Report on Pure Storage, Inc.’s Pure Storage System and Pure1 Edge Services Relevant to Security, Availability, and Confidentiality Throughout the Period December 1, 2024 to November 30, 2025

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: Pure Storage, Inc. ("Pure")

Scope

We have examined Pure's accompanying assertion titled "Assertion of Pure Storage, Inc. Management" (assertion) that the controls within the Pure Storage System and Pure1 Edge Services (system) were effective throughout the period December 1, 2024 to November 30, 2025, to provide reasonable assurance that Pure'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)*, in AICPA, *Trust Services Criteria*.

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 Pure, to achieve Pure's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Pure'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.

Pure uses subservice organizations to provide data center colocation 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 Pure, to achieve Pure'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 Pure'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

Pure 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 Pure's service commitments and system requirements were achieved. Pure has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Pure 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 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 Pure'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 Pure'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 Pure Storage System and Pure1 Edge Services were effective throughout the period December 1, 2024 to November 30, 2025, to provide reasonable assurance that Pure'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 Pure's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Louisville, Colorado
January 7, 2026

Section 2

Assertion of Pure Storage, Inc. Management

Assertion of Pure Storage, Inc. (“Pure”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Pure Storage System and Pure1 Edge Services (system) throughout the period December 1, 2024 to November 30, 2025, to provide reasonable assurance that Pure’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)*, in AICPA, *Trust Services Criteria*. 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 Pure, to achieve Pure’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of Pure’s controls.

Pure uses subservice organizations for data center colocation 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 Pure, to achieve Pure’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 Pure’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 December 1, 2024 to November 30, 2025, to provide reasonable assurance that Pure’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 Pure’s controls operated effectively throughout that period. Pure’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 December 1, 2024 to November 30, 2025, to provide reasonable assurance that Pure’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Pure Storage, Inc.

Attachment A

Pure Storage, Inc.’s Description of the Boundaries of Its Pure Storage System and Pure1 Edge Services

Type of Services Provided

Pure Storage, Inc. (“Pure” or “the Company”) believes data is foundational to customers’ digital transformation and is focused on delivering data storage solutions that enable customers to maximize the value of their data. The Company’s solutions serve data workloads on-premises, in the cloud, or in hybrid environments and include mission-critical production, test, development, analytics, disaster recovery, backup, and recovery.

Pure provides the following services:

- Solutions that allow applications, analytics, and development to move and execute quickly, helping customers make more impactful decisions. This is achieved by delivering low-latency, high-bandwidth, and maximum-density technologies.
- The opportunity to transform data management into a full or hybrid cloud model.
- Dashboards that present real-time and intuitive platform analytics that include artificial intelligence (AI)-based optimization that analyzes future workloads and global network issues to limit unforeseen infrastructure problems. AI-based dashboards are consistent with the EU AI Act, allowing customers to opt in and administer the option to shut off functionality altogether if desired.
- A subscription with total cost of ownership, eliminating the need for forklift hardware replacements, and providing customizable capacity and mobility, whether on-premises or in the cloud or hybrid cloud.

The Pure Storage System provides these services via the following applications:

- FlashArray: On-premises FlashArray sends metering (subscription usage data) and telemetry or system logs (collectively known as PhoneHome) to the ingestion servers. The ingestion servers apply processing and store the logs in Amazon Simple Storage Service (Amazon S3) buckets for consumption by the Pure1 Platform. Additionally, the ingestion servers send a copy of the metering logs to the Amazon Web Services (AWS) subscription processing account. The AWS subscription environment processes the metering logs, which translate into usage and billing.
- RemoteAssist: The RemoteAssist feature is used by Pure customer support to remotely access customer array consoles via Secure Shell Protocol (SSH) for support purposes. Customers must consent and activate the RemoteAssist function in order for Pure support staff to remotely SSH to on-premises FlashArray. Accessing the RemoteAssist function requires authorized personnel to first authenticate to the PureLogin authentication service, which is served from the dedicated AWS Security Account.
- Pure1 Platform: Telemetry or system logs used by support and engineering to support Pure customers are processed and used by several key web applications:
  - Pure1 Manage: A fleet management and monitoring web portal for customers available over the Internet.
  - Skyline: A customer management portal used by Pure and authorized support partners available over the Internet.
  - Playback: A read-only reconstruction of a customer’s array dashboard. The Playback feature requires authenticated and authorized access to Skyline.

Pure1 is a cloud-based centralized monitoring and reporting system for FlashArray and FlashBlade arrays. Coupled with RemoteAssist and the later addition of Pure1 Meta, Pure1 has evolved into a tool for:

- Monitoring system health and performance
- Optimizing storage and planning for future needs (with AI assistance)
- Performing upgrades and resolving issues (with assistance from Pure Technical Services)

As customers deploy larger fleets of systems, however, they have requested the ability to enable their systems more comprehensively and with greater autonomy. They are able to deploy entire groups of systems and install routine upgrades, optimizations, and optional features without assistance from Pure Technical Services.

Pure1 Edge Services (PES) is designed for advanced storage management by providing secure communications between management applications in the Pure1 cloud and companion agents on installed systems. The service also manages agent installations and upgrades. With PES, applications that both increase customer autonomy and simplify the management of Pure systems are possible.

PES functions as a platform for advanced storage management by providing opt-in secure communication between management applications in the Pure1 cloud and companion agents on installed systems. The companion agents use PES for installation and updates and, ultimately, as a gateway for functionality to securely flow between Pure1 and PES-enabled appliances.

PES is presented as a Pure1 dashboard enabling users to manage and monitor the main components of the system: Pure Edge Gateway (PEG) and agents.

PEG is the software on the customer system required to enable PES functionality. It is the entry point that provides an interface for over-the-air (OTA) software management and facilitates bi-directional communication between appliances and the cloud. It is also the endpoint of a secure communication channel between control planes in the Pure1 cloud and agents on edge devices.

Agents are PES-managed software components that use PEG for bi-directional communication. PES must be enabled on appliances to access full functionality. By downloading and installing agents, users opt in to advanced features.

Once PEG is enabled on the appliance, customers can use the Pure1 Manage dashboard to monitor at-a-glance gateway health information and update status for enabled appliances in their fleet. The dashboard also provides the ability to upgrade both PEG and agents.

Once each agent is downloaded and installed, it runs in its own unprivileged container (i.e., a container with no root access) and responds to messages from its companion control plane in the cloud. An orchestrator integrated with the base software in supported edge devices manages the agent containers. PEG itself also runs in a container.

Aspects of existing PES applications are as follows:

- Self-Service Upgrades (Purity//FA Upgrade Agent): Pure minimizes the operational impact of storage system software upgrades. Customers can schedule upgrades with Pure Technical Services engineers, who utilize the secure RemoteAssist channel to perform them. Using PES, the Self-Service Upgrade facility further streamlines the process by enabling customers to upgrade their systems without assistance from Pure Technical Services. The upgrade agent allows customers to monitor and act on everything from assessing upgrade readiness to initiating and monitoring Purity software upgrades for an entire fleet, all on the customer’s own schedule and without assistance from Pure Technical Services.

- Automated Issue Mitigation (Purity//FA Optimization Agent): Occasionally, issues impacting customer systems arise, usually related to common hardware components or external environments. For these situations, Pure develops corrective actions, identifies systems that might be affected, alerts their owners, and obtains approval to download and install corrections under customer control.

Using PES, the Purity Optimization Agent puts customers in control of corrective actions by eliminating the need for Pure Technical Services to oversee installation. Once customers have approved an action, downloading, verification, and installation are automatic.

PES applications (i.e., Self-Service Upgrades or Automated Issue Mitigation) each use a dedicated cloud provider account. In general, these applications formulate the interactions with Purity edge device software required to accomplish high-level tasks requested by Pure1 users (e.g. upgrading Purity or downloading approved corrections) and then send control commands to edge device agents. Agents interact with their edge devices to accomplish the tasks.

Pure Storage arrays appear to client computers (e.g. FlashArray hosts) as logical systems, with redundancy provided by two or more functionally equivalent physical components (e.g. FlashArray controllers). PES agents run on all physical components of a logical system in either active-active mode (e.g. Self-Service Upgrade) or active-standby mode. Each agent, as well as PEG itself, runs in a container managed by an orchestrator that is part of the operating environment. Agents are idle except when performing their management functions, so the overhead they impose on systems is negligible.

Pure Protect / DRaaS supports VMware vSphere workloads and AWS and works whether or not the customer uses Pure Storage arrays. Pure Storage arrays are optional and provide additional acceleration and integration. The DRaaS is delivered as part of the Pure1 Platform and operates within the scope of the Pure Storage System and PES. It provides disaster recovery for on-premises VMware vSphere environments, enabling customers to fail over protected virtual machines either to native AWS EC2 instances in the customer's VPC or to another VMware site, with orchestration and management performed through the Pure1 interface.

DRaaS uses VMware vSphere Storage APIs for Data Protection (VADP) and Change Block Tracking (CBT) to capture VM-level backups from on-premises vSphere environments, independent of the underlying storage array vendor, and replicates those backups into the customer's AWS environment according to customer-defined policies. During a test or production failover, DRaaS orchestrates provisioning of the recovery environment (for example, AWS networking and EC2 instances) and recovery of protected workloads using Pure1 workflows, while compute, storage, and networking are hosted by subservice organizations.

DRaaS shares the same infrastructure, security, and operational control framework as other Pure1 services in scope, including AWS data centers, segmented VPCs and security groups, centralized authentication via PureLogin, and PES agents and ingestion services that collect and process telemetry from customer arrays and edge components.

The boundaries of the system in this section details the Pure Storage System and PES. Any other Company services are not within the scope of this report.

The Boundaries of the System Used to Provide the Services

The boundaries of Pure Storage System and PES 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 Pure Storage System and PES.

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

Infrastructure

The Company utilizes AWS, MongoDB Atlas, and Snowflake to provide the resources to host Pure Storage System and PES. The Company leverages the experience and resources of AWS, MongoDB Atlas, and Snowflake to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Pure Storage System and PES architecture within AWS, MongoDB Atlas, and Snowflake to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, as shown in the table below:

Infrastructure	
Production Tool	**Business Function**
Amazon DynamoDB	Storing array software deployment configuration and statuses
Amazon S3	Storing the agent software packages
AWS IoT Core MQTT	Message broker for secure communication to and from devices
AWS IoT Greengrass	Managing and deploying software on arrays
Database as a Service (DBaaS): MongoDB Atlas	Data storage, configuration, and telemetry
Databases: MySQL, Snowflake	Customer FlashArray configuration, telemetry data storage, and ATOM storage database
Virtual server instances	Connection to physical servers via a hypervisor

Software

Software consists of the programs and software that support Pure Storage System and PES (operating systems (OSs), middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Pure Storage System and PES include the following business functions:

- Backup and replication
- Observability/ticketing platform for vulnerabilities
- Security information and event management (SIEM), logging system

- Threat detection, security posture
- Web application firewall (WAF)
- Endpoint detection and response (EDR), anti-malware
- Infrastructure monitoring
- Application monitoring, SIEM, logging system
- Source code management
- Third-party management platform
- Help desk, ticketing system
- Authentication and single sign-on (SSO) service for access to enterprise tools, federated SSO for customer integration
- Virtual private network (VPN) for client remote access
- Providing account information to Phonebook and non-SSO authentication
- Tracking customer support cases
- Patch management, configuration management
- SIEM
- Scanning cloud environment and vulnerability management
- Human Resources (HR) management system

People

The Company develops, manages, and secures Pure Storage System and PES via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
ATOM Team	Responsible for developing, testing, deploying, and maintaining cloud applications for automated installations of patches/mitigations on customer Pure systems to mitigate known software and hardware issues with Purity.
CDU Team	Responsible for downloading Purity upgrades, bundling the FlashArrays, and then executing the upgrades via customer-facing application programming interface (API) calls on the FlashArray.
Cloud Platform Engineering	Responsible for system reliability of the product environment.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the Pure Storage System and PES.
Global Information Security Office (GISO)	Responsible for information security across the Company.
HR	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

People	
Group/Role Name	**Function**
PES Team	Responsible for development, testing, and support of the PES platform, as well as for deployment of the platform's cloud services. The PES platform components that enable cloud-initiated features (e.g. those developed by the ATOM and CDU teams) are integrated to hosting systems by respective integration teams.
Product Security Team	Responsible for security, governance, and assurance of Company products. The Product Security Team is part of the GISO Organization.
Pure Information Technology (IT)	Responsible for management of endpoints.
System Integration Teams (FlashArray)	Responsible for PES platform components integration, orchestration, product-side testing, and distribution within the appliance systems.

Procedures

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

The following table details the policies, standards, and procedures as they relate to the operation of Pure Storage System and PES:

Policies/Standards/Procedures	
Policy/Standard/Procedure	**Description**
Data Classification Standard	Standard to ensure that employees can securely access all the information required to perform their job duties at any time and in a way that protects Pure's intellectual property and information solely meant for Company use.
Data Retention and Destruction Standard	Standard that sets forth the requirements of data retention and destruction at the Company in accordance with applicable legislation to support business requirements and enable business continuity.
Encryption Standard	Standard to ensure that employees can securely access all the information required to perform their job duties at any time and in a way that protects Pure's intellectual property and information meant solely for Company use.
Enterprise Resiliency Policy	Policy to address critical infrastructure, business continuity, disaster recovery, crisis management, and compliance needs and obligations.
Information Security Policy	Policy to ensure that employees can securely access all the information required to perform their job duties at any time and in a way that protects Pure's inventions and information meant solely for Company use.
Product Security Incident Response Standard	Standard to ensure the receipt and response of incoming security events and incidents impacting Company products or the cloud infrastructure supporting Company products that are publicly visible, customer affecting, or in general requiring public response.

Policies/Standards/Procedures	
Policy/Standard/Procedure	**Description**
Risk Management Standard	Standard regarding risks to Pure products and services for the purposes of identifying, assessing, and mitigating risk to Company platforms and services, such as the FlashArray and Pure1 systems.
Software Development Life Cycle (SDLC) Standard	Standard that details a formal SDLC methodology that governs the project planning, design, acquisition, testing, implementation, maintenance, and decommissioning of information systems and related technologies.
Vendor Risk Management Standard	Standard that details the acquisition, onboarding, status, approval, statement of work, and nondisclosure agreement (NDA) for vendors.
Vulnerability Management Standard	Standard that applies to employees involved in the development, testing, and deployment of Pure products and services for the purposes of identifying, classifying, mitigating, or remediating vulnerabilities within defined service level agreements (SLAs).

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer or end-user defines and controls the data they load into and store in the Pure Storage System and PES production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in the customer's own array and in accordance with their own data management policies and practices.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for Pure Storage System and PES:

Data	
Production Application	**Description**
Playback	Read-only reconstruction of customer's local array dashboard
Pure1 DRaaS	Disaster recovery service for on-premises VMware environments
Pure1 Edge Services	Control plane agents
Pure1 Edge Services	Infrastructure that enables control planes
Pure1 Edge Services	Service and control plane configuration
Pure1 Manage	Customer-created tags, or "labels," assigned to arrays
Pure1 Manage	Customer setup, performance summary, volume, and snapshot information
Skyline	Support tool for monitoring customer arrays

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities.

- User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list
- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities grant access to the Company's system to authorized and trained personnel.
- Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
- User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.
- User entities are responsible for understanding and complying with their contractual obligations to Pure Storage.
- User entities are responsible for notifying Pure Storage of changes made to technical or administrative contact information.
- User entities are responsible for ensuring the completeness and accuracy of data entered by user entity into applications.
- User entities are responsible for using strong passwords and for SSO, the configurations.
- User entities are responsible for maintaining their own system of record.
- User entities are responsible for supervising, managing and control of use of Pure Storage services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans to address the inability to access or utilize Pure Storage services.

Complementary User Entity Controls (CUECs)

The Company's controls related to the DRaaS cover only a portion of overall internal control for each user entity of the DRaaS. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC6.1 CC6.2 CC6.3 CC6.6 A1.2	• DRaaS on-premises VMware environments: User entities are responsible for designing, implementing, and operating controls over the hypervisors, vCenter, guest OS hardening, network segmentation, access control, patching, and backups.
CC6.1 CC6.2 CC6.3 CC6.7 A1.1 A1.2 A1.3	• For underlying non-Pure storage related to DRaaS: User entities are responsible for designing, implementing, and operating controls over configurations, availability, encryption, access control, and any data-at-rest protections on that array, which are outside Pure's system boundary.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS, MongoDB Atlas, and Snowflake as subservice organizations for data center colocation services. The Company's controls related to Pure Storage System and PES cover only a portion of the overall internal control for each user entity of Pure Storage System and PES.

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. CSOCs are expected to be in place at AWS, MongoDB Atlas, and Snowflake related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS, MongoDB Atlas, and Snowflake's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS, MongoDB Atlas, and Snowflake's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS, MongoDB Atlas, and Snowflake SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, MongoDB Atlas, and Snowflake 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 agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to AWS, MongoDB Atlas, and Snowflake management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Pure Storage System and PES to be achieved solely by the Company. The CSOCs that are expected to be implemented at AWS, MongoDB Atlas, and Snowflake are described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS, MongoDB Atlas, and Snowflake encrypt databases in their control.
CC6.4	• AWS, MongoDB Atlas, and Snowflake restrict data center access to authorized personnel. • AWS, MongoDB Atlas, and Snowflake monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 C1.2	• AWS, MongoDB Atlas, and Snowflake securely decommission and physically destroy production assets in their control.
CC7.2 A1.2	• AWS, MongoDB Atlas, and Snowflake install fire suppression and detection and environmental monitoring systems at the data centers. • AWS, MongoDB Atlas, and Snowflake protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS, MongoDB Atlas, and Snowflake oversee the regular maintenance of environmental protections at their data centers.

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 Pure Storage System and PES. Commitments are communicated in End User Agreements, the Privacy Notice, and the Purity Operating Environment Data Sheet.

System requirements are specifications regarding how Pure Storage System and PES 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 Pure Storage System and PES include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Pure protects information entrusted to the Company. • Pure implements physical, administrative, and technical safeguards designed to protect information from unauthorized access, use, or disclosure.	• Information Security Policy • Product Security Incident Response Standard • Risk Management Standard • Vendor Risk Management Standard • System Hardening Standard • Vulnerability Management Standard
Availability	• Pure uses commercially reasonable efforts to provide Pure Storage System and PES as a service to the end user with an uptime commitment of 99.9999% availability.	• Business Continuity and Disaster Recovery Policy
Confidentiality	• Pure ensures, in the event that an end user provides Pure with customer data (i.e., business contact details) in connection with the performance of the End User Agreement, that such customer data is disclosed and handled in accordance with applicable data protection laws. • Pure will not use or disclose any confidential information except as expressly authorized by the End User Agreement in the event that an end user provides Pure with customer data. • Pure will promptly return or destroy all customer data upon written request.	• Encryption Standard • Data Classification Standard • Data Retention and Destruction Standard