevant security and privacy commitments, made available on its public-facing website or by written request.
- When major changes to security commitments are made, the Company communicates these changes to impacted stakeholders via updated commitments on the Company’s public-facing website.

Brinqa will proactively monitor their environment to identify and mitigate all risks to the business.

- The company has defined and implemented a risk management process, overseen by top-level management, that includes identification of risks, the process for evaluating risks based upon identified threats, likelihood, impact, and the Company's specified risk treatment plans. A formal risk assessment is completed bi-annually.
- The Company performs continuous internal vulnerability scans of the system. Management assesses and prioritizes the results of the scans and tracks issues of medium criticality or above to final remediation.
- The Company engages a third-party to perform external penetration tests of the system on an annual basis. Management assess and prioritizes the results of the penetration test and tracks issues of medium criticality or above to final remediation.
- The Company leverages system monitoring tools to review and report on system performance in order to support the functioning of internal control.

Brinqa will ensure the security, confidentiality, and integrity of data coming in contact with third parties.

- The Company has established a third-party risk management program and conducts annual assessments of its service providers in order to collect, track, and manage third-party security controls based upon the risk presented to the business. Any issues identified during the assessment are tracked through to remediation.
- The Company has implemented a vendor risk management policy that manages risks associated with vendors and business partners.
- Corporate Master Services Agreements (MSA) are established to help define third-party requirements for maintaining security and related regulatory and policy commitments for Tier 1 vendors.

Brinqa will ensure logical access controls limit access to customer data to only authorized users.

- The Company has implemented role-based access controls that limit access to sensitive information to only those individuals who require access based on job function, active employment, and management approval.
- Access to promote source code to the production environment is limited to only appropriate individuals based on job function and active employment with the Company.
- Administrative level access to critical system components (including databases and system infrastructure components) is restricted to appropriate individuals based on job function and current employment with the Company.

Brinqa will ensure that security monitoring is in place to verify controls are working as designed.

- The Company leverages system monitoring tools to review and report on system performance in order to support the functioning of internal control.
- The Company has designated the CIO and Director of Information & Risk as responsible for monitoring controls and commitments related to company security practices. Top-level management reviews the results of internal and external security assessments on a quarterly basis. Results of these reviews are integrated into management strategy and business objectives and tracked to final remediation.
- The Company has implemented detection and monitoring tools to identify anomalies, including potential changes to configurations that result in the introduction of new vulnerabilities as well as

susceptibilities to newly discovered vulnerabilities. Management receives alerts based on pre-defined thresholds which are logged and tracked to final remediation.

Brinqa establishes operational and system requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Brinqa’s system policies and procedures, system design documentation, and in contracts with customers. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained.