Report on YugabyteDB, Inc.'s YugabyteDB Managed Services Relevant to Security, Availability, and Confidentiality Throughout the Period April 1, 2023 to September 30, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: YugabyteDB, Inc. ("YugabyteDB")

Scope

We have examined YugabyteDB's accompanying assertion titled "Assertion of YugabyteDB, Inc. Management" (assertion) that the controls within the YugabyteDB Managed Services (system) were effective throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that YugabyteDB'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 (With Revised Points of Focus—2022)* (2017 TSC).

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at YugabyteDB, to achieve YugabyteDB's service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

YugabyteDB uses subservice organizations to provide cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at YugabyteDB, to achieve YugabyteDB's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of YugabyteDB's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

YugabyteDB 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 YugabyteDB's service commitments and system requirements were achieved. YugabyteDB has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, YugabyteDB 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 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.

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

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 YugabyteDB'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 YugabyteDB'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 YugabyteDB Managed Services were effective throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that YugabyteDB's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of YugabyteDB's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
November 16, 2023

Section 2

Assertion of YugabyteDB, Inc. Management

Assertion of YugabyteDB, Inc. (“YugabyteDB”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within theYugabyteDB Managed Services (system) throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that YugabyteDB’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 (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at YugabyteDB, to achieve YugabyteDB’s service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

YugabyteDB uses subservice organizations for cloud hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at YugabyteDB, to achieve YugabyteDB’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of YugabyteDB’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that YugabyteDB’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of YugabyteDB’s controls operated effectively throughout that period. YugabyteDB’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 April 1, 2023 to September 30, 2023 to provide reasonable assurance that YugabyteDB’s service commitments and system requirements were achieved based on the applicable trust services criteria.

YugabyteDB, Inc.

Attachment A

YugabyteDB, Inc.’s Description of the Boundaries of Its YugabyteDB Managed Services

Type of Products Provided

YugabyteDB, Inc. (“YugabyteDB” or “the Company”) is a global, database-as-a-service (“DBaaS”) software company founded in January 2016 and headquartered in Sunnyvale, California. The Company’s offerings serve business-critical applications with SQL query flexibility, high performance, and cloud-native agility. YugabyteDB’s offering consists of three products: (1) YugabyteDB, (2) YugabyteDB Anywhere, and (3) YugabyteDB Managed, collectively the “YugabyteDB Managed Services System.” See the subsections below for more information on each product.

YugabyteDB

The YugabyteDB offering, launched as a 100% open source solution under the Apache 2.0 license in 2019, is a distributed SQL database developed to support global-scale and cloud native applications. Built using a combination of high-performance document store, per-shard distributed consensus replication, and multi-shard atomicity, consistency, isolation, and durability (ACID) transactions (inspired by Google Spanner), YugabyteDB serves both relational database management system (RDBMS) and online transaction processing (OLTP) workloads with low query latency resulting in resilience against database failures and global data distribution. As a cloud-native database, it can be deployed across public and private clouds, as well as in containerized environments such as Kubernetes.

The YugabyteDB offering was built with built-in security features including, but not limited to, role-based access control (RBAC), data encryption at rest and in transit, audit logging, and column-level permissions. Row level security (RLS) and column-level encryption are available for more advanced use cases.

YugabyteDB Anywhere

YugabyteDB Anywhere is for YugabyteDB customers that host their own YugabyteDB environment. With YugabyteDB Anywhere, customers can deliver a private DBaaS at scale by deploying YugabyteDB across any cloud environment anywhere in the world. YugabyteDB Anywhere simplifies day-to-day operations through automation, and gives customers visibility to support, scale, and manage their YugabyteDB environment. YugabyteDB Anywhere is best fit for mission-critical deployments, such as production or pre-production testing. The YugabyteDB Anywhere console supports management of YugabyteDB universes, or clusters, on one or more regions (across public cloud and private on-premise data centers).

YugabyteDB Managed

YugabyteDB Managed allows developers to create and connect to a scalable, resilient PostgreSQL compatible database with minimal operational overhead. It is available in over 30 regions in two major cloud service providers. It applies information security control best practices to manage infrastructure and database security, including daily backups, non-disruptive software upgrades, continuous availability, database usage monitoring, logging and auditing, identify and access management, data encryption, and key rotation.

The system description in this section of the report details the YugabyteDB Managed Services System. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations). While the Company has physical offices, no production data is stored or processed at Company office locations.

The Components of the System Used to Provide the Services

The boundaries of the YugabyteDB Managed Services System are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the YugabyteDB Managed Services System.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes single or multi-tenant virtual private clouds (VPCs) within third-party cloud service providers to host the YugabyteDB Managed Services System. The Company leverages the experience and resources of third-party cloud service providers to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the YugabyteDB Managed Services System architecture to ensure the availability, security, and resiliency requirements are met.

The YugabyteDB offering reuses PostgreSQL's query layer to achieve compatibility with existing PostgreSQL applications or those that can be migrated from PostgreSQL. This enables developers to be immediately productive with the ecosystem of PostgreSQL compatible frameworks, applications, drivers, and tools.

The YugabyteDB Managed offering consists of control and data planes. The control plane is responsible for creating and managing customer data plane instances. The data plane hosts the customers' YugabyteDB clusters deployed on public cloud provider infrastructure.

Network

The Company maintains a Network Security Policy that establishes technical guidelines for network design and security and communicates controls in support of securing the Company's network. The scope of the Network Security Policy applies to IT systems, devices, rules, and configurations designed to protect the confidentiality, integrity, and availability of the networks maintained by the Company.

Guidelines regarding use of the network and Company assets are in place and are regularly communicated to users. Violations of any guidelines governing the use of the network may result in disciplinary action, up to and including termination of employment.

The network is divided into two logical environments: non-production and production. The non-production environment is used for supporting services such as software development and testing activities. Customer data within YugabyteDB Managed is classified as Confidential commensurate with the Company's Data Classification Policy, and such data is maintained entirely within a secured environment. User access is controlled via access control lists (ACLs) and encrypted VPN sessions and is granted based on business need and job function.

Solutions are employed for their respective cloud service environments to provide an additional layer of security against distributed denial of service (DDoS) and other network-based attack vectors.

Software

Software consists of the programs and software that support the YugabyteDB Managed Services System (operating systems [OSs], middleware, and utilities). Third-party software systems are utilized to support the YugabyteDB Managed Services System via the following:

- System and network monitoring
- Ticketing and workflow management
- Vulnerability management
- Backup tools
- Email/Content management
- System logging
- Anti-malware
- Human Resources information system
- Accounting and payroll systems
- Customer relationship management system

People

The Company develops, manages, and secures the YugabyteDB Managed Services System via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Provides overall governance and direction for the Company, as well as develops strategies and oversees risk management discussions. The Executive Management team, led by the Chief Executive Officer (CEO), maintains clear and concise communication channels to disseminate information regarding internal control requirements to appropriate levels within the organization.
People	Supports the Executive Management team with talent acquisition, talent management, performance management, and payroll under the direction of the Vice President (VP) & General Counsel.
Software Development	Owns responsibility for software architecture, design, and development under the direction of the Chief Technology Officer (CTO).
Information Technology (IT)	Provides technical infrastructure and application support for internal teams and ensures that processes are compliant with IT and Information Security policies under the direction of the Sr. Director of Information Security & Compliance.
Cloud Operations	Manages and operates the production infrastructure hosted by cloud service providers under the direction of the Senior Vice President, Engineering.
Product Management	Sets functional priorities for product development, owns the product roadmap, and is responsible for translating business requirements into specifications for the Software Development team under the direction of the CTO.

People	
Group/Role Name	**Function**
Security & Compliance	Owns responsibility for risk management, due diligence, and internal compliance under the direction of the VP & General Counsel. Ensures the Company delivers on service commitments and system requirements to business partners and customers.
Business Operations	Supports day-to-day operations including the finance and accounting functions under the direction of the VP, Operations.
Sales	Provides business development and customer solution implementations under the direction of the CEO.
Product Strategy & Solutions	Provides brand management and external communication services under the direction of the VP, Product Strategy and Solutions.
Customer Success	Provides customer-facing technical support, professional services, and product training under the direction of the Sales Vice President.
Technical Support	Provides customer-facing technical support under the direction of the VP of Global Support Services.

The Company is managed under the direction of the Executive Management Team, which is responsible for various operational areas of the Company, including general management and administration. The following organization chart reflects the Company's internal structure related to the groups discussed above:

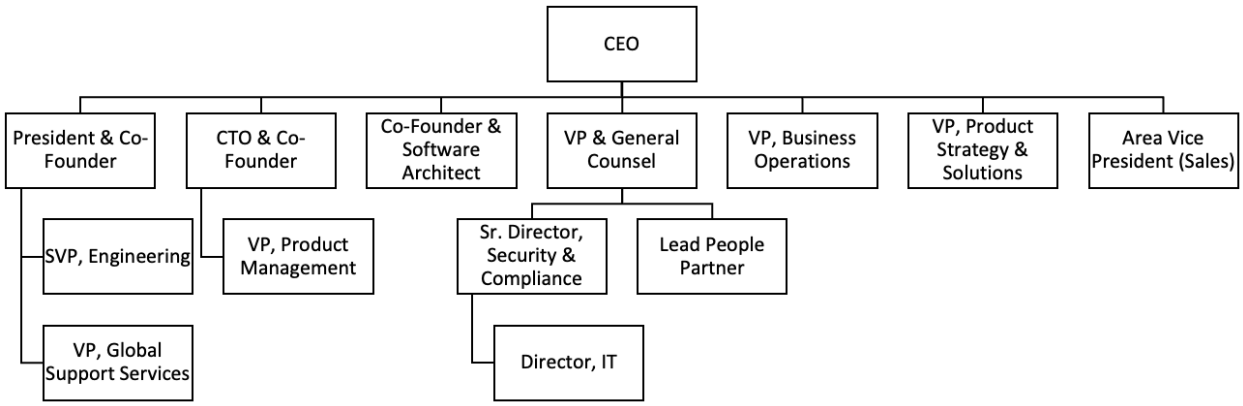

Figure 3: Company Organization Chart

Procedures

Procedures include the automated and manual procedures involved in the operation of the YugabyteDB Managed Services System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security & compliance, IT, and People. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the YugabyteDB Managed Services System:

Procedures	
Procedure	**Description**
Access Management	How the Company restricts system access, provisions and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with the Company's Data Classification Policy and Records Retention Schedule, as well as in accordance with applicable regulations and other requirements formally established in customer contracts.

The following table details the data classification levels used by the Company to assign appropriate safeguards:

Data	
Data Type	**Description**
Public Information	Information that is not confidential and already in the public domain or that the Company has intentionally released to the public.
Sensitive Information	Information intended for internal use or distribution to a limited audience with restricted business need to know. Unauthorized disclosure of this information would inconvenience the organization but would be unlikely to result in material financial loss or serious damage to the brand.
Confidential Information	Information that could be misused in such a way as to jeopardize the financial, legal, and social position of the person or entity described by the information. Unauthorized disclosure of this information is likely to result in negative financial outcomes, loss of customer trust, damage to the brand, regulatory penalties, civil or criminal complaint, or a strategic disadvantage for the Company.

Data	
Data Type	**Description**
Confidential-Restricted Information	Information that is particularly sensitive Confidential Information. Confidential-Restricted Information is any data whereby the unauthorized disclosure, alteration, or destruction of such data is likely to result in significant-to-catastrophic damage to the Company's business.

Data Encryption

Data at rest is encrypted using Advanced Encryption Standards (AES-256). Additionally, the Company leverages industry standards to encrypt sensitive data in transit. Communications at the client to server and server to system level is encrypted using TLS 1.2 or higher.

Data Retention and Destruction

Customer data is fully managed over the life cycle of use, from submission to destruction. The Company's customers are responsible for any data backups beyond the scope of the backup services offered as part of the YugabyteDB Managed offering.

The Company reserves the right to scrub or delete customer data used in YugabyteDB Managed after thirty (30) days from the date of termination of the applicable cloud agreements. Customer data retention requirements differing from the 30-day standard may be configured based on mutually agreed upon terms within standard service agreements. Storage systems used for customer data are securely purged before final decommissioning.

Subservice Organizations

The Company uses subservice organizations for cloud hosting services. The Company's controls related to the YugabyteDB Managed Services System cover only a portion of the overall internal control for each user entity of the YugabyteDB Managed Service System. The description does not extend to the cloud hosting services provided by the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the subservice organizations' SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the facilities, and relay any issues or concerns to management of the subservice organizations.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the YugabyteDB Managed Services System. Commitments are communicated in the Company's Terms of Service, Data Processing Addendum, and Data Backup Policy.

System requirements are specifications regarding how the YugabyteDB Managed Services System should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the YugabyteDB Managed Services System include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will notify the customer without undue delay of any security incident affecting customer personal information, and take reasonably necessary steps to remedy any non-compliance with the Data Processing Addendum. • YugabyteDB shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	• Implementation of proper access controls to ensure the principle of least privilege is enforced. • Data is encrypted in transit and at rest to protect it from unauthorized disclosure or theft. • Change management processes are implemented to track and authorize system changes, reducing the risk of unauthorized modifications.
Availability	• YugabyteDB will use commercially reasonable efforts to ensure the availability of the system. • YugabyteDB shall implement effective data backup measures to protect the confidentiality, integrity, and availability of information assets.	• Business continuity and disaster recovery processes have been defined to minimize the impact of negative events.
Confidentiality	• The Company will implement administrative, technical, and physical safeguards to prevent the loss, unauthorized use, access, or disclosure of Company proprietary and customer data. • The Company shall limit access to customer personal information to those employees or other personnel who have a business need to have access to such customer personal information.	• Data is classified into categories based on sensitivity and controls are implemented accordingly.