Quickbase, Inc.
Report on Controls at a Service Organization Relevant to Security, Confidentiality, and Availability

SOC 3SM Report

For the Period July 1, 2020 to June 30, 2021

SOC 3 is a registered service mark of the American Institute of Certified Public Accountants (AICPA)
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 were effective throughout the period July 1, 2020 to June 30, 2021, 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.

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, 2020 to June 30, 2021, 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.

Fairway, KS
August 6, 2021
Assertion of Quickbase Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Quickbase platform throughout the period July 1, 2020 to June 30, 2021, 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, 2020 to June 30, 2021, to provide reasonable assurance that July 1, 2020 to June 30, 2021’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, 2020 to June 30, 2021, to provide reasonable assurance that Quickbase's service commitments and system requirements were achieved based on the applicable trust services criteria.

Quickbase, Inc.
August 6, 2021
Overview of Operations

Company Background

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. Our 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. Quickbase helps nearly 6,000 customers, including over 80 percent of the Fortune 50. Visit quickbase.com to learn more.

Description of Services Provided

Quickbase is a low-code application development platform that enables users to quickly and easily create custom business applications that manage their data and processes. The Quickbase core platform 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 Webhooks**: An integration and workflow automation capability that enables Quickbase to notify, in real time, a Quickbase application, a cloud application, or a web-enabled, on-premise system about changes in Quickbase data.

- **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 Pipelines**: Quickbase Pipelines enables application developers to access data and integrate to external systems and orchestrate workflows using simple business logic.

- **Quickbase Audit Logs**: Provides Quickbase customer administrators a record of user activity, app data, and app schema changes within a customer realm. 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.
**Principal Service Commitments and System Requirements**

Quickbase designs its processes and procedures related to the Quickbase platform to meet its objectives and commitments to customers, legal and regulatory requirements that govern Quickbase services, and the financial, operational, and compliance requirements that Quickbase has established internally for its services. Security, confidentiality, and availability commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

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

- Features and configuration settings designed to enable Quickbase application builders to build applications which permit access to users based on authorization, which may be, for example, based on their Quickbase platform role or membership in a group, while restricting unauthorized users from accessing information not needed for their role;
- Use of firewalls and intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system;
- Regular vulnerability scans over the Quickbase website and network, and 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 commitments to user entities, and of the HIPAA Security Rule and DFARS.

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

- The use of encryption technologies to protect Quickbase platform 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;
- Responding to customer requests including the restoration of customer apps;
- 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.

**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 and Software

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 AWS's US-West region for platform features including Quickbase Webhooks, Quickbase Sync, and Quickbase Audit Logs. Quickbase utilizes Google Cloud Platform US-Central region for Quickbase Pipelines.

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. Customer requests to the Quickbase web applications are encrypted using Transport Layer Security (TLS) supported by certificates from an established third party certificate authority. Certificates are monitored and rotated prior to expiration.

Remote access to the Quickbase corporate network and administrator access to Quickbase production infrastructure systems requires an encrypted VPN connection and requires multi-factor authentication. Additionally, Quickbase platform data and file attachments are encrypted at the application layer using Advanced Encryption Standard (AES) 256-bit encryption.

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

- **Server hardware**: Cisco UCS servers; and,
- **Network components**: Cisco switches, Palo Alto firewalls, and F5 local traffic managers (LTMs).

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.

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.

The core Quickbase platform including web, app and database servers as well as servers that support Quickbase Sync, utilize a Microsoft Active Directory domain separate and independent from the Corporate Active Directory domain. The application, web and database servers run on Microsoft Windows operating systems. Metadata (e.g., user credentials and session information) are stored in a Microsoft SQL database. Quickbase applications when accessed are loaded in the proprietary in-memory database. Files that contain app data are encrypted at the application layer and stored in AES 256-bit encrypted format on flat files on the NetApp storage arrays where files are backed up and replicated to the alternate data center.

Customers access Quickbase applications via the internet using any modern web browser. Quickbase employees authenticate via a user account and password. Additionally, Quickbase employees can utilize the single sign-on (SSO) federation of authentication via SAML 2.0.
Quickbase Webhooks, Quickbase Sync, and Quickbase Audit Logs are built in Amazon AWS using AWS services residing in a virtual private cloud (VPC). Services that support the system include:

- **Elastic Compute Cloud (EC2):** Provides Infrastructure as a Service (IaaS) to Quickbase for scalability and hosts the application logic, Postgres databases, and service components.

- **Elastic Container Services (ECS):** A highly scalable, high-performance container orchestration service that supports Docker containers running Quickbase services.

- **Relational Database Service for PostgreSQL (RDS for PostgreSQL):** Scalable high performance relational database service supporting Quickbase services.

- **Simple Storage Service (S3):** Provides a web interface used to store and retrieve data from anywhere on the web. S3 APIs provide both bucket- and object-level access control. Quickbase uses S3 to store the application data files and file uploads. S3 is on a private cloud and controlled through the AWS IAM interface. Data is stored as files and may contain packets classified as confidential. S3 buckets containing sensitive data are encrypted both in transit and at rest.

- **Identity and Access Management (IAM):** Controls access to Amazon services at the user, operation, and cluster level.

- **Elastic Load Balancer (ELB):** Load balancer that automatically distributes Quickbase traffic across multiple EC2 instances.

Quickbase Pipelines is built in the Google Cloud Platform utilizing the Google Cloud App Engine. Google Cloud services that support the system include:

- **Cloud Tasks:** Facilitates workload distribution.

- **Cloud Storage:** Transitional storage needed during execution of some pipeline instances.

- **KMS:** Stores Realm level encryption key and performs envelope encrypt/decrypt of Data Encryption Keys.

- **Stackdriver:** Performance monitoring and diagnostics.

- **BigQuery:** Statistical usage data. No customer data is saved in BQ.

- **Memcache:** Operational data cache and distributed locking. If customer data is put in the cache, it is prior encrypted on the app-level with a DEK. Provided and operated by Google Cloud as part of App Engine Standard Environment.

- **Cloud Data Store:** Main application database. Stores both long-living and transitional data. Long living data includes user profile, pipeline definitions, channel accounts credentials, and pipeline execution audits. Transitional data includes operational info needed during the execution.

**People**

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

- **Senior Leadership Team:** Responsible for overseeing business-wide activities, establishing and accomplishing strategic goals, and overseeing objectives.

- **Security and Compliance Team:** Responsible for overseeing the Compliance and Security Program including the development of information security policies, monitoring of compliance with internal controls and frameworks, and reporting to senior leadership on developments in governance, risk, and control.
● **Site Reliability Engineering (SRE) Team**: Responsible for the engineering and maintenance of Quickbase's infrastructure components and the 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 Team**: 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 Team**: Responsible for the development and testing of the Quickbase platform code; key personnel within this group include program managers, developers, and quality assurance (SQT) engineers.

● **Human Resources (HR)**: Responsible for communicating and overseeing HR policies and procedures with a focus on key HR areas such as talent acquisition, employee retention, compensation, performance management, employee relations, and career development.

● **IT Team**: Responsible for the deployment and management of Quickbase's corporate information technology services.

● **Business Enablement Team**: Develops and enhances Quickbase applications used to support Quickbase business and operations workflows and processes.

● **Architecture Review Board**: Assess risk related to new product developments. The ARB is a cross-functional team that includes the Chief Architect, the Chief Security and Compliance Officer, the VP of Platform Operations, developers, and systems architects.

**Procedures**

Documented information security policies and procedures are in place to guide IT and operations personnel in information security administration processes, including, but not limited to: acceptable usage, access provisioning, password management, change management, incident response, physical access procedures, confidentiality, and data retention and classification. These policies are reviewed by management on at least an annual basis, and updated as necessary.

Security, confidentiality, availability, and regulatory obligations and commitments are communicated to employees and authorized users of the Quickbase platform through security awareness training that is completed as part of onboarding procedures, and annually thereafter.

The policies and procedures used to safeguard the Quickbase platform includes:

- Information Security Oversight
- Data Classifications and Responsibilities
- Audit and Accountability
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Security Incident Response
- Mobile Devices
Data

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. Data is encrypted by the Quickbase platform, and then stored in flat files on storage arrays in the Flexential colocation data centers. Metadata (e.g., user credentials and session information) are stored in a Microsoft SQL database. Quickbase functionality allows for the following:

- **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.

- **Managing data**: Quickbase allows users to create custom reports, automated graphs, charts, tables, and summary views by removing overwrites or manual data consolidation.

- **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.

- **Syncing 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. Quickbase purges customer data from the online Quickbase platform upon service termination. After which, data will be 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.

Quickbase Sync, Quickbase Webhooks, and Quickbase Audit Logs are optional Quickbase services hosted in Amazon AWS US-West region. These services utilize core functions and APIs to send data from the Quickbase app servers in the Flexential colocation data center to the AWS hosted services.
Quickbase Sync then integrates to third party web-based applications through customer managed connections involving syncing, sharing and alerting as designed by customer-created workflows.

Quickbase Pipelines provides Quickbase customers an intuitive way to integrate their Quickbase application data with third party services such as Slack, Gmail, and OneDrive 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 apps. 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

You can also have 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.

Pipelines is developed in the Python programming language and deployed in Google Cloud App Engine in the US-Central region. Pipelines is structured as a set of App Engine Standard environment services. Quickbase deploys Python code to Google Cloud and delegates responsibility to Google’s Standard Environment for all low-level infrastructure security aspects. Additionally, Quickbase uses the automatic scaling feature of the App Engine Standard Environment to achieve horizontal scalability.

Quickbase has data classification and handling guidelines that govern information labeling, handling, and disposal in accordance with guidelines established in company policy, customer agreements, and applicable regulations. Quickbase categorizes all data entered into the system by customers as confidential 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 encrypted in transit and at rest. Customers are able to create additional access controls to restrict access to their data through the application interface using Quickbase roles and permissions. Quickbase policies prohibit the downloading of any customer confidential data by Quickbase employees from the Quickbase platform and infrastructure environment.

**Achieving High Security**

The Quickbase services are accessed via the internet via encrypted sessions. Quickbase services are only accessible over TLS 1.2 or 1.3. Quickbase customers may use Quickbase as the primary authentication authority or implement single sign-on via SAML 2.0. Customer administrators may configure password and session options applicable to organizational users in the Quickbase administrative portal. Logical access, configured by customer administrators, segregates each customer’s application data, controlled via authentication and authorization, at the realm, account, application, and table layers.
Quickbase's product functionality and system architecture are designed with security as a goal. Quickbase encrypts all information at rest and uses role-based security for Quickbase site administration, customer care, and other administrative roles.

Quickbase integrates security testing into each phase of the development life cycle, including static code security scans and dynamic web scans. Developers complete role-based training on secure code development best practices. Quickbase commissions an annual security penetration test, and supports customers performing their own security assessments.

Quickbase's security, HIPAA, and DFARS requirements and commitments are communicated to third parties through contractual agreements. The Chief Security and Compliance Officers responsible for ensuring contracts are in place for all third parties with access to the Quickbase platform. The Compliance and Information Security Officer is additionally responsible for confirming third party access is authorized and provisioned per these agreements.

**Achieving High Availability**

High availability is one of the most important architectural considerations at Quickbase. In order to help ensure high availability of the Quickbase platform, Quickbase data that resides at Flexential colocation data centers is continuously replicated from the production to the hot standby data center for use in the event of an outage at the primary data center. Quickbase services that reside at AWS are replicated across multiple availability zones in the AWS US-West region. Load balancers are used, where routing is needed, to manage access to multiple assets. Quickbase services that reside at GCP are allocated dynamically by GCP across the US-Central. Dynamic availability is used by Google to manage the availability of those services applications by making them available across all of the zones that make up the specific region.

**Achieving High Performance**

Quickbase is committed to delivering its services in a manner that ensures users of the system are able to use the application at optimal performance. This is accomplished by keeping the code algorithmically efficient, reducing the number of layers, and using caching where applicable. At the database layer, high performance is achieved through a data model designed with appropriate indexes to facilitate access patterns. The results of regularly scheduled performance tests are analyzed and architectural decisions are made to ensure that all applications perform at acceptable levels. Users of Quickbase can view live availability statistics and subscribe to operational updates on Quickbase's public-facing status page at https://service.quickbase.com.

**Monitoring Performance, Scalability, and Availability**

Splunk and Pingdom are used to monitor performance and availability of the services at the Flexential colocation data centers, AWS and GCP environments as well as the public-facing Quickbase website. Paessler PRTG, Datadog are used to monitor the infrastructure at the Flexential colocation data centers and AWS. Additional internally developed Quickbase applications are used to monitor and alert on the performance and availability of Quickbase custom applications. Monitoring tools such as Splunk Enterprise Security, are configured to monitor for, and alert on, security related issues. Quickbase operations personnel are on call 24/7 and have issues escalated to them via the VictorOps service.
Complementary User Entity Controls

Quickbase controls were designed with the assumption that certain internal controls would be in place at customer organizations. The application of such internal controls by customer organizations is necessary to achieve certain criteria identified in this report. In addition, there may be control activities that are not identified in this report that would be appropriate for processing of transactions for Quickbase customers, related to the information processed.

For customers to rely on the information processed through the Quickbase platform, each customer is expected to evaluate its own internal controls to ensure appropriate control activities are in place. The following general procedures are controls that should be considered. They should not, however, be regarded as a comprehensive list of all controls that should be implemented by customer organizations.

- User entity is responsible for managing user accounts including user IDs and password controls, or to configure single sign-on (SSO) within their organization’s Quickbase realm.
- User entity is responsible for reviewing customer access to their Quickbase applications periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to their Quickbase realm and apps.
- User entity is responsible for removing terminated employee access to their Quickbase realm and apps.
- User entity is responsible for implementing policies and procedures over the types of data that are allowed to be entered into their Quickbase realm and apps.
- User entity is responsible for implementing a change and configuration management program over user systems and apps built in the Quickbase platform.
- User entity is responsible for notifying Quickbase if they detect or suspect a security incident related to the Quickbase platform.
- User entity is responsible for reviewing email and other forms of communications from Quickbase, related to changes that may affect the Quickbase customers and users, and their security or availability obligations.
- User entity is responsible for establishing, monitoring, and maintaining controls over the security for system-generated outputs and reports from the Quickbase website.
- User entity is responsible for deleting their own data within the Quickbase website.
Complementary Subservice Organization Controls

Quickbase uses subservice organizations to provide data center hosting, colocation, and infrastructure services in support of its Quickbase platform. Quickbase’s controls related to the Quickbase platform cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria requirements over the Quickbase platform to be achieved solely by Quickbase. Therefore, user entity controls must be evaluated in conjunction with Quickbase’s controls described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Quickbase periodically reviews the quality of the outsourced operations by various methods including:

- Review of subservice organizations’ SOC reports;
- Regular meetings to discuss performance; and,
- Non-disclosure agreements.

<table>
<thead>
<tr>
<th>Control Activity Expected to be Implemented by Subservice Organization</th>
<th>Subservice Organization</th>
<th>Applicable Trust Services Criteria</th>
</tr>
</thead>
</table>
| Physical access to the data center facility is restricted to authorized personnel. | • Flexential  
• AWS  
• GCP | CC6.4 |
| Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements. | • Flexential  
• AWS  
• GCP | CC6.4  
A1.2 |
| Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically. | • Flexential  
• AWS  
• GCP | A1.3 |
| Customer confidential data is identified, maintained, and disposed of per customer agreements. | • AWS  
• GCP | C1.1  
C1.2 |
| Disposal of decommissioned media is sanitized according to the National Institute of Standards and Technology (NIST) specifications. | • AWS  
• GCP | C1.2 |