



PingCAP

PINGCAP (US), INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

TIDB MANAGED CLOUD SERVICES SYSTEM

FOR THE PERIOD OF FEBRUARY 1, 2022, TO MARCH 31, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To PingCAP (US), Inc.:

Scope

We have examined PingCAP (US), Inc.'s ("PingCAP") accompanying assertion titled "Assertion of PingCAP (US), Inc. Service Organization Management" ("assertion") that the controls within PingCAP's TiDB Managed Cloud Services system ("system") were effective throughout the period February 1, 2022, to March 31, 2023, to provide reasonable assurance that PingCAP'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

PingCAP uses various 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 PingCAP, to achieve PingCAP's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

PingCAP 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 PingCAP's service commitments and system requirements were achieved. PingCAP has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, PingCAP 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 systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve PingCAP's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve PingCAP'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.

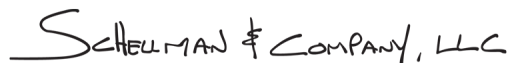
Because of their nature, controls may not always operate effectively to provide reasonable assurance that PingCAP's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness 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 PingCAP's TiDB Managed Cloud Services system were effective throughout the period February 1, 2022, to March 31, 2023, to provide reasonable assurance that PingCAP's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Emphasis of Matter

PingCAP's description of its TiDB Managed Cloud Services system states that PingCAP manually disposes of customer confidential data within 30 business days of receipt of request from customer administrators or upon service termination. However, during the period February 1, 2022, to March 31, 2023, PingCAP did not receive any requests for data deletion or customer service terminations that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criterion C1.2, which states "The entity disposes of confidential information to meet the entity's objectives related to confidentiality." Our opinion is not modified with respect to this matter.

 SCHILLMAN & COMPANY, LLC

Columbus, Ohio
June 29, 2023

ASSERTION OF PINGCAP SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within PingCAP (US), Inc.'s ("PingCAP") TiDB Managed Cloud Services system ("system") throughout the period February 1, 2022, to March 31, 2023, to provide reasonable assurance that PingCAP's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 March 31, 2023, to provide reasonable assurance that PingCAP'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. PingCAP's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 March 31, 2023, to provide reasonable assurance that PingCAP's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Our description of our TiDB Managed Cloud services system states that PingCAP manually disposes of customer confidential data within 30 business days of receipt of request from customer administrators or upon service termination. However, during the period February 1, 2022, through March 31, 2023, PingCAP did not receive any requests for data deletion or customer service terminations that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, the tests of operating effectiveness could not be performed for those controls as evaluated using trust services criterion C1.2, which states "The entity disposes of confidential information to meet the entity's objectives related to confidentiality."

DESCRIPTION OF THE BOUNDARIES OF THE TiDB MANAGED CLOUD SERVICES SYSTEM

Company Background

PingCAP seeks to help companies efficiently manage databases by providing secure, high performance, and scalable database-as-a-service (DBaaS) solutions. The fully managed service empowers companies to spend less resources on deploying, maintaining, and operating complex databases so focus can be redirected toward developing their applications.

PingCAP was founded in 2015 by Max Liu, Dylan Cui, and Edward Huang to satisfy the demand for databases that are easily managed, scaled, and maintained. Embracing the open-source community, PingCAP continues to value open communication and collaboration in providing a one-stop DBaaS solution.

Description of Services Provided

The TiDB Managed Cloud Services (“TiDB Cloud” or the “Service”) is a secure DBaaS solution that delivers a fully managed instance of TiDB, PingCAP’s flagship product. TiDB is a cloud-native hybrid transactional and analytical processing (HTAP) database that is MySQL compatible. TiDB Cloud can be deployed in both Amazon Web Services (AWS) and Google Cloud Platform (GCP) environments, providing users flexibility and resilience.

Instances of the TiDB Cloud are deployed in segregated virtual private cloud (VPC) environments which are peered with the user’s environment for secure connectivity. Users can horizontally scale their database by adding additional nodes within the TiDB Cloud portal. Data distribution is automatically balanced across the nodes and availability zones.

TiDB Cloud instances provide information regarding host data status, storage and performance analyses, and SQL issues in visual diagnostics for ease of monitoring. Updates released by PingCAP can be readily applied to running instances for up-to-date features and security.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

PingCAP has designed policies and procedures related to the TiDB Cloud service to meet its objectives, including the fulfillment of service commitments to customers, compliance with applicable laws and regulations, and the financial, operational, and compliance requirements that PingCAP has established. PingCAP’s commitments are communicated in standardized terms of service, service level agreements, and on the company’s public-facing website.

System requirements are specifications regarding how the TiDB Cloud system should function to meet PingCAP’s principal commitments to user entities. System requirements are specified in PingCAP’s policies and procedures, which are available to employees.

PingCAP's principal service commitments and system requirements related to the TiDB Cloud system include the following.

Principal Service Commitments and System Requirements		
Trust Services Category	Service Commitments	System Requirements
Security	<ul style="list-style-type: none"> • Maintain administrative and technical safeguards to protect the security of databases and customer data • System access is granted to authorized personnel only • Protection of data at rest and in transit • Regular security assessments • Identification and remediation of security incidents/events • Protection of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards • Develop, implement, and maintain an information security program designed to protect the security of the system and its information 	<ul style="list-style-type: none"> • Procedures for provisioning access to in-scope systems on a need-to-know basis, performing periodic access reviews, and managing credentials • Employee provisioning and deprovisioning standards • Minimum password standards • Use of multifactor authentication (MFA) • Periodic access reviews • Encryption standards for data at transit and at rest • Encryption key management standards • Configuration management • System logging, monitoring, and alerting • Incident handling standards • Antivirus on employee workstations • Penetration testing • Semi-annual internal audits • Change management standards • Vendor management • Background checks • Employee security policy acknowledgment • Security awareness training • Sanction procedures for misconduct
Availability	<ul style="list-style-type: none"> • Provide uninterrupted service to customers except during unforeseeable events • Continuous communication of TiDB Cloud service availability • Ability to recover and restore customer data in the event of a business disruption or disaster 	<ul style="list-style-type: none"> • System monitoring • Backup and recovery standards • Automated server recovery • Service status communicated through the company website • Host the TiDB Cloud service in geographically redundant locations • Disaster recovery plan tested annually

Principal Service Commitments and System Requirements		
Trust Services Category	Service Commitments	System Requirements
Confidentiality	<ul style="list-style-type: none"> • Maintain all customer data as confidential and not to disclose information to any unauthorized parties without written consent • Protect data from unauthorized deletion • Delete data upon service termination • Delete data within 30 days of written consent from customer 	<ul style="list-style-type: none"> • Data classification standards • Retention and destruction standards • Confidentiality agreements with employee and third parties prior to sharing customer data • Defined retention periods • Defined destruction procedures • Access to customer and confidential data limited to those with a business need

In accordance with PingCAP's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

The TiDB Managed Cloud Services system is deployed on AWS and GCP cloud infrastructure in the US. Infrastructure is deployed and replicated across multiple data centers for single-region resilience. TiDB Cloud is deployed on virtual compute instances; virtual firewalls are utilized to restrict inbound traffic to these instances. Persistent block storage volumes are attached to the virtual compute instances to support workloads. To further ensure the recoverability of data, backups are performed on a daily basis to object storage solutions.

Customer instances of TiDB Cloud are segregated in unique VPCs to prevent crosstalk. Customers are responsible for notifying PingCAP of changes to their systems that may result in an impact to the TiDB Cloud service or the customer's ability to access the service, such as changes to IP addresses or firewall rules. Customer data outside of TiDB Cloud instances are marked with unique identifiers in PingCAP-managed datastores to prevent customers from accessing other customer data.

PingCAP operates under a shared responsibility model and does not own or maintain any of the hardware located within AWS or GCP. As such, AWS and GCP are responsible for the respective underlying cloud infrastructure and PingCAP is responsible for securing the DBaaS platform deployed in AWS and GCP.

Access to the public facing application is encrypted using TLS, which is configured consistently through the use of configuration management tools. Frontend assets are delivered using a content delivery platform. Access to the platform's backend infrastructure is accessible through AWS for authenticated users.

Infrastructure and configurations are managed as code; PingCAP utilizes standardized configuration files and scripts to instantiate the service platform. Documented procedures are in place to guide PingCAP personnel in the performance of quality assurance (QA) approvals of source code, build jobs in the continuous integration tool, and code analysis.

The in-scope infrastructure consists of multiple applications, operating system platforms, and databases, as shown in the table below:

Primary Infrastructure			
Production Application	Business Function Description	Operating System Platform	Physical Location
TiDB Database	Underlying database used to support the TiDB Cloud service.	SQL	AWS / GCP (US)
Servers	Virtualized compute infrastructure to support the TiDB Cloud service.	Linux	
Firewall System	Virtual firewall system configured to protect the network perimeter and limit inbound and outbound access.	N/A – Managed Service	
Block Storage	Block storage volumes used as datastores for the TiDB Cloud service.		
Object Storage	Object storage leveraged for datastore backups.		
Bastions	Privileged access authentication to in-scope infrastructure components.	Linux	

Secondary infrastructure and supporting software include the tools used to support the development and change management processes (version control repositories and source code management software, as well as tools used to deploy changes and configuration items); security and availability logging, monitoring, analytics, and alerting systems; security logging tools; threat / intrusion detection system (IDS) tools; orchestration and cloud management platforms; endpoint protection software; password management and MFA systems; communications tools for internal messaging; workflow management systems for ticketing, issue tracking, and project management activities; disk encryption solutions for servers and workstations.

People

Responsibilities of managing internal controls over PingCAP’s security, availability, and confidentiality commitments are designated to the following roles:

- Executive management – responsible for overseeing company-wide activities, initiatives, and risk management. Management ensures personnel are appropriately trained and adhere to company policies and are responsible for ensuring those policies and procedures are sufficiently designed to meet commitments made to customers. Furthermore, management is responsible for implementing initiatives to realize the objectives set by the board of directors.
- Board of directors – responsible for establishing the company’s financial, operational, strategic, and compliance objectives and to lead by example to ensure company policies and code of conduct are adhered to.
- CISO – responsible for overseeing the security and compliance program; the design and operation of internal controls to satisfy customer commitments; and delegating responsibilities to other roles to ensure security and compliance objectives are met.
- Human resources (HR) – responsible for recruiting, employee record-keeping, organizational development, performance and behavior management, personnel development, and investigating reported misconduct.
- Information technology (IT) – responsible for managing corporate systems, which do not include production and pre-production TiDB Cloud environments, and for managing technical controls such as single sign-on (SSO) and antivirus software.
- Engineering – responsible for the secure development and maintenance of the TiDB Cloud service components and features and responsible for planning, developing, reviewing, and testing code changes when incidents or vulnerabilities require changes for remediation.

- Site reliability engineers (SRE) – responsible for the operation and availability of the TiDB Cloud service and for deploying changes developed by the engineering team and monitoring for anomalous activities that are indicative of a security, availability, or confidentiality incident. In addition, SRE members rotate through an on-call schedule to ensure immediate response to service issues is available.
- Product management – responsible for the planning of new features and components to the TiDB Cloud service based on market research, customer surveys and industry trends. In addition, product management sets the roadmap for the improvement of the TiDB Cloud service.
- Customer success – responsible for responding to and resolving customer issues and for escalating customer issues to appropriate teams (e.g., engineering, SRE, security committee) as needed.
- Security committee – responsible for administering the operation of internal controls, assessing PingCAP's risks, evaluating vendor relationships, and conducting internal audits to validate control operational effectiveness.

Procedures

PingCAP's information security policies and procedures are documented and made available to employees via the company intranet to support the operation of internal controls and maintain service commitments. Policies and procedures cover topics including, but not limited to, access control, change management, data retention and destruction, risk management, vendor management, and vulnerability management. PingCAP reviews policies and procedures at least annually to ensure accuracy over time. PingCAP management is responsible for maintaining, approving, and enforcing policies and procedures.

Access, Authentication, and Authorization

Access to system information is protected by multiple authentication and authorization mechanisms. Authorized users can access in-scope infrastructure by authenticating to the bastion host or AWS and GCP management console with a username, password, and MFA. Access to the TiDB customer portal is configured to authenticate users with a user account and password.

The production networks are administered remotely by authorized individuals who are provisioned access through identity and access management (IAM) roles. PingCAP utilizes role-based access controls (RBAC) by predefining authorized access groups. Groups are organized by job function and mapped to system access in a default access matrix (DAM). IT conducts semi-annual reviews of the DAM to ensure access mapping is accurate and up to date. Administrative privileges are further limited to a subset of individuals with business need for administrative access.

To further ensure the security of the in-scope systems, PingCAP utilizes virtual firewalls to restrict inbound traffic to these instances. By default, virtual firewalls are configured to block unauthorized inbound network traffic unless explicitly permitted by a firewall rule. VPC peering is also utilized to securely route traffic between PingCAP's internal virtual network and customer environments.

Outside of the system boundaries included within this report, user entities are responsible for configuring the authentication requirements (e.g., password policies and MFA requirements) and secure connections for their instances of the TiDB Cloud environment.

Access Requests and Access Revocation

PingCAP maintains an access control policy to guide personnel in performing access management activities including provisioning access, deprovisioning access, and conducting user access reviews.

Upon hire, access is provisioned to employees based on their job title and the DAM. The DAM identifies the default level of system access authorized for each job role. Requests for access beyond the standard privileges stated in the DAM require explicit approval by managers. Access requests and provisioning activities are documented in tickets for inter-departmental coordination and record-keeping.

When an employee is terminated, HR or the employee submits a termination ticket to communicate access removal responsibilities and the terminated employee's access is revoked within two business days to mitigate the risk of unauthorized access.

PingCAP performs user access reviews to further ensure access is restricted to authorized personnel. The user access review includes compiling user access lists from in-scope systems, requesting review from system owners, recording anomalies, confirming that inappropriate access has been rectified, and verifying that the DAM is up-to-date. Changes needed to the DAM are tracked and approved to ensure access is controlled.

Encryption keys are utilized to encrypt data at rest within databases and servers in accordance with PingCAP's encryption standards. Access to encryption keys used in the production environment is tightly controlled to a limited group of personnel to protect keys from unauthorized access or disclosure.

Individual customer instances are outside of the system boundaries defined within this report, and customers are responsible for maintaining and administering their users' access permissions within their instance of TiDB Cloud.

Change Management

PingCAP has established change management policies and procedures to outline separation of duties within the change management process and guide personnel in the request, documentation, testing, and approval of changes. PingCAP utilizes the agile software development methodology for application and infrastructure-as-code development. PingCAP's change management process involves participation from multiple functional units within the organization to ensure separation of duties. The planning phase of the change management process begins with customer feedback from the product management team and operational observations from the SRE and engineering teams. Change management meetings are held to discuss and communicate the ongoing and upcoming projects that affect the system and to translate plans and requirements into development objectives to be carried out by the engineering team.

Changes to production are comprised of three categories: application code changes, infrastructure changes, and manual changes. Application code and infrastructure changes are documented, developed, tested, approved, and tracked in GitHub repositories. Version control system is utilized to restrict access to source code and branch protections are configured to require peer review and approval by two individuals, other than the individual initiating the pull request, prior to implementation. The ability to modify branch protections is limited to authorized administrators and changes to branch protections are logged and reviewed to verify that change management procedures are not bypassed. A continuous integration tool is in place to automate building, testing (when applicable), tagging releases, and assigning versions. Static code analysis is performed to identify vulnerabilities in the source code and prevent the release of vulnerable code.

Application and infrastructure code changes are first deployed to pre-production environments to monitor for potential issues. The product manager, SRE team, and engineering team plan for deployment and document pre-release checklists to validate that the required procedures were followed, including approvals, prior to implementation to production. The ability to deploy to production is limited to the authorized SRE team who initiates the deployment following release approval.

Manual changes are performed as needed to resolve customer issues and maintain the operability of the service. A change ticket is created to document the nature of the manual change. Approvals are obtained prior to implementation and commands executed via SSM are logged in a dedicated S3 bucket. Management performs a review of manual changes to ensure that changes made directly to the production environment were documented in a change management ticket and approved. The review consists of the reviewer tracing SSM logs back to a change management ticket. If the reviewer fails to find an associated ticket, it is indicative that the manual change was unauthorized and should be investigated.

The production and development environments are logically segmented to help ensure the production environment is not impacted during the development and testing process. In addition, PingCAP generates dummy data for the purposes of testing when performing QA in pre-production environments to ensure confidential information is not used during the system design, development, testing, implementation, and change processes.

Configuration management tools are utilized to consistently deploy, maintain, and manage infrastructure-as-code using baseline configuration templates. Changes to baseline configurations are subject to the same change management process as application code changes. In addition, security updates and patches are installed on an as-needed basis or when a vulnerability or threat has been identified and follow the standard change management process.

Antivirus and Full Disk Encryption

Workstations are protected with full disk encryption and configured with antivirus software that has been configured to automatically update virus signatures and scan registered clients daily. Workstations are audited to ensure that antivirus software is up-to-date and operating as expected, and that full disk encryption is enabled.

System Monitoring

The security committee routinely monitors control operations through an annual internal controls review to ensure compliance with service commitments and control responsibilities. If control deficiencies are identified, strategies for remediation are discussed, approved, and implemented to promote continuous improvement. Results of control monitoring are communicated to executive management.

Logging applications are configured to monitor the availability of the TiDB Cloud service and alert SRE personnel for investigation and corrective action. When workloads surpass defined thresholds, SRE personnel are alerted to scale production resources to sustain service availability. The SRE team has also configured alerts when cloud resource quotas reach defined thresholds to trigger a request for a quota expansion from the cloud service provider.

Security monitoring tools and an IDS are configured to continuously monitor for suspicious activity indicative of malicious or unauthorized activity. Upon receiving security alerts, SRE personnel investigate and respond as needed to mitigate the risk of a security incident. Confirmed vulnerabilities affecting the TiDB Cloud service are triaged to determine whether action is merited. Third-party specialists perform annual penetration tests. Remediation plans are documented based on the penetration test findings and are monitored through resolution by PingCAP, if applicable. Vulnerabilities requiring remediation are done so in accordance with the standard change management process. SRE personnel also receive alerts and advisories from trusted sources to stay informed regarding new threats or developments in the security landscape.

Incident Response

Documented incident response and escalation procedures are in place to guide personnel in the monitoring, documenting, escalating, and resolving of problems affecting the Service. The customer portal is configured to allow customers to submit support requests and report potential incidents. A centralized ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting the Service. In the event an incident requires a change to the system, the standard change control process is followed to design, develop, review, test, approve, and deploy the change. Upon successful resolution of an incident, postmortem meetings are held, when applicable, to determine the root cause and identify lessons learned. Incident response plans are tested annually to identify gaps and promote continuous improvement.

Data Backup and Disaster Recovery

Backup policies and procedures are in place to guide personnel in the process of data backup and infrastructure recovery to meet PingCAP's availability objectives. An automated backup system is configured to perform full backups of production data at least daily to comply with documented data retention commitments and optimize recovery point objectives. The automated backup application monitors the status of backups and sends alert notifications to SRE personnel in the event of backup failures. Backups are encrypted at rest to secure data and protect sensitive information. The SRE team performs annual backup restoration tests to help ensure that PingCAP can reliably recover from a backup in the event of a disaster.

In some cases, an incident may rise to the level of a disaster. The incident response team escalates the incident to a disaster and triggers documented disaster recovery procedures. Production systems are implemented in a high availability architecture across multiple availability zones to help maintain availability during a disaster. Disaster recovery and incident response procedures are tested annually to ensure that the TiDB Cloud service can be successfully and efficiently restored.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Type	Data Description	Classification
Customer data - data uploaded to instances of TiDB Cloud	Customer data uploaded to TiDB Cloud is accessible by customers through the customer-facing TiDB Cloud platform and any connections to database instances configured by the customer.	Confidential
Customer metadata - data produced regarding customers' usage of TiDB Cloud	Customer metadata is reported through the customer facing TiDB Cloud platform for monitoring of performance metrics.	

Subservice Organizations

The cloud hosting services provided by AWS and GCP were not included within the scope of this examination.

The following table presents the applicable trust services criteria that are intended to be met by controls at AWS and GCP, alone or in combination with controls at PingCAP, and the types of controls expected to be implemented at AWS and GCP to achieve PingCAP's service commitments and system requirements based on the applicable trust services criteria.

Control Activities Expected to be Implemented by AWS and GCP	Applicable Trust Services Criteria
AWS and GCP are responsible for implementing controls that ensure logical access to the underlying network and virtualization management software is managed for its cloud hosting services where in-scope systems reside.	CC6.1 – CC6.3 CC6.5 – CC6.6
AWS and GCP are responsible for implementing controls that ensure physical access to data center facilities, backup data, and other system components such as virtual systems and servers is restricted to authorized personnel.	CC6.4 – CC6.5
AWS and GCP are responsible for implementing controls that ensure the data center facilities are equipped with physical and environmental security safeguards.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the TiDB Managed Cloud Services system.