Quickbase, Inc.

Report on Controls at a Service Organization Relevant to Security, Confidentiality, Availability

SOC 3®

For the Period July 1, 2022 to June 30, 2023

Independent Service Auditor’s Report

To the Management of Quickbase, Inc. (“Quickbase”):

Scope

We have examined Quickbase’s accompanying assertion titled "Assertion of Quickbase Management" (assertion) that the controls within the Quickbase Platform (system) were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Quickbase's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Service Organization’s Responsibilities

Quickbase 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 Quickbase's service commitments and system requirements were achieved. Quickbase has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Quickbase 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 Quickbase's service commitments and system requirements based on the applicable trust services criteria; and,
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Quickbase's service commitments and system requirements based on the applicable trust services criteria.

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

Relevant Ethical Requirements

We are required to be independent of Quickbase and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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 Quickbase Platform were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Quickbase's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

BARR Advisory, P.A.

Fairway, KS

August 15, 2023

Assertion of Quickbase Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Quickbase's Quickbase Platform (system) throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that Quickbase's service commitments and system requirements relevant to security, confidentiality, and availability were achieved. Our attached system description of the Quickbase Platform identified 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 July 1, 2022 to June 30, 2023, to provide reasonable assurance that Quickbase's service commitments and system requirements were achieved based on the trust services criteria relevant to security, confidentiality, and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). Quickbase'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 the attached system description.

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 July 1, 2022 to June 30, 2023, to provide reasonable assurance that Quickbase's service commitments and system requirements were achieved based on the applicable trust services criteria.

Quickbase, Inc.

August 15, 2023

Overview of Operations

Company Background

Headquartered in Boston, Massachusetts, Quickbase provides a low code operational agility platform that enables organizations to improve operations through real-time insights and automation of complex processes across disparate systems. Quickbase's goal is to help companies achieve operational agility—to be more responsive to customers, more engaging to employees, and as adaptable as possible to what's next.

Description of Services Provided

Quickbase is a low-code application development platform that enables users to create custom business applications that manage their data and processes. The Quickbase Platform (the "system") includes the following key capabilities:

- Data management
- Custom forms
- Visual app building
- Automations
- Integrations
- Governance
- Mobile
- App marketplace

In addition to the Quickbase core platform, Quickbase provides the following optional ancillary services:

- **Quickbase Audit Logs:** Provides Quickbase customer administrators with a record of user activity, app data, and app schema changes. Customers may choose to retain logged data for six months, one year, three years, or seven years. Quickbase Audit Logs provides realm admins with the functionality to monitor adherence to their organization's security standards and compliance policies.
- **Quickbase JavaScript Object Notation (JSON) RESTful application programming interface (API) Gateway:** Provides API access to Quickbase apps over Hypertext Transfer Protocol (HTTP) with JSON payloads.
- **Quickbase Pipelines:** Quickbase Pipelines enables application developers to access data and integrate to external systems and orchestrate workflows using simple business logic.
- **Quickbase Sync:** A data integration feature that allows Quickbase application builders to integrate their Quickbase applications with third-party services such as Salesforce and NetSuite, file services like Dropbox and Box, and email services.
- **Quickbase Webhooks:** An integration and workflow automation capability that enables Quickbase to notify, a Quickbase application, cloud application, or web-enabled, on-premise system about changes in Quickbase data.

- **Quickbase Pipelines:** Enables Quickbase customers to integrate their Quickbase application data with third-party services, such as Slack, Gmail, OneDrive, or virtually any system with a RESTful API, and automate processes between disparate systems via triggers and actions. Using a visual interface, Quickbase builders can design pipelines that specify what and how data flows between applications. You can build complex pipelines that:
  - Span disparate cloud and on-premise systems
  - Have many steps in them
  - Include conditional branching and iteration over collections of records
  - Transform data using a powerful template engine
  - Use date and time conversions
  - Schedule pipelines to run at selected intervals

Users can also leverage a multi-part workflow that strings many pipelines together, where one pipeline triggers another in succession.

While Quickbase Pipelines is part of Quickbase, customers do not need to have a Quickbase application as part of their workflow. Pipelines can be used between any combination of supported channels.

Components of the System Used to Provide the Services

The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure

The core Quickbase Platform is hosted at Flexential Tier IV Data Centers located in North Las Vegas, Nevada, and Englewood, Colorado.

Additionally, Quickbase utilizes Amazon Web Services's (AWS) US-West region for platform features including Quickbase Audit Logs, Quickbase JSON RESTful API Gateway, Quickbase Sync, and Quickbase Webhooks.

Quickbase utilizes Google Cloud Platform (GCP) US-Central region for Quickbase Pipelines. Quickbase utilizes Microsoft Azure to host active directory.

A multi-tier network topology and security architecture protects the components of the platform from unauthorized external access. The network topology includes segmented virtual local area networks (VLANs) and AWS virtual private cloud (VPC) networking segregation. Quickbase employs a third party edge network, via Cloudflare, that complements and protects the platform. The hosted platform utilizes stateful packet inspection firewalls and network load balancers.

Remote access to the Quickbase corporate network and administrator access to the Quickbase Platform requires an encrypted virtual private network (VPN) connection and requires multi-factor authentication (MFA).

The hardware components that make up the core Quickbase Platform include the following:

- **Server hardware:** Cisco Unified Computing System (UCS) servers.
- **Network components:** Cisco switches, Palo Alto firewalls, and F5 local traffic managers (LTMs).
- **Storage hardware:** NetApp filers.

Redundancy is achieved within each data center via server clustering, Internet Protocol (IP) and domain name service (DNS) load balancing, and multiple internet service providers (ISPs). Data is continuously replicated from the primary data center to the hot standby disaster recovery data center.

Software

Quickbase is responsible for managing the development and operation of the Quickbase Platform including maintenance of infrastructure components such as servers, databases, and storage systems hosted in the colocation data centers.

People

The following Quickbase personnel are involved in the operation of the system:

- **Board of Directors:** Responsible for oversight and strategic guidance.
- **Executive Leadership:** Responsible for overseeing business-wide activities, establishing and accomplishing strategic goals, and overseeing objectives.
- **Enterprise Risk Committee (ERC):** Responsible for enterprise risk management oversight including but not limited to establishing, monitoring, and approving action plans. Membership includes the members of the board of directors and executive leadership.
- **Security and Compliance:** Responsible for overseeing the governance, risk, third-party risk management, compliance and security programs, including the development of information security policies, monitoring of compliance with internal controls and frameworks, and reporting to executive leadership on developments in governance, risk, and control.
- **Risk Oversight Steering Committee:** Responsible for the identification, evaluation and mitigation of operational, technical, strategic, and external environment risks and the maintenance of the enterprise risk register. The risk oversight steering committee is a cross-functional team that includes members of security and compliance, product, finance, IT, customer success, employee experience (EX), and legal.
- **Site Reliability Engineering (SRE):** Responsible for the engineering and maintenance of Quickbase's infrastructure components, deployment of changes, and monitoring the Quickbase services.
- **Systems Quality Team (SQT):** Improves the quality and stability of software products and processes through the value-added delivery of system-level testing and release support.
- **Customer Success:** Responsible for providing prompt response and resolution to customer technical issues; key personnel within this group include technical support representatives and support managers.
- **Product Development:** Responsible for the development and testing of the Quickbase Platform code; key personnel within this group include program and product managers, developers, and system quality assurance (SQT) engineers.

- **Employee Experience (EX):** Responsible for communicating and overseeing EX policies and procedures with a focus on key EX areas, such as talent acquisition, employee retention, compensation, performance management, employee relations, and career development.
- **General Counsel/Legal:** Responsible for compliance with applicable laws and regulations in the jurisdictions that Quickbase operates as well as the agreements that Quickbase executes with its customers, vendors, and other third-parties.
- **IT:** Responsible for the deployment and management of Quickbase's corporate information technology services.
- **Business Enablement:** Develops and enhances Quickbase applications used to support Quickbase business and operations workflows and processes.
- **Architecture Review Board (ARB):** Assess risk related to new product developments. The ARB is a cross-functional team that includes the chief architect, chief security and compliance officer, VP of platform operations, developers, and systems architects.

Data

Quickbase has data classification and handling guidelines that govern information labeling and handling, in accordance with guidelines established in company policy, customer agreements and applicable regulations. All data is to be assigned one of the following sensitivity levels:

Classification Levels	Description	Example(s) of Data
Public	Public information has been approved for release to the general public and is freely shareable both internally and externally.	• Information published on the Quickbase website • Published blog posts and press releases
Internal	Internal information is potentially sensitive and generally should not be disclosed outside of Quickbase without the express permission of the person or group that created and maintains the information.	• Employee handbook • Company policies, procedures, and guides • Presentations, memos, correspondence, and meeting minutes
Confidential	Confidential information is highly-valuable or proprietary, sensitive information that, if made available to unauthorized parties, may adversely affect individuals or the business of Quickbase.	• Intellectual property • Potential or actualized security or privacy incidents • Quickbase financial data
Restricted	Restricted information is highly-valuable, highly-sensitive information and the level of protection is dictated externally by legal, regulatory, and/or contractual requirements.	• Customer application data • Source code • Public key infrastructure (PKI) cryptographic keys

Quickbase categorizes all data entered into the system by customers as restricted as it may include personally identifiable information (PII), electronic protected health information (ePHI), and controlled unclassified information (CUI). A business associate agreement (BAA) is in place with AWS due to the presence of ePHI in the Quickbase Platform components hosted in AWS data centers.

Data is received by the Quickbase web servers from users' web browsers or using APIs, and encrypted during transit using a 256 bit (SHA2) over TLS version 1.2 or 1.3 connection. Network load balancers forward requests to web servers that forward requests to Quickbase app servers, where the requests are executed and responses returned to the user's web browser, or originating client (for API calls). The following types of data are collected and stored in the Quickbase Platform:

Term	Description	Examples
Customer Data	Data entered into fields by users of a specific Quickbase application.	● The value **Ed** being placed into a field called **First Name**
Customer Schema (i.e., Metadata)	Information that describes an application, entered by builders or administrators, and inferred outcomes.	● The applications name is **Quality Control Management** ● The owner of the application is **Jane Doe** ● The table name called **Products**
Analytical Information	Non-customer specific aggregate information.	● Average monthly recurring revenue (MRR) of applications that use email notification

- **Collecting data:** Quickbase users can import data from an existing application, or they can add, edit, and delete information directly in Quickbase by filling in customizable forms. Customers can also use integrations, code, and other tools to get data into Quickbase via XML and JSON APIs.
- **Managing data:** Quickbase allows users to create custom reports, automated graphs, charts, tables, and summary views.
- **Sharing data:** As a web-based database, Quickbase allows users to share information among team members, customers, and/or partners in real time. Quickbase also gives users complete control of their information. Users set custom roles and permissions to determine each team member's level of access to data so they only see the right information.
- **Integrating data:** When used in conjunction with Quickbase Sync, Quickbase custom applications can be integrated with other third party web-based applications, allowing users to automatically sync data between Quickbase and those other third party web-based applications.
- **Logging data:** When used in conjunction with Quickbase Audit Logs, Quickbase realm admins can view user activity logs including changes made to data and schema.
- **Deleting data:** Customer application data is automatically deleted from the production platform upon initiation from the customer and held in Quickbase backup systems for six months. Upon data being fully purged from Quickbase backup systems, Quickbase will send authorized customer contacts a certificate of data destruction via email.

Processes and Procedures

Quickbase has developed and communicated policies and procedures to manage the information security of the system. Policies are reviewed on an annual basis and changes are made to the policies when necessary. Policies are approved by the security and compliance team on an annual basis. The following policies and procedures are in place:

- Access Control (AC) Policy
- Assessment, Authorization, and Monitoring (CA) Policy
- Audit and Accountability (AU) Policy
- Awareness and Training (AT) Policy
- Configuration Management (CM) Policy
- Contingency Planning (CP) Policy
- Data Classification Policy
- Free and Open Source Software Policy
- Identification and Authentication (IA) Policy
- Incident Response (IR) Policy
- Maintenance (MA) Policy
- Media Protection (MP) Policy
- PII Processing and Transparency Control Policy
- Personnel Security (PS) Policy
- Physical and Environmental Protection (PE) Policy
- Planning (PL) Policy
- Program Management (PM) Policy
- Risk Assessment (RA) Policy
- Supply Chain Risk Management Policy
- System and Communication Protection (SC) Policy
- System and Information Integrity (SI) Policy
- System and Service Acquisition (SA) Policy
- Technology Acceptable Use Policy (AUP)

Principal Service Commitments and System Requirements

Quickbase designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Quickbase makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that Quickbase has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services. Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role;
- Training and resourcing to enable builders to make sound security decisions;
- Use of firewalls and intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Continuous vulnerability scans over the Quickbase website, weekly vulnerability scans for the colocation network, and annual penetration tests covering the production platform;
- Operational procedures for managing security incidents and breaches, including notification procedures; and,
- Operational procedures supporting the achievement of security, availability, and confidentiality commitments to user entities.

Confidentiality commitments include, but are not limited to, the following:

- Contractual obligations of data privacy and compliance with data privacy laws;
- The use of encryption technologies to protect Quickbase application data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between Quickbase and user entities.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to ensure the consistent delivery of the Quickbase Platform and its components;
- Contractual commitments to platform uptime based on customer specific SLAs negotiated in master service agreements (MSAs) or the default terms of service;
- Responding to customer requests including the restoration of customer applications;

- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities; and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in Quickbases's system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems are protected. These include policies around how the service is designed and developed, how the service is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the service. Information security policies, including sanctions for policy violations, are approved by management at least annually and published on internal collaboration tools (i.e., Quickbase Internal) accessible to all personnel with access to the company systems.