QuickBase, Inc.

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

SOC 3[SM] Report

For the Period July 1, 2018 through June 30, 2019

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. (Quick Base):

We have examined management's assertion that Quick Base, during the period of July 1, 2018 through June 30, 2019, maintained effective controls to provide reasonable assurance that:

- the Quick Base system was protected against unauthorized access, use, or modification to meet Quick Base's commitments and system requirements
- the Quick Base system was available for operation and use to meet Quick Base's commitments and system requirements
- the Quick Base system information designated as confidential was protected to meet the entity's commitments and system requirements

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' (AICPA) TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).* This assertion is the responsibility of Quick Base management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA and, accordingly, included (1) obtaining an understanding of Quick Base's relevant controls; (2) testing and evaluating the operating effectiveness of the controls; and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions based on our findings to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls, or a deterioration in the degree of effectiveness of the controls.

In our opinion, Quick Base's management assertion referred to below is fairly stated, in all material aspects, based on the aforementioned criteria for security, availability, and confidentiality.

BARR Advisory, P.A.

Fairway, KS

July 31, 2019

Quick Base's Assertion on the Description of the Quick Base System

Quick Base maintained effective controls over the security, availability, and confidentiality of its Quick Base system to provide reasonable assurance that:

- the Quick Base system was protected against unauthorized access, use, or modification to meet Quick Base's commitments and system requirements
- the Quick Base system was available for operation and use to meet Quick Base's commitments and system requirements
- the Quick Base system information designated as confidential was protected to meet the entity's commitments and system requirements

during the period July 1, 2018 through June 30, 2019, based on the criteria for Security, Confidentiality, Availability principles set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Our attached system description of the Quick Base system identified the aspects of the system covered by our assertion.

Subservice providers are used to provide data center hosting, colocation, and infrastructure services.

QuickBase, Inc.

July 31, 2019

Overview of Operations

Company Background

Quick Base provides a cloud-based platform that empowers problem solvers to turn ideas for better ways to work into apps that make their organizations more efficient. For 20 years, people of technical and non-technical backgrounds have been using the Quick Base platform to create solutions that streamline processes, capture real-time data, and improve company operations while working in concert with existing IT systems. Based in Cambridge, MA, Quick Base has thousands of customers spanning all industries and company sizes.

Description of Services Provided

Quick Base 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 Quick Base core platform includes the following key capabilities:

- Data Management
- Custom Forms
- Visual App Building
- Automations
- Integrations
- Security and Compliance
- Governance
- Mobile
- App Marketplace

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

- **Quick Base Webhooks:** An integration and workflow automation capability that enables Quick Base to notify, in real time, a Quick Base app, a cloud application, or a web-enabled, on-premise system about changes in Quick Base data.
- **Quick Base Sync:** A data integration feature that allows Quick Base app builders to integrate their Quick Base apps with third party services such as Salesforce and NetSuite, file services like Dropbox and Box, and email services.
- **Quick Base Audit Logs:** Provides Quick Base customer administrators 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. Quick Base 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

Quick Base designs its processes and procedures related to the Quick Base system to meet its objectives and commitments to customers, legal and regulatory requirements that govern Quick Base services, and the financial, operational, and compliance requirements that Quick Base 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:

- System features and configuration settings designed to enable Quick Base app builders to build applications which permit access to users based on authorization, which may be, for example, based on their Quick Base 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 Quick Base website and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Operational procedures supporting the achievement of security commitments to user entities.

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

- The use of encryption technologies to protect Quick Base app data both at rest and in transit.
- Confidentiality and nondisclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Quick Base 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 Quick Base 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.
- 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 Quick Base platform is hosted at Flexential (previously branded as ViaWest) Tier IV Data Centers located in North Las Vegas, NV, and Englewood, CO. Additionally, Quick Base utilizes Amazon AWS' US-West region for ancillary services, including Quick Base Webhooks, Quick Base

Sync, and Quick Base Audit Logs.

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. Quick Base 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 Quick Base web applications are encrypted using Transport Layer Security (TLS) supported by certificates from an established third party certificate authority.

Remote system administration access to the Quick Base web and app servers is available through an RSA advanced encryption standard (AES) 128-bit encrypted virtual private network (VPN) connection and requires multi-factor authentication.

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

- **Server hardware:** A combination of Hewlett Packard (HP) and Dell servers; and,
- **Network components:** Cisco routers, Palo Alto firewalls, F5 local traffic managers (LTMs), MCP/SCP load balancers.

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.

The core Quick Base web and app servers, including servers that support Quick Base Sync, reside in a Microsoft Active Directory domain. The application and web servers run on Microsoft Windows operating systems. Metadata (e.g., user credentials and session information) are stored in a Microsoft SQL database. Quick Base apps utilize a 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.

Customers access Quick Base apps via the Internet using any modern web browser. Users authenticate via a user account and password. Quick Base supports Single Sign-On (SSO) via SAML 2.0 and integration with user entities' LDAP services.

Quick Base Webhooks, Quick Base Sync, and Quick Base Audit Logs are built with AWS services residing in an AWS Virtual Private Cloud (VPC). Services that support the system include:

- **Elastic Compute Cloud (EC2):** Provides Infrastructure as a Service (IaaS) to Quick Base for scalability and hosts the application logic, postgres databases, and service components.
- **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. Quick Base 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 are 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 Quick Base traffic across multiple EC2 instances.

People

The following Quick Base 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 team**: Responsible for the engineering and maintenance of Quick Base's infrastructure components and the deployment of changes and monitoring the Quick Base services.
- **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 Quick Base application code; key personnel within this group include program managers, developers, and quality assurance (QA) 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 Quick Base's corporate information technology services.
- **Business Enablement team:** Develops and enhances Quick Base apps used to support Quick Base business and operations workflows and processes.

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, 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 Quick Base system through security awareness training that is completed as part of onboarding procedures, and annually thereafter.

The policies and procedures used to safeguard Quick Base systems include:

- Information Security Oversight;
- Data Classifications and Responsibilities;
- Audit and Accountability;
- Configuration Management;
- Contingency Planning;

- Identification and Authentication;
- Security Incident Response;
- Mobile Devices;
- Open Source Software;
- Acceptable Encryption;
- System Level Access Control;
- System and Services Acquisition;
- Vulnerability Management;
- Security Awareness; and,
- Physical and Environmental Security.

Data

Data is received by the Quick Base web servers from users' web browsers, and encrypted during transit using a 256 bit (SHA2) over TLS version 1.2 connection. Network load balancers forward requests to web servers that forward requests to Quick Base app servers, where the requests are executed and responses returned to the user's web browser. Data is encrypted by the Quick Base app, 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. Quick Base functionality allows for the following:

- **Collecting data**: Quick Base users can import data from an existing application, or they can add, edit, and delete information directly in Quick Base by filling in customizable forms.
- **Managing data:** Quick Base 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, Quick Base allows users to share information among team members, customers, and/or partners in real time. Quick Base 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 Quick Base Sync, Quick Base custom applications can be integrated with other third party web-based applications, allowing users to automatically sync data between Quick Base and those other third party web-based applications.
- **Logging data:** When used in conjunction with Quick Base Audit Logs, Quick Base realm admins can view user activity logs including changes made to data and schema.

Quick Base Sync, Quick Base Webhooks, and Quick Base Audit Logs utilize APIs to pull data from the Quick Base app servers in the Flexential colocation data center to AWS services located in the AWS US-West region. Data is then sent to third party web-based applications through automated connections for syncing, sharing, alerting, and/or workflow-continuation as designed by customer-created Quick Base workflows.

Quick Base has data classification guidelines and security labels that govern information labeling, handling, and disposal in accordance with guidelines established in company policy, customer

agreements, and applicable regulations. Quick Base 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 Quick Base system 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 Quick Base roles and permissions. Quick Base policies prohibit the downloading of any customer confidential data by Quick Base employees from the Quick Base app and infrastructure environment. This includes restriction of transmitting data to workstations.

Achieving High Security

The Quick Base site is only accessible over TLS 1.2. Quick Base users are authenticated to access their applications and data stored in those applications. Logical access segregates each customer's data, controlled via authentication and authorization, at the realm, account, and application layers.

Quick Base's product functionality and system architecture are designed with security as a goal. Quick Base encrypts all information at rest and uses role-based security for Quick Base site administration, customer care, and other administrative roles.

Quick Base integrates security testing into each phase of the development lifecycle, including daily static code security scans and dynamic web scans. Developers complete role-based training on secure code development best practices.

Quick Base's security commitments are communicated to third parties through contractual agreements. The Compliance and Information Security Officer is responsible for ensuring contracts are in place for all third parties with access to the Quick Base system. 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 Quick Base. In order to help ensure high availability of the Quick Base platform, Quick Base data that reside at Flexential colocation data centers are continuously replicated from the production to the hot standby data center for use in the event of an outage at the primary data center. Quick Base 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.

Achieving High Performance

Quick Base 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 Quick Base can view live availability statistics and subscribe to operational updates on Quick Base's public-facing status page at https://service.quickbase.com.

Monitoring Performance, Scalability, and Availability

Paessler PRTG, Datadog, and Pingdom, are used to monitor performance and availability of the IT infrastructure at Flexential colocation data centers and AWS, as well as the public-facing Quick Base

website. Additional internally developed Quick Base apps are used to monitor and alert on the performance and availability of Quick Base custom apps. Quick Base operations personnel are on call 24/7 and can be reached through the VictorOps paging service. Monitoring tools such as Splunk and Threat Stack are configured to monitor for, and alert on, performance and availability issues as well as system and user anomalies.

Complementary User Entity Controls

Quick Base 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 Quick Base customers, related to the information processed.

For customers to rely on the information processed through the Quick Base application, 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 protecting established user IDs and passwords within their organizations Quick Base realm.
- User entity is responsible for reviewing customer access to their Quick Base apps periodically to validate appropriateness of access levels.
- User entity is responsible for approving and creating new user access to their Quick Base realm and apps.
- User entity is responsible for removing terminated employee access to their Quick Base 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 Quick Base realm and apps.
- User entity is responsible for implementing a change and configuration management program over user systems and apps built in the Quick Base system.
- User entity is responsible for notifying Quick Base if they detect or suspect a security incident related to the Quick Base system.
- User entity is responsible for reviewing email and other forms of communications from Quick Base, related to changes that may affect the Quick Base 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 Quick Base website.

Complementary Subservice Organization Controls

Quick Base uses subservice organizations to provide data center hosting, colocation, and infrastructure services in support of its Quick Base system. Quick Base's controls related to the Quick Base system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over the Quick Base system to be achieved solely by Quick Base. Therefore, user entity controls must be evaluated in conjunction with Quick Base'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.

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

- Review of subservice organizations' SOC reports;
- Regular meetings to discuss performance; and,
- Nondisclosure agreements.

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Trust Services Criteria
Physical access to the data center facility is restricted to authorized personnel.	• Flexential • AWS	CC6.4
Environmental protections, including monitoring and alarming mechanisms, are implemented to address physical security and environmental control requirements.	• Flexential • AWS	CC6.4
Business continuity and disaster recovery procedures are developed, reviewed, and tested periodically.	• Flexential • AWS	A1.3

