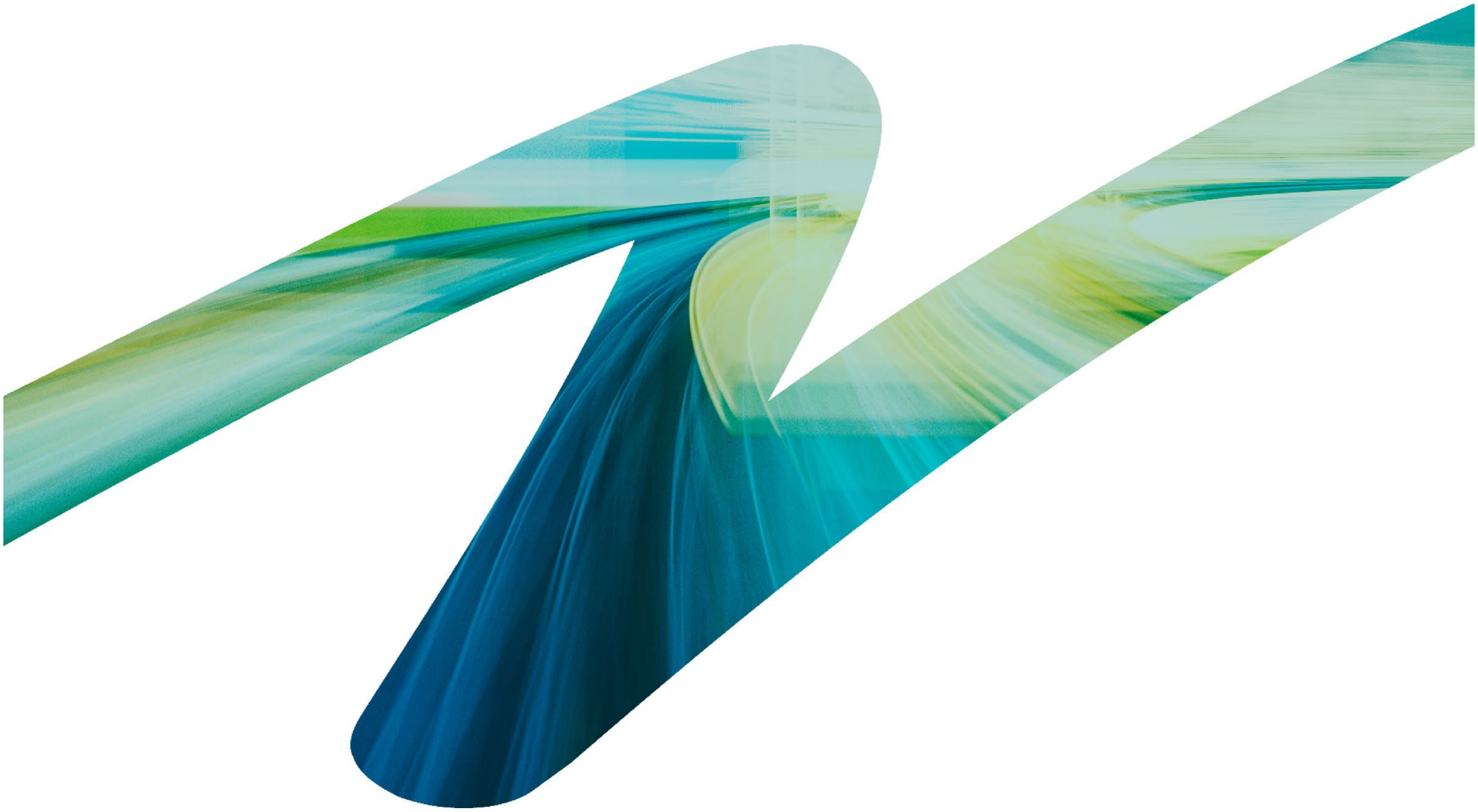

Quickbase Inc.

SOC 3 Report

Report on the Quickbase Platform throughout the period July 1, 2024 to June 30, 2025

Contents

plante moran

Plante & Moran, PLLC
Suite 600
8181 E. Tufts Avenue
Denver, CO 80237
Tel: 303.740.9400
Fax: 303.740.9009
plantemoran.com

Independent Service Auditor's Report

To Management
Quickbase, Inc.

Scope

We have examined management of Quickbase, Inc.'s (Quickbase) accompanying assertion titled "Quickbase, Inc. Management's Assertion" (the "assertion") that the controls within Quickbase, Inc.'s Quickbase Platform (the "system") were effective throughout the period July 1, 2024 to June 30, 2025 to provide reasonable assurance that Quickbase, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (the "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, Inc. 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, Inc.'s service commitments and system requirements were achieved. Quickbase, Inc. management has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Quickbase, Inc. management is responsible for selecting, and identifying in its assertion, the applicable trust services 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 the 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 the following:

- 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, Inc.'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 Quickbase, Inc.'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.

To Management
Quickbase, Inc.

Service Auditor's Independence and Quality Control

We are required to be independent 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 Quickbase, Inc.'s Quickbase Platform were effective throughout the period July 1, 2024 to June 30, 2025 to provide reasonable assurance that Quickbase, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated in all material respects.

This report is intended solely for the information and use of Quickbase, user entities of Quickbase's Quickbase Platform, business partners of Quickbase subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities, and business partners and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Plante & Moran, PLLC

January 12, 2026

January 12, 2026

Plante & Moran, PLLC

To Service Auditors:

We are responsible for designing, implementing, operating, and maintaining effective controls within Quickbase, Inc.'s Quickbase Platform throughout the period July 1, 2024 to June 30, 2025, to provide reasonable assurance that Quickbase, Inc.'s service commitments and system requirements relevant to security, availability, and confidentiality (applicable trust services criteria) 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 July 1, 2024 to June 30, 2025, to provide reasonable assurance that Quickbase, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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, Inc.'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 July 1, 2024 to June 30, 2025, to provide reasonable assurance that Quickbase, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Very truly yours,

Signed by:

Deepali Bhoite

9C185D2AD2CA4D1...

Deepali Bhoite, Chief Information Security Officer

Attachment A. Quickbase's Description of the Boundaries of its Quickbase Platform

A. Company Overview

Company Background

Founded in 1999 and headquartered in Boston, Massachusetts, Quickbase provides a cloud-based operations platform that allows businesses to create custom applications and workflows to streamline their processes and improve productivity. It provides a range of tools for building, customizing, and managing applications without requiring any coding experience. Quickbase offers features such as data collection, reporting and analytics, workflow automation, and collaboration tools. With Quickbase, businesses can automate manual processes, consolidate their data, and get real-time insights. The Platform is highly customizable and can be tailored to meet the unique needs of different teams and departments across an organization.

Description of the Services Provided

Quickbase is a cloud-based, AI-powered operations platform that enables business users to create custom applications and automate workflows, while giving IT administrators the visibility and control they need for compliance and oversight. The Quickbase Platform (or the "Platform") includes the following key capabilities:

- Data management
- User interface (forms, dashboards, etc.)
- Visual app and workflow building
- Automations
- Integrations
- Governance
- Mobile
- App template library

The description details the Quickbase Platform System and the related policies, procedures, and control activities for the Quickbase Platform System. The description does not include any other services.

The system described herein is bounded by the specific aspects of Quickbase's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers, and the data that is processed by the system. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. The components that directly support the services provided to user entities are as follows:

Infrastructure

The core Quickbase US instance of the Platform is hosted at the Amazon Web Services (AWS) US-West-2 and US-East-2 regions. The core Quickbase EU instance of the Platform is hosted at the AWS EU-Central-1 and EU-West-1 regions. Redundancy at AWS is achieved within each region using availability zones. Data is continuously replicated from the active region to the warm standby region.

A multitier 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.

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

- **Compute:** AWS ECS/Fargate Containerized Services and AWS EC2 Server Based Services
- **Database(s):** SBServer (Quickbase proprietary in memory database) and Microsoft SQL Server 2022
- **Network Components:** Cloudflare, AWS WAF, AWS ALB
- **Storage:** NetApp Filers and AWS FSx for NetApp

Quickbase Core Platform

The core Quickbase Platform operates using Amazon Web Services (AWS) using services residing in a virtual private cloud (VPC). It includes web, app, and database servers that reside in 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., hashing, encryption, user credentials, and session information) are stored in a Microsoft SQL Server database.

Quickbase applications, when accessed, are loaded in the proprietary in-memory database (SBServer). Files that contain app data are encrypted at the application layer and stored in Advanced Encryption Standard (AES) 256bit encrypted format on flat files on the NetApp storage arrays where files are backed up and replicated to the standby region.

Customers access Quickbase applications via the internet using any modern web browser. Authentication to the Quickbase Platform via browser can be done using a native Quickbase user account and password or single sign-on (SSO) via SAML 2.0.

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

Quickbase Audit Logs, Quickbase JSON API Gateway, Quickbase Sync, and Quickbase Webhooks operate using Amazon Web Services (AWS) using services residing in a Virtual Private Cloud (VPC). AWS 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, 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.
- 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 Identity and Access Management (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.
- IAM: Controls access to Amazon services at the user, operation, and cluster levels.
- Elastic Load Balancer (ELB): Load balancer that automatically distributes Quickbase traffic across multiple EC2 instances.

Quickbase Pipelines operate using Google Cloud Platform (GCP) utilizing the Google Cloud App Engine. The Pipelines system in the Quickbase US instance of the Platform is hosted in the US-Central-1 region. For Quickbase EU, it is hosted in the Europe-West-1 region.

GCP services that support the system include:

- Cloud Tasks: Facilitates workload distribution.
- Cloud Storage: Transitional storage needed during execution of some pipeline instances.
- Key Management System (KMS): Stores realm level encryption key and performs envelope encrypt/decrypt of data encryption keys (DEKs).
- Google Cloud's Operations Suite: Performance monitoring and diagnostics.
- BigQuery: Statistical usage data with no customer data saved.
- Memcached: Operational data cache and distributed locking. If customer data is put in the cache, it is first encrypted on the application level with a DEK. Provided and operated by Google Cloud as part of App Engine standard environment.
- Cloud Datastore: Main application database that 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 information needed during the execution.

Software

Quickbase is responsible for managing the development and operation of the Quickbase Platform including infrastructure components such as servers, databases, and storage systems unless otherwise specified in the Complementary Subservice Organization Controls table.

People

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

- **Board of Directors:** Responsible for oversight of the performance of internal controls and strategic guidance.
- **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.
- **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, GRC, product, finance, IT, customer success, employee experience (EX), and legal.
- **Security:** Responsible for protecting the organization's information and systems through continuous security monitoring, rapid incident response, and proactive vulnerability management. Detects and responds to threats in real time, investigates and contains breaches, and identifies and fixes security weaknesses to prevent future attacks.
- **HIPAA Security Officer:** A member of the security team who is additionally responsible for Quickbase's HIPAA compliance program, HIPAA policies, procedures as necessary to incorporate changes to HIPAA or the HIPAA Security Rule or to improve compliance, and reviewing and approving or disapproving proposed projects or activities that may require Quickbase to receive, store, process, transmit, create, or access and use protected health information (PHI). The Chief Information Security Officer is the Quickbase HIPAA Security Officer.
- **Governance, Risk and Compliance (GRC)**: Responsible for overseeing the governance, risk, third-party risk management, and compliance 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.
- **Site Reliability Engineering (SRE):** Responsible for the engineering and maintenance of Quickbase’s infrastructure components, deployment of changes, and monitoring the Quickbase services.
- **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 and Product Management:** 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.
- **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.

- **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.

- **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.

- **Enterprise Business Systems (EBS):** 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 Technology Officer, Chief Information Security Officer, VP of Platform Operations, developers, Systems Architects, and Legal.

Procedures

Quickbase has developed and communicated policies and procedures to manage the information security of the system. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system access, auditing, configuration management, breach or incidents, disaster recovery, intrusion detection, vulnerability assessment, data integrity, vendor management, and so on. Policies are reviewed on an annual basis by the GRC team, coordinating with the chief information security officer (CISO), and changes are made to the policies when necessary.

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 BAA is in place with AWS due to the presence of ePHI in the Quickbase Platform components hosted in AWS.

Data is received by the Quickbase web servers, via Cloudflare, 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 application 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.

B. Subservice Organizations

Management of Quickbase assumed, in the design of the Quickbase Platform that certain controls at subservice organizations are necessary, in combination with controls at Quickbase, to provide reasonable assurance that Quickbase's service commitments and system requirements would be achieved. These complementary subservice organization controls and the related trust services criteria are described below. Subservice organizations are responsible for implementing such controls.

The following are the subservice organizations used by Quickbase, the services provided by them, and the trust services criteria that are applicable to the services that they provide:

- **Amazon Web Services** - Quickbase utilizes AWS to host the Quickbase Platform. In addition, Quickbase leverages database, load balancing, and cloud computing AWS services. AWS is responsible for maintaining and operating controls related to physical security and environmental protection over its data centers in which the servers used to host the system are housed.
- **Google Cloud Platform** - Quickbase utilizes GCP to host the Pipelines functionality within the Quickbase Platform. Quickbase leverages cloud computing, storage, database, key management, and data warehouse GCP services. GCP is responsible for maintaining and operating controls related to physical security and environmental protection over its data centers in which the servers used to host the system are housed.

Applicable Trust Services Criteria	Expected Controls to be Implemented by the Subservice Organizations
Common Criteria 6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS and GCP have logical access policies and procedures in place to protect against unauthorized access to AWS/GCP resources that could impact the security of user entity content. AWS and GCP firewall devices are configured to restrict access to production networks. AWS and GCP conduct proper training for employees.
Common Criteria 6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Physical access procedures are in place to allow authorized access and deny unauthorized access.
Common Criteria 6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	AWS and GCP securely decommission and physically destroy production assets in their control.

Applicable Trust Services Criteria	Expected Controls to be Implemented by the Subservice Organizations
Common Criteria 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	AWS and GCP are responsible for patching and fixing flaws within the infrastructure.
Availability Criteria 1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Business continuity and disaster recovery plans to identify, respond, and recover from a major event are in place and tested. Fire detection and suppression equipment are in place and operational in facilities. Climate control capabilities are in place to maintain appropriate temperature levels for servers and hardware. Procedures are in place to provide data redundancy across multiple facilities.
Availability Criteria 1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Business continuity and disaster recovery plans to identify, respond, and recover from a major event are in place and tested.

C. Complementary User Entity Controls

Management of Quickbase assumed, in the design of Quickbase's Quickbase Platform that certain controls will be implemented by user entities, and those controls are necessary, in combination with controls at Quickbase, to provide reasonable assurance that Quickbase's service commitments and system requirements would be achieved. These complementary user entity controls and the related trust services criteria are described below. User entities are responsible for implementing such controls.

- User entity is responsible for reviewing access to their Quickbase account periodically to validate appropriateness of access levels for their users.
- User entity is responsible for user administration within their Quickbase account, including access provisioning, deprovisioning, and user permissions in accordance with internal user entity policies and requirements.
- 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 implementing policies and procedures over the use case and associated data types that are allowed to be entered into their Quickbase account and retained.
- User entity is responsible for the configuration, testing, and approval of user entity custom code or configurations implemented within their Quickbase accounts.

- User entity is responsible for implementing a change and configuration management program over user systems and applications built in the Quickbase Platform.
- User entity is responsible for understanding the data they intend to collect and store in their Quickbase account and for ensuring that risk and compliance requirements are addressed and correlate to the importance and classification of that data.
- User entity is responsible for deleting their own data within their Quickbase realm and applications.
- User entities are responsible for notifying Quickbase of changes made to technical or administrative contact information.
- User entities are responsible for requesting that Quickbase restore their backup files when needed.

Attachment B. 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.

Quickbase has the following service commitments and system requirements to achieve company objectives, industry best practices, and compliance with in-scope trust services criteria and regulations.

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

- **Security Policies** – Quickbase will maintain commercially reasonable data security policies intended to prevent unauthorized access, use, modification, deletion, and disclosure of customer data.
- **Vendor Management** – Before sharing customer data with third-party service providers, Quickbase will ensure that the third party maintains, at a minimum, reasonable data practices for maintaining the confidentiality and security of customer data and preventing unauthorized access.
- **Antivirus** – Quickbase will make commercially reasonable efforts to prevent a computer virus, worm, timebomb, logic bomb or other similar computer program from impacting customers' use of the Quickbase Platform.
- **Cybersecurity Insurance** – Quickbase maintains liability insurance to provide additional protection in the event of a breach related to cybersecurity.
- **Notification** – Quickbase commits to notifying affected customers of any unauthorized access to information via e-mail or phone.
- **Training** – Quickbase employees are trained and required to safeguard customer information.
- **Access Safeguards** – Electronic and procedural safeguards are used to restrict access to customer information to those employees and agents who require access for business purposes only.
- **Backup Restoration** - Quickbase will use commercially reasonable efforts to restore lost or corrupted customer data and customer applications from the latest backups maintained by Quickbase in accordance with its archival procedures.
- **Availability** – Quickbase will use reasonable commercial efforts to ensure that the Hosted Service will be available 99.9% (ninety-nine and nine-tenths percent) of the time, seven (7) days per week, 24 (twenty-four) hours per day, excluding permitted outages.
- **Availability Report** – Quickbase will measure and report its average availability percentage on the Quickbase service page.

- **Availability** – - Quickbase data is continuously replicated from the production to the warm standby data center. Quickbase maintains 14 daily snapshots and 6 months of weekly snapshots.

Quickbase establishes system requirements that support the achievement of service commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- **Monitoring** – Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures.

- **Security requirements** – Business processing rules, standards, and regulations, including security requirements under HIPAA, data security measures as required by Defense Federal Acquisition Regulation Supplement (DFARS) and Cloud Security Alliance (CSA) Cloud Control Matrix (CCM).

- **Encryption** – Quickbase encrypts customer data in motion and at rest. All communications over non-trusted Internet networks are encrypted at up to 256 bit (SHA2) TLS certificate, TLS 1.2 and 1.3. Quickbase encrypts all customer app data and any files attached therein using an AES 256 key.

- **Pen Test** – At least annually, Quickbase engages an independent penetration testing firm to perform a timebound security assessment of the Quickbase Platform, internet-facing systems, applicable infrastructure, and supporting policy and procedure documentation.

- **Incident Response** – Quickbase's operations team employs automated incident detection, escalation technologies and procedures which ensure that any infrastructure or sub-service provider issue is rapidly addressed, 24/7/365.

- **Vulnerability management** – Quickbase employs a variety of tools and processes to detect, protect and respond to security vulnerabilities.

- **Disaster recovery** – At least annually Quickbase switches between the two data centers as part of its normal disaster recovery plan validation process.

- **Availability** – Quickbase maintains two geographically diverse, production-ready datacenters for all core infrastructure components.

- **Availability** – Production data is replicated to the warm standby data center with up to a 15 minute delay, i.e., a recovery point objective (RPO) of 15 minutes.

- **Availability** – If an issue were to impact the production site, Quickbase only needs 2 hours to bring up production at the DR site, i.e., a recovery time objective (RTO) of 2 hours;

- **Availability** - Quickbase data is continuously replicated from the production to the warm standby data center. Quickbase maintains 14 daily snapshots and 6 months of weekly snapshots.