Frazier & Deeter
CPAs & ADVISORS

Independent Service Auditor's System and Organizational Controls SOC3® Report

On Yugabyte, Inc.'s Assertion of the Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality

Throughout the Period February 1, 2022 to July 31, 2022

yugabyteDB

Yugabyte, Inc.
771 Vaqueros Avenue
Sunnyvale, California 94085

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations ™

Assertion of Yugabyte, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Yugabyte, Inc.'s ("Yugabyte" or "the Company") YugabyteDB, YugabyteDB Anywhere and YugabyteDB Managed Services System (the System) throughout the period February 1, 2022 to July 31, 2022, to provide reasonable assurance that Yugabyte's service commitments and system requirements relevant to security, availability, and confidentiality were achieved throughout the period February 1, 2022, to July 31, 2022. Our description of the boundaries of the System (description) 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 February 1, 2022, to July 31, 2022, to provide reasonable assurance that Yugabyte'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*).

As certain controls did not operate during the examination period, in part or in whole, as circumstances that would warrant operation of those controls, in part or in whole, did not exist, our evaluation could not and did not extend to the effectiveness of those controls. Accordingly, tests of operating effectiveness could not be and were not performed by the Independent Service Auditor for those controls as evaluated using the applicable Trust Services Criteria for the System throughout the period February 1, 2022, to July 31, 2022.

Yugabyte uses subservice organizations to provide production information technology (IT) service management and infrastructure hosting, cloud hosting, and firewall hosting services. The boundaries of our System indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Yugabyte, to achieve Yugabyte's service commitments and system requirements based on the applicable Trust Services Criteria. The description does not disclose the actual controls implemented at the complementary subservice organizations.

The description of the boundaries of our System indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Yugabyte, to achieve Yugabyte's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Yugabyte's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Yugabyte's controls.

Yugabyte'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 February 1, 2022, to July 31, 2022, to provide reasonable assurance that Yugabyte's service commitments and system requirements were achieved based on the applicable Trust Services Criteria relevant to security, availability, and confidentiality.

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

System Overview & Services Provided

Yugabyte, Inc. ("Yugabyte") is a global database-as-a-service ("DBaaS") software company founded in January 2016 and headquartered in Sunnyvale, California. While Yugabyte has physical offices, production data is not stored or processed at the offices. Yugabyte's System consists of (1) YugabyteDB, (2) YugabyteDB Anywhere, a commercial enterprise software offering used to deploy, manage and monitor YugabyteDB instances, and (3) YugabyteDB Managed, a managed DBaaS offering based on YugabyteDB).

YugabyteDB

YugabyteDB is a distributed SQL database built to power global-scale and cloud native applications. Built using a unique combination of high-performance document store, per-shared 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 like Kubernetes.

YugabyteDB had its public beta release in 2017. Yugabyte launched YugabyteDB as 100% open source under the Apache 2.0 license in 2019.

YugabyteDB was built with data security in mind, allowing organizations to maintain security with built-in security features including, but not limited to, Lightweight Directory Access Protocol (LDAP) authentication, 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 Yugabyte 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-premises data centers).

YugabyteDB Managed

In September 2021, Yugabyte released its first fully managed commercial DBaaS service offering featuring YugabyteDB called 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 Amazon Web Services (AWS) and Google Cloud Platform (GCP). It applies information security control best practices to manage infrastructure and database security, including daily backups, non-

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

disruptive software upgrades, continuous availability, database usage monitoring, logging, auditing, identity and access management, data encryption, and key rotation.

Components of the System Used to Provide the Services

Infrastructure

YugabyteDB Managed uses single or multi-tenant virtual private clouds (VPCs) and hosted in AWS and GCP.

Yugabyte relies on AWS and GCP to provide enterprise level hosting with redundant power supply, environmental controls, redundant internet connections, and physical security. Yugabyte uses both virtual and physical server hosts. Independent third-party attestation reports (SOC 2 - Type II) are issued by AWS and GCP for Data Center Hosting Services and reviewed by Management.

As depicted in Figure 1 below, YugabyteDB reuses PostgreSQL's (an open-source object-relational database system) query layer to achieve compatibility with existing PostgreSQL applications or those that can be migrated to PostgreSQL. This also means that developers can be immediately productive with the ecosystem of PostgreSQL compatible frameworks, applications, drivers, and tools.

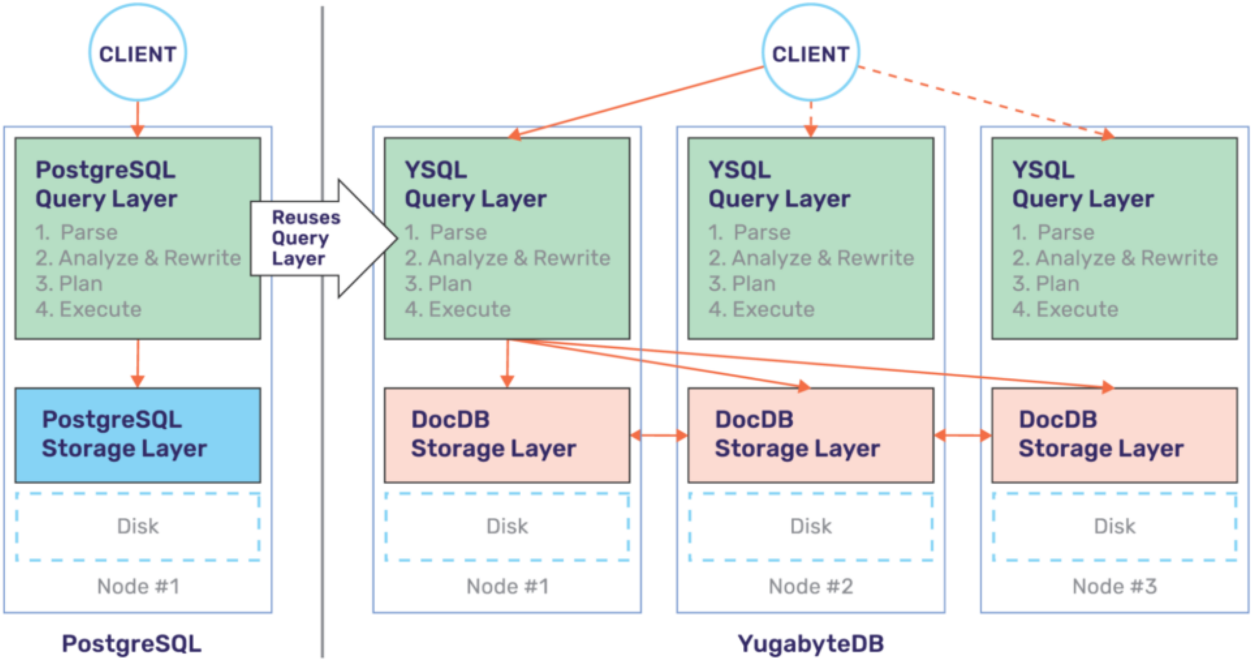


Figure 1: How YugabyteDB reuses PostgreSQL query layer

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

YugabyteDB Managed consists of control and data planes. The control plane is responsible for creating and managing customer data planes. The data plane hosts the customer's YugabyteDB clusters deployed on public cloud provider infrastructure. See Figure 2 below.

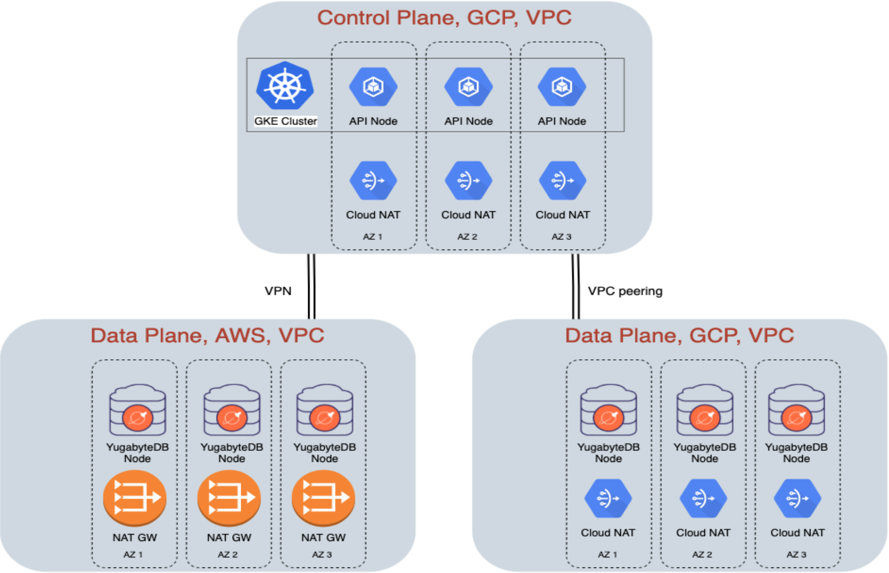


Figure 2: Control and Data Plane

Network

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

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

The data 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 Yugabyte Confidential Information and maintained entirely within a secured environment. User access is controlled via access control listings (ACLs), encrypted VPN sessions, and granted based on business need and job function.

AWS Shield for AWS hosted services and Google Cloud Armor for GCP hosted services and are employed to provide an additional layer of security, protecting against distributed denial of service (DDOS) and to provide additional protections for various network-based attack vectors.

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

A documented Disaster Recovery Policy is reviewed and tested annually. The Disaster Recovery Policy describes processes for recovery of IT systems, applications, data, and business operations in the event of a major outage.

Software

Yugabyte software is developed in-house, with the support of third-party service providers, and follows a software development lifecycle (SDLC) that supports testing of software releases before being released to production.

Yugabyte uses third-party software systems and applications in the following areas to support its processes:

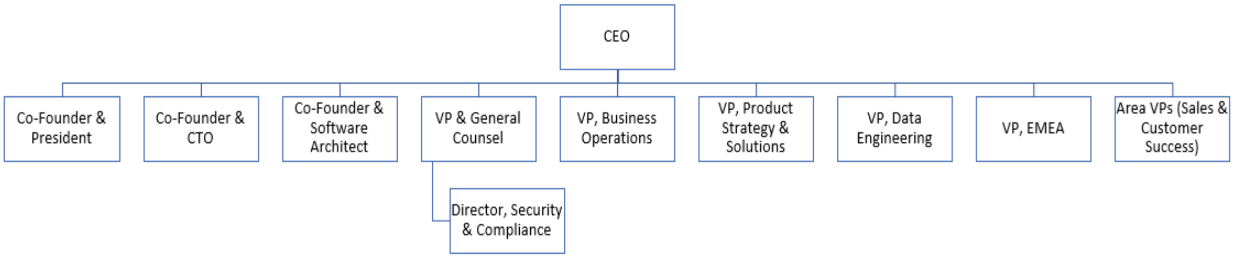
- System and networking monitoring
- Ticketing and workflow management
- Vulnerability management
- Google Workspace (Email Management & Others)
- Backup tools
- System logging
- Anti-malware
- Badge access
- Accounting and payroll systems
- Customer relationship management system

People

Organizational Structure

Yugabyte has a Board of Directors which includes members independent from Yugabyte, who possess relevant skills and expertise to provide oversight responsibilities for Yugabyte. The Board operates under the Yugabyte Board of Directors Security Charter which establishes the Board's information security and compliance oversight requirements, information security compliance reporting requirements, and requirements related to achievement of Yugabyte's service commitments and system requirements.

Yugabyte is managed by and under the direction of an Executive Management Team, responsible for various operational areas of Yugabyte, including general management and administration. Refer to Figure 3 below for the Yugabyte Executive Management Team organizational chart.


CEO
Co-Founder & President
Co-Founder & CTO
Co-Founder & Software Architect
VP & General Counsel
VP, Business Operations
VP, Product Strategy & Solutions
VP, Data Engineering
VP, EMEA
Area VPs (Sales & Customer Success)
Director, Security & Compliance

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

Figure 3: Org Chart

Yugabyte personnel are separated by job functions and divided into teams with defined responsibilities. These teams and their responsibilities, including the Executive Management Team, are as follows:

Team	Responsibilities
Executive Management	Provides overall Company governance and direction, 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 Team	Supports the Executive Team with talent acquisition, talent management, performance management and payroll under the direction of the Vice President (VP) / General Counsel.
Development	Owns responsibility for software architecture, design, and development under the direction of the Chief Technology Officer (CTO).
IT	Provides technical infrastructure and application support for internal teams and ensures processes are compliant with IT and Information Security Policies under the direction of the VP/General Counsel.
Cloud Operations	Manages and operates the production infrastructure hosted by cloud service providers under the direction of VP of Engineering.
Product Development & Management	Sets functional priorities for product development. Owns Product Roadmap and responsible for translating business requirements into specification for Software development team under the direction of the CTO.
Security & Compliance	Owns responsibility for risk management, due diligence, and internal compliance under the direction of the VP & General Counsel. The Security & Compliance department ensures Yugabyte 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 of Operations.
Product Strategy & Solutions	Provides brand management and external communication services under the direction of the VP of Product Strategy and Solutions.
Sales	Provides business development and customer solution implementations under the direction of the CEO.
Yugabyte Customer Success	Provides customer facing technical support, professional services, and product training under the direction of the Area Vice President.

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

Data

Yugabyte Data Security and Privacy Governance Procedures are formally documented to provide guidance for Yugabyte personnel regarding data classification.

Yugabyte's Data Classification Policy applies to data stored within the Yugabyte System and defines how Yugabyte categorizes data it stores, including the following:

Data Type	Description
Public Information	Information that is not confidential and already in the public domain or that Yugabyte 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 Yugabyte.
Confidential-Restricted Information	Information that is particularly sensitive Confidential Information. Confidential-Restricted data is any data whereby the unauthorized disclosure, alteration, or destruction of such data is likely to result in significant-to-catastrophic damage to Yugabyte's business.

Data Retention and Destruction

Customer data is fully managed over the lifecycle of use, from submission to destruction. Yugabyte's customers are responsible for any data backups beyond the scope of backup services offered by Yugabyte through YugabyteDB Managed.

Yugabyte reserves the right to scrub and/or delete customer data used in YugabyteDB Managed after ninety (90) days from the date of termination of the applicable Cloud Agreements. Client data retention requirements, differing from the 90-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.

Data Encryption

Data at rest is encrypted using advanced encryption standards (AES)-256. Yugabyte uses industry standards to encrypt sensitive data in motion. Internal communications from server to system level are encrypted using TLS 1.2 or higher along with secure ciphers.

Attachment A

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

Processes and Procedures

Yugabyte has formal policies and procedures for processes that could materially impact the security of its products. Policies and procedures are designed to segregate duties and enforce responsibilities for Yugabyte's internal controls. Policies are communicated to employees and made available on a central repository. Policies and procedures are reviewed and approved by Management at least annually. These policies include:

- Internal administrative policies: regulate internal functions such as Human Resources.
- Operational Procedures: define the standards and policies which govern software development and YugabyteDB Managed operations and management.
- Information Technology Policies: establish the framework of policies, procedures, controls, and assessment processes along with usage guidelines to mitigate risks of loss, misuse, damage, injury, illegal, or unethical acts.
- Information Security and Usage Policies: support the protection of customer data and Company confidential information.

Subservice Organizations

Yugabyte utilizes subservice organizations to perform certain key operating functions, specifically related to hosting services (Cloud computing service such as Platform as a Service (PAAS)) and IT Managed Services. The accompanying description includes only those policies, procedures, and controls at Yugabyte, and does not include policies, procedures, and controls at the third-party subservice organizations described below. The examination by the independent auditors did not extend to policies, procedures, and controls at the subservice organizations.

The types of controls at the subservice organizations expected to be in place to address the applicable Trust Services Criteria below, were assumed in the design of Yugabyte's controls, and are significant to Yugabyte's system, in combination with controls at Subservice organizations:

Subservice Organization	Service(s) Provided	Applicable Trust Services Criteria
Amazon Web Services (AWS)	Infrastructure hosting, network connectivity, firewalls, and hardware maintenance and support services	CC6.1 – Logical and Physical Access CC6.4 – Physical Access CC7.4 – Incident Response Plan CC 8.1 – Change Management CC9.1 – Risk Management A.1.1 – Processing Capacity and System Component Monitoring

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

Subservice Organization	Service(s) Provided	Applicable Trust Services Criteria
		A1.2 – Environmental Security Monitoring A1.3 – Recovery plan and procedures
Google Cloud Platform (GCP)	Infrastructure hosting, network connectivity, firewalls, and hardware maintenance and support services	CC6.1 – Logical and Physical Access CC6.4 – Physical Access CC7.4 – Incident Response Plan CC 8.1 – Change Management CC9.1 – Risk Management A.1.1 – Processing Capacity and System Component Monitoring A1.2 – Environmental Security Monitoring A1.3 – Recovery plan and procedures

Yugabyte, Inc.'s Description of the Boundaries of Its YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System

Complementary User Entity Controls

Yugabyte's System was designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation by user entities to complement Yugabyte's controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

User entities are responsible for considering whether the following controls have been placed in operation and are operating effectively as they are relevant to the service organization's achievement of its service commitments and system requirements based on the applicable Trust Services Criteria.

Applicable Trust Services Criteria	Complementary User Entity Controls
CC2.2, CC2.3	Customers are responsible for communicating relevant security, availability, and incidents to Yugabyte through Identified Channels.
CC6.1, CC6.6	Customers are responsible for configuration password settings and options that control access, including password preferences, IP address authentication, integrated authentication, and API controls.
CC6.1; CC6.2	Customers are required to securely store authentication credentials. These include but are not limited to: user account ID, password, authentication certificates or other access control, encryption, and security measures.
CC6.1, CC6.2, CC6.3	Customers are responsible for ensuring logical access to the System remains restricted, with access granted on a need only basis. Monitoring activities are performed to verify that access levels are suitable for each authorized user employee over time and ensuring access credentials are removed when user employee access is no longer authorized.
CC6.3	Customers are responsible for managing internal user access to specific customer data.
CC6.4	Customers are responsible for restricting physical access to facilities housing sensitive information to authorized personnel.

Attachment B

Yugabyte, Inc.'s Principal Service Commitments and System Requirements

Service Commitments

Yugabyte makes service commitments to its customers and has established system requirements as part of YugabyteDB Managed. Service commitments are principal to the performance of the System and are made in consideration of the applicable Trust Services Criteria, laws and regulations that govern the provision of Yugabyte's services, and the financial, operational, and compliance requirements established by Yugabyte.

Specific to YugabyteDB Managed, new customers are provided and required to agree to Terms of Service, Service Level Agreement ("SLA"), Support Services Terms and Conditions, an Acceptable Use Policy, Data Processing Addendum, and other applicable customer agreements (collectively, the "Cloud Agreements"). The Cloud Agreements are the formal contract and usage policy agreed to by Yugabyte and its customers, including descriptions of the service offerings, service and security commitments and minimum system requirements. The Cloud Agreements and updates thereto, as well as descriptions of service offerings, security commitments and minimum system requirements are communicated to customers/users via Yugabyte's website and related ordering documents.

YugabyteDB Managed Service commitments include, but are not limited to, the following:

- Administrative, technical, and physical safeguards to prevent the loss, unauthorized use, access, or disclosure of Yugabyte proprietary data and customer data.
    - Access to YugabyteDB Managed Services' Support Team, who are available to address advanced features of the Software; advanced troubleshooting; and working with Yugabyte Engineering to address underlying issues within the product, core database, or code base.
- Daily backups of Yugabyte customer data (only available for paid YugabyteDB Managed Service).
- Standard scheduled maintenance performed during pre-determined times during which access to YugabyteDB Managed Services may be disrupted.
    - If possible, customers are notified prior to unplanned or emergency maintenance that falls outside scheduled maintenance windows. Notifications are delivered via Yugabyte's System status page. Additionally, customers have the ability to select maintenance windows.

System Requirements

Yugabyte establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Requirements are communicated in Yugabyte's policies and procedures, system design documentation, and contracts with customers. Information security policies define a Company-wide approach to systems and data protection. These policies address how services are designed and developed, system operation, management of internal business systems and networks, and the process for hiring and training employees. In addition, these documented policies and operating procedures address manual and automated processes required in the operation and development of Yugabyte's information systems, products, and services.

Report of Independent Service Auditors

To the Management of Yugabyte, Inc.:

We have examined Yugabyte, Inc.'s ("Yugabyte" or "the Company") accompanying assertion entitled "Assertion of Yugabyte, Inc. Management" (assertion) that the controls within Yugabyte's YugabyteDB, YugabyteDB Anywhere, and YugabyteDB Managed Services System (the System) were effective throughout the period February 1, 2022, to July 31, 2022, to provide reasonable assurance that Yugabyte'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).

Yugabyte uses subservice organizations to provide production infrastructure and customer database hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Yugabyte, to achieve Yugabyte's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Yugabyte's controls, the applicable Trust Service Criteria, and the types of complementary subservice organization controls assumed in the design of Yugabyte's controls. The description does not disclose the actual controls at the subservice organizations. 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.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Yugabyte, to achieve Yugabyte's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents Yugabyte's controls, the applicable Trust Services Criteria, and the complementary user entity controls assumed in the design of Yugabyte's controls. 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.

As certain controls did not operate during the examination period, in part or in whole, as circumstances that would warrant operation of those controls, in part or in whole, did not exist, we were unable to test and did not test the operating effectiveness of those controls as evaluated using the applicable Trust Services Criteria for the System throughout the period February 1, 2022, through July 31, 2022.

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

Report of Independent Service Auditors

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 February 1, 2022, to July 31, 2022, to provide reasonable assurance that Yugabyte'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 (AICPA). 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 examination engagement.

Our examination included:

- Obtaining an understanding of the System and Yugabyte's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Yugabyte'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 Yugabyte'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.

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 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 policies or procedures may deteriorate.

In our opinion, Management's assertion that the controls within Yugabyte's System were effective throughout the period February 1, 2022, to July 31, 2022, relevant to security, availability, and confidentiality to provide reasonable assurance that Yugabyte's service commitments and system requirements were achieved based on the applicable Trust Services Criteria is fairly stated, in all material respects.

Frazier + Deeter, LLC

September 30, 2022
Tampa, Florida