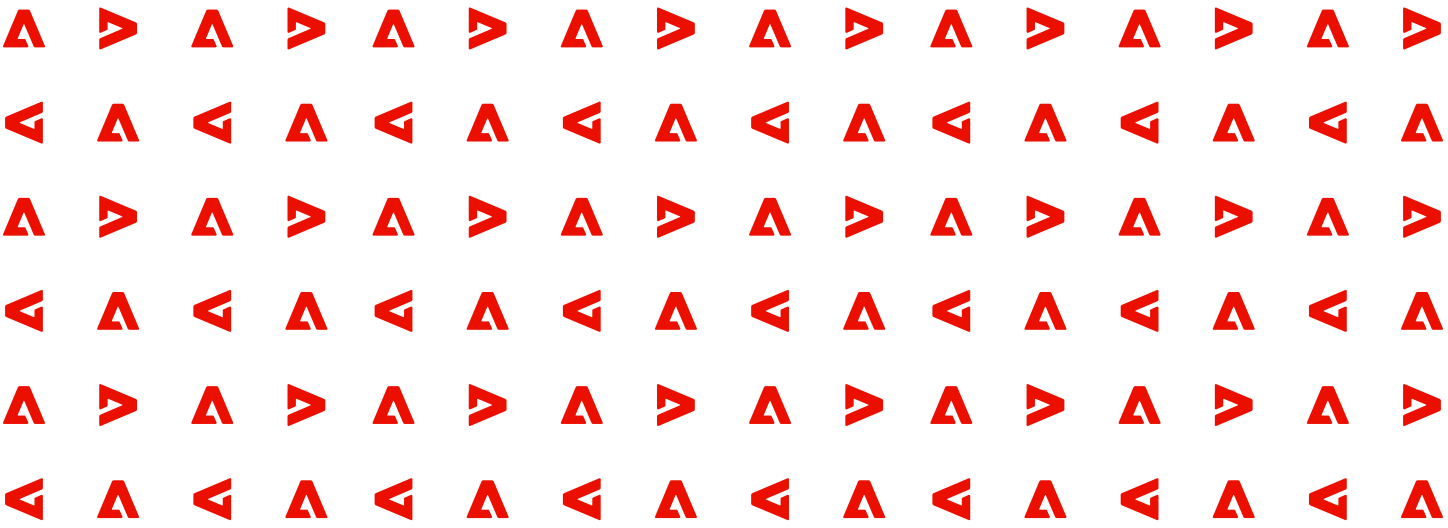
Adobe

SYSTEM AND ORGANIZATION CONTROLS 2 (SOC2) TYPE 2

Adobe Document Cloud

Report on Adobe's Description of its Adobe Document Cloud System and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security, Availability, and Confidentiality throughout the period November 1, 2022, to October 31, 2023.



Adobe

Contents

I.Independent Service Auditor's Report on a SOC 2 Examination

Tel: 415-397-7900
Fax: 415-397-2161
www.bdo.com

One Bush Street, Suite 1800
San Francisco, CA 94104

Independent Service Auditor's Report on a SOC 2 Examination

To the Board of Directors of Adobe Incorporated
San Jose, California

Scope

We have examined Adobe Incorporated's (Adobe or service organization) accompanying description of its Document Cloud system (the system) titled *Adobe Incorporated's Description of Its Document Cloud System* throughout the period November 1, 2022 to October 31, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Adobe'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*, in AICPA *Trust Services Criteria*.

The information included in Section V, *Other Information Provided by Adobe Incorporated That Is Not Covered by the Independent Service Auditor's Report on a SOC 2 Examination*, is presented by Adobe management to provide additional information and is not part of Adobe's description. Information included in Section V has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve Adobe's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Adobe uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Adobe, to achieve Adobe's service commitments and system requirements based on the applicable trust services criteria. The description presents Adobe's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Adobe'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.

Service Organization's Responsibilities

Adobe 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 Adobe's service commitments and system requirements were achieved. Adobe has provided the accompanying assertion, titled *Assertion of Adobe Incorporated Management* (assertion), about the description and the suitability of the design and operating effectiveness of controls stated therein. Adobe is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria

and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risks that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section IV.

Opinion

In our opinion, in all material respects:

a. The description presents Adobe's Document Cloud system that was designed and implemented throughout the period November 1, 2022 to October 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Adobe's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Adobe's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Adobe's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Adobe's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Adobe, user entities of Adobe's system during some or all of the period November 1, 2022 to October 31, 2023, business partners of Adobe subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

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

BDO USA, P.C.

November 21, 2023

II. Assertion of Adobe Incorporated Management

Adobe
345 Park Avenue
San Jose, CA 95110-2704
Phone 408 536.6000, Fax 408 537.6000

Assertion of Adobe Incorporated Management

We have prepared the accompanying description of Adobe Incorporated's (Adobe or service organization) Document Cloud system (the system) titled *Adobe Incorporated's Description of Its Document Cloud System* throughout the period November 1, 2022 to October 31, 2023 (description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with Adobe's system, particularly information about system controls that Adobe has designed, implemented, and operated to provide reasonable assurance that its 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,* in AICPA *Trust Services Criteria*.

Adobe uses subservice organizations to perform certain activities. A list of these subservice organizations and the activities performed is provided in Section III. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Adobe, to achieve Adobe's service commitments and system requirements based on the applicable trust services criteria. The description presents Adobe's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Adobe's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Adobe's Document Cloud system that was designed and implemented throughout the period November 1, 2022 to October 31, 2023, in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Adobe's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Adobe's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period November 1, 2022 to October 31, 2023 to provide reasonable assurance that Adobe's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Adobe's controls operated effectively throughout that period.

Adobe Incorporated

November 21, 2023

III.Adobe Incorporated's Description of Its Document Cloud System

Adobe Incorporated's Description of Its Document Cloud System

Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of Adobe Incorporated's (Adobe, service organization, or Company) Document Cloud system (the system) and the controls in place to provide reasonable assurance that Adobe'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,* in AICPA *Trust Services Criteria*, throughout the period November 1, 2022 to October 31, 2023 (the period), which may be relevant to the users of the system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Adobe.

Based on the nature of Adobe's Document Cloud system, mobile devices do not serve as information assets in relation to the system. As such, mobile device and security controls are not included in Section IV of this report.

Adobe uses subservice organizations to perform certain services. A list of these subservice organizations and the services performed is provided in the following table. The description does not disclose the actual controls at the subservice organizations.

Subservice Organization	Services Performed
Amazon Web Services, Inc. (AWS)	Provides infrastructure as a service through its AWS platform.
Microsoft Corporation (Microsoft)	Provides infrastructure as a service through its Azure platform.

Company Background

Founded in 1982, Adobe is one of the largest and most diversified software companies in the world. Adobe offers a line of products and services to consumers for creating, managing, delivering, measuring, optimizing, and engaging with compelling content and experiences across multiple operating systems, devices, and media. Adobe continues to market and license a broad portfolio of products and solutions in digital media, digital marketing, and content and document management. Adobe is a SEC-registered, publicly traded company and is subject to Sarbanes-Oxley (SOX) 404 compliance.

Services Provided

Adobe Document Cloud is a complete portfolio of secure digital document solutions that speeds business and drives better customer experiences by making manual, paper-based processes 100% digital. Document Cloud includes PDF Services and Adobe Acrobat Sign along with web and mobile applications that can be used standalone or integrated with an organization's existing document processes, business applications, or enterprise systems. The scope of this report includes all AWS regions hosting the Document Cloud systems in North America, Europe, Australia, Japan, and India, as well as Azure systems in North America.

The core solutions of the Adobe Document Cloud are briefly described in the table below:

Document Cloud Solution	Description
Adobe Acrobat Sign	Adobe Acrobat Sign enables businesses and consumers to collect legally binding electronic signatures through a web browser, mobile device, or in existing business applications or systems of record, while maintaining secure audit trails and meeting regulatory compliance requirements.
Acrobat Web	Acrobat Web enables its customers to convert, combine, and organize PDF documents. Features include integration with third parties, tabbed viewing, enhanced camera-to-PDF, accessibility, optimization for touch devices, improved PDF export, and Fill and Sign for iPhone.
Acrobat Services (PDF Services API)	Acrobat Services (PDF Services API) enables third-party developers to use PDF tools API for creating, combining, exporting PDFs and more.
Storage Stack	Storage Stack consists of Adobe's shared web services platforms. It offers a consistent approach to asset storage and management, social application programming interfaces (APIs), data services, search, and synchronization.
Identity Stack	Identity Stack includes the group of services that are responsible for providing access to creation and management of enterprise customers' user IDs. The user ID is the key component for authentication and access to Document Cloud.
Licensing &Entitlement Stack	Entitlement Stack includes the group of services that are responsible for providing the core entitlement engine for Adobe's Document Cloud that possesses the business logic to confirm what features, products and licenses are entitled to be used by an organization's account.
Administrative Consoles Stack	Admin Console Stack is an administrative console that allows Document Cloud team administrators to manage the users within their organization. It enables enterprise customers to manage their users, seats, licenses, subscription, and entitlements. It also allows customer admins to invite users within their organization to join their enterprise subscription account so they can use Document Cloud applications and services. Some key functionalities of the service include: • Administering user accounts and entitlements. • Corresponding with Adobe support. • Creating and managing software packages. • Configuring single sign-on and authentication options. Supporting Admin Console Stack is the Invite Accept engine/workflow that enables enterprise customers and Adobe administrators to accept an invitation to join the subscription. The stack provides users with the ability to create, edit, visualize, and manage access to the allocation and use of resources across the organizations within their hierarchy. As part of workflows to support legacy users, Document Cloud also has an additional identity system known as Neptune with identical functionalities.

Document Cloud Solution	Description
Collaboration Stack	Collaboration Stack includes a group of services that allows Document Cloud users to easily collaborate across applications remotely, offers an auto-complete search to find contacts and groups stored in address books, provides APIs for storing sharing policies in the database, and allows applications to detect and indicate user status on a resource
Adobe Developer Platform and Edge Gateway	Adobe Developer Platform is a suite of pre-integrated services/offerings that help in providing a consistent and cohesive developer experience across Adobe. Edge Gateway is a proxy layer that exposes internal Adobe services as internet facing endpoints and Software Development Kits. Adobe mobile and desktop applications connect with Adobe's Acrobat Sign through the Edge Gateway. Edge Gateway also provides traffic shaping, API security and API analytics features. Event Gateway enables customers to build event-driven experiences on top of Experience, Creative, and Acrobat Sign by providing cross-cloud events.
Configuration Stack	Configuration Stack includes services like the Janus Interaction Layer (JIL), which is a set of APIs that enables clients like Admin Console to fetch configurations used for data enabling, retrieving, and maintaining appropriate Document Cloud accounts. Hoolihan is also a service in this stack, which is a distributed "eventing" system with guaranteed delivery and sequential consistency. In addition to its high availability for publishers and low latency, it provides multiple options for consumers in how they receive events and supports both push (to a webhook) and pull (random access) models for consuming events, as well as a variant with load balancer semantics.
Search Stack	Search Stack enhances end-customers' search experience by providing a search feature that spans all Adobe products and services, regardless of the internal representation of systems.
Sensei	Sensei is a service with APIs that others can call for using different Sensei features like Async, Sync over Async, Streaming, and Batch.

Principal Service Commitments and System Requirements

In order to meet with security, availability, and confidentiality commitments of the services offered, Adobe has implemented several technology, process, and physical controls across its environments. Adobe documents and communicates its service commitments to its customers in form of its service-level agreements (SLAs) and contracts with customers. Service commitments include, but are not limited to:

Security

- Designing and implementing access control measures so that the fewest number of operators have access to data.
- Defining and deploying role-based access to restrict privileged access to information resources based on the concept of least privilege.
- Using a monitoring solution to identify any spikes in activity above a predefined critical security and availability threshold.

- Establishing trigger alerts for identified anomalies, and then using established procedures to address them and any potential security threats they may represent.
- Designing and implementing processes to ensure that changes to the network or production environment are documented, tracked, tested, authorized, and approved prior to migration to production.
- Using a monitoring solution to evaluate and check logs for potential misconfigurations.
- Using encryption technologies to protect customer data and/or assets, both at rest and in transit.
- Executing periodic vulnerability scans and penetration tests to identify vulnerabilities. Tracking and remediating them on a risk basis using defined SLAs.

Availability

- Designing and implementing controls to ensure system availability.
- Establishing business continuity and disaster recovery mechanisms to minimize data loss and ensure return to operations in the case of a disaster, using industry-standard mechanisms.
- Testing disaster recovery plans annually.
- Establishing mechanisms to notify its customers of potential operational issues that could impact the service availability.

Confidentiality

- Establishing commitments for customer data confidentiality and for data deletion and retention, as appropriate, within the customer contracts.
- Designing and implementing controls to ensure that data is kept confidential, retained, and deleted per customer contracts.

Customers have the ability to contact Adobe for product support, sales, and security-related queries through various channels, including phone and e-mail. Important information regarding security vulnerabilities that could affect specific versions of Adobe products and services is published on the Adobe Security Bulletin and Advisory website. An Adobe service status dashboard is maintained and made available at all times to its customers. Current status information can be checked by the customer on the service status dashboard.

Adobe also establishes operational requirements that support the achievement of these service commitments, relevant laws and regulations, and other systems requirements. These requirements are communicated in Adobe's policies and standards documentation. Policies define an organizationwide approach to how systems and data are protected and made available. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks, are managed and how employees are hired and trained.

System Incidents

A system incident is an incident that leads to the loss of, or disruption to, operations, services, or functions and results in Adobe's failure to achieve its service commitments or system requirements. Such an occurrence may arise from a security event, security incident, failure to comply with applicable laws and regulations, error, or other means. In

determining whether a system incident occurred resulting in Adobe's failure to achieve one or more of its service commitments or system requirements, considerations may include, but are not limited to, the following:

- Whether the occurrence resulted from one or more controls that were not suitably designed or operating effectively.
- Whether public disclosure of the occurrence was required (or is likely to be required) by cybersecurity laws or regulations.
- Whether the occurrence had a material effect on the service organization's financial position or results of operations and required disclosure in a financial statement filing.
- Whether the occurrence resulted in sanctions by any legal or regulatory agency.
- Whether the occurrence resulted in the service organization's withdrawal from material markets or cancellation of material contracts.

Incidents and events relevant to Adobe's service commitments and system requirements based on the applicable trust services criteria are important in monitoring, identifying, and evaluating if a system incident has occurred; however, incidents and events relevant to Adobe's service commitments and system requirements based on the applicable trust services criteria do not always rise to the level of a system incident. The evaluation of an incident or event relevant to Adobe's service commitments and system requirements based on the applicable trust services criteria will make that determination.

Adobe did not identify any system incidents that occurred during the period November 1, 2022 to October 31, 2023 resulting in Adobe's failure to achieve one or more of its service commitments or system requirements based on these considerations.

Components of the System Used to Provide the Services

Adobe maintains a Common Controls Framework (CCF) that is used in the implementation of control measures as a risk mitigation strategy to support Adobe operations, technology infrastructure, and security management activities. The domains are stated in the beginning of Section IV. Further details on these control domains and associated control activities are detailed throughout Section III and are identified by the phrase "(CCF XXX)" where XXX identifies the short acronym for the CCF domain. All CCF domains are explicitly mentioned in Section III except for Risk Management (CCF RM), which is detailed within multiple COSO Common Criteria (e.g., Risk Assessment, Monitoring Activities, Control Activities, Risk Mitigation).

Infrastructure

Adobe's Document Cloud infrastructure supporting the achievement of security, availability, and confidentiality criteria includes Adobe data centers and the subservice providers AWS and Microsoft. Management of the Adobe infrastructure and associated components within these environments is executed by the infrastructure team within Adobe's Document Cloud department.

Key elements of the infrastructure and subservice organizations are included in the following table:

Infrastructure	Description
AWS (Subservice Organization)	AWS directs and controls operations as well as establishes, communicates, and monitors policies and procedures for some of the production environments for Adobe's Document Cloud solutions. In addition, it operates, manages, and controls the components from the virtualization layer to the physical security of the facilities in which Adobe's Document Cloud components operate. In turn, Adobe assumes responsibility and management of the operating system (including updates and security patches), application software, and the configuration of the security group firewall provided by the subservice organization. Key AWS services utilized by Adobe include: • Elastic Compute Cloud (EC2) • Simple Storage Service (S3) • Relational Database Service (RDS) • Identity Access Management (IAM) • Virtual Private Cloud (VPC) • Security Groups • Lambda Functions Adobe periodically reviews third-party assurance reports to verify that AWS continually subscribes to a defined physical, environmental, and virtual security model.
Microsoft (Subservice Organization)	Microsoft directs and controls operations as well as establishes, communicates, and monitors policies and procedures for some of the production environments for Adobe's Document Cloud solutions. In addition, it operates, manages, and controls the components from the virtualization layer to the physical security of the facilities in which Adobe's Document Cloud components operate. In turn, Adobe assumes responsibility and management of the operating system (including updates and security patches), application software, and the configuration of the security group firewall provided by the subservice organization. Key Azure services utilized by Adobe include: • Virtual Machines • Managed Disk • Blob Storage • Managed Disk Snapshot • Azure Active Directory • Virtual Network • Network Security Groups Adobe periodically reviews third-party assurance reports to verify that Azure continually subscribes to a defined physical, environmental, and virtual security model.

Infrastructure	Description
Adobe Ethos	Ethos is an Adobe-wide service providing continuous integration and continuous delivery/continuous deployment (CI/CD) of containerized applications in public clouds and private data centers. Ethos is one of the core services of Adobe Foundation. The service is a compute platform running on standardized container engines. Ethos is based on the pillars of containerization, clusterization, CI/CD, and pipeline orchestration.
Adobe Oregon Data Center (OR1)	OR1 is an Adobe-owned data center located in Hillsboro, Oregon. The facility houses Adobe personnel, maintenance staff, and a production data center. Physical and environmental controls, as well as technical general controls for supporting systems, are operational within the facility.
Adobe Data Rooms	Adobe data rooms are Adobe-owned, fully serviced facilities that are located in Adobe San Jose (California), Lehi (Utah), and Maidenhead (London, United Kingdom) campus locations. These rooms are operationally much smaller than a standard data center, are managed by dedicated Adobe personnel and are not used as production data environments. Physical and environmental controls are common and operational within each facility — the only difference is that the Maidenhead data room is not supported by an emergency generator.
Bastion Hosts	Bastion hosts provide an additional authentication layer for internal users requiring logical access to Adobe Document Cloud production servers. Adobe personnel must first authenticate to the Adobe corporate network before being allowed to connect to the production network. To access the production network, users must authenticate through a bastion host with valid Adobe Active Directory (AD) credentials before being granted access to the production environment. Bastion hosts are only accessible from trusted Adobe networks and require multifactor authentication.

Software

Adobe Management has a focus on scaling software solutions to efficiently support Adobe's Document Cloud operational environment. The following key systems and applications are leveraged to support Adobe's Document Cloud core solutions:

Application	Description
Change Management	
GitHub Enterprise	GitHub is a centralized source code control system. It is implemented internally for the management of code repositories.
Service Knowledge Management System (SKMS)	SKMS is an internally developed set of tools, information, and systems that govern change and support Adobe technical operations.
Jenkins	Jenkins is an open-source continuous integration tool for dissemination of builds and change management controls for the production environment. Jenkins' server schedules builds and other deployment related tasks including testing where required.

Application	Description
Jira	Jira provides a system of planning, scheduling, implementing, and tracking changes that need to be completed for certain Adobe Document Cloud services.
Moonbeam	Moonbeam is a web application for continuous delivery flow.
Configuration Management	
Hubble	Hubble module is an enterprise tool that provides on-demand profile-based auditing, real-time security event notifications, automated remediation, alerting and reporting. It is used to monitor Windows and Linux hosts for compliance with Adobe-defined security hardening and configuration baselines.
MAVLink and Public Cloud Lockdown (PCL)	MAVLink collects available data from public cloud service providers including access logs, resource configurations, security alerts, and best practice recommendations into its centralized log repository. This data is consolidated in Splunk and provides visibility into asset information, network logs, and identity management. PCL enforces security policy and resource compliance requirements across public cloud accounts.
Image Factory	Image Factory is a solution for providing security hardened images (as per Adobe Security Standard) for AWS and Azure. Service team take these images as their base for hosting their service.
Identity and Access Management	
CAMP	CAMP is Adobe's proprietary tool for creating AWS accounts or Azure subscriptions and managing the "root" user for AWS accounts and Azure subscriptions.
HashiCorp Vault	HashiCorp Vault secures, stores, and controls access to tokens, passwords, certificates, API keys, and other secrets.
IAM Portal	IAM Portal is an Adobe proprietary tool used to manage access to LDAP groups. Each LDAP group is assigned an owner who is responsible for approving who can have access to that specific group.
KLAM	KLAM is Adobe's proprietary tool for access management to the AWS console and applicable production systems. KLAM is integrated with Adobe single sign-on (via Okta) and is used to map Adobe's corporate AD groups to AWS IAM roles.
Lightweight Directory Access Protocol (LDAP)	LDAP is a directory service protocol that provides a mechanism used to connect to, search, and modify directories. The LDAP directory service is based on a client-server model and syncs with Adobe's AD. Adobe LDAP implementations are synced with AD and deployed to provide efficient identity management for subsets of the organization's users.
Microsoft Active Directory (AD)	Adobe's AD stores user accounts, group memberships, and account data, and is used to manage access to the Adobe corporate network. Internal users are required to have an Adobe AD username and password to be able to authenticate to the Adobe corporate network and the Adobe Document Cloud production servers.
Okta	Access to production environments at Adobe requires Okta multifactor authentication.
SailPoint	The SailPoint identity management solution is the back-end technology that executes approved logical access changes requested within the IAM Portal.

Application	Description
Zero-Trust Enterprise Network (ZEN)	The Adobe ZEN platform enables employees with Adobe-managed devices to access many secure applications, resources, and data from anywhere without the use of a virtual private network (VPN).
People Resources	
Workday	Workday is a People Resources tool used to manage account and employment information of Adobe personnel.
Risk Management and Workstream Applications	
Jira	Jira is a ticketing application used to track and assign work items.
Site Operations	
Apogee/EcoStruxure	Apogee/EcoStruxure are the systems used to monitor HVAC/climate control within OR1.
CCURE	CCURE is an identity management platform used to manage badge readers at Adobe-owned facilities.
Security Access Management System (SAMS)	SAMS is an identity management platform used to facilitate physical access to Adobe-owned facilities.
StruxureWare/ EcoStruxure	StruxureWare/EcoStruxure are the systems used to monitor power to critical infrastructure within OR1.
Systems Monitoring	
New Relic	Software product used to monitor the availability of production systems and communicate alerts to appropriate personnel.
PagerDuty	PagerDuty software is used to communicate availability monitoring alerts to appropriate personnel.
ServiceNow	ServiceNow is an enterprise IT service management solution used to document availability monitoring tickets.
Splunk	Splunk is a log aggregation and analysis platform used to collect, analyze, index security logs such as system audit logs and report on Adobe-defined, critical system events.
Prometheus	Prometheus is an open-source monitoring solution for collecting and aggregating metrics for system monitoring and alerting toolkit which is supported by Platform Monitoring team within Adobe.
Training and Awareness	
Adobe Learning Manager	Adobe Learning Manager is used to deliver security training modules to Adobe personnel, collect completed module results, and remind users and management of incomplete modules.

Application	Description
Vulnerability Management	
Hubble	Hubble module is an enterprise tool that catalogs host properties including, but not limited to, installed packages, version information, running processes, and outbound connections. Hubble data is leveraged to quickly assess the environments' exposure to existing, or emerging, vulnerabilities and prioritize remediation.
Rapid7 Nexpose	Rapid7 Nexpose is a vulnerability assessment tool that scans, identifies, and reports vulnerabilities found on the network.
CrowdStrike Falcon	Next-generation endpoint detection and response (EDR) solution (malware detection).

People

Security Governance (CCF SG)

Adobe is led by the Chief Executive Officer (CEO) with the assistance and corporate oversight of the Board of Directors. The CEO and Board of Directors provide the overall strategic direction for Adobe. The CEO and Board of Directors meet at least quarterly and perform management review in regard to the overall company risk, audit, and governance.

Adobe has an established governance framework that supports relevant aspects of information security with policies and standards. Led by the Chief Security Officer (CSO), the governance framework includes an organizational structure for security, availability, and confidentiality, and is defined by roles and responsibilities for supporting the information security management system.

The Adobe Information Security Management Standard outlines the structure, roles, and responsibilities of principal participants in Adobe's Information Security Program. This standard is available on the Adobe intranet and applies to all security personnel from executive management to business process control owners.

Within the Adobe organization, personnel and business functions are segregated into departments according to job responsibilities. Adobe coordinates all security efforts under the CSO. The office of the CSO coordinates all product and security initiatives, Adobe's policy and standard governance model, security awareness training, and the implementation of Adobe security practices within the Adobe Service Lifecycle (SLC).

The CSO also manages various teams of security specialists who consult with key Adobe product and operations teams to achieve a high level of security for products and services. Security specialists also advise teams on security practices and advocate clear and repeatable development, deployment, operations, and incident response programs. The CSO conducts regular staff meetings to discuss priorities, projects, communication needs, compliance, and program performance. Reference Figure 1 below for further details on the teams managed by the CSO.

Technology Governance, Risk and Compliance (Tech GRC) is the primary driver for governance efforts at Adobe, including the CCF and technology compliance certifications. Tech GRC continuously revises and updates the process for unifying security and compliance requests, and channels them to the appropriate Adobe teams. Additionally, Tech GRC focuses on control automation and continuous audit to help maintain operating effectiveness.

People Resources (CCF PR)

The People Resources (PR) department is responsible for managing the Adobe workforce from onboarding to exit from the Company, via the human resources information system, Workday.

Adobe's Legal department is responsible for reviewing relevant policies and standards, including the Adobe Code of Business Conduct; identified inconsistencies with law, regulation, or Adobe policy are remediated.

Background Checks

Adobe new hires are interviewed to determine knowledge, competence, and cultural fit for their prospective roles and must pass a background check as a condition of their employment. There are two separate background check processes in place:

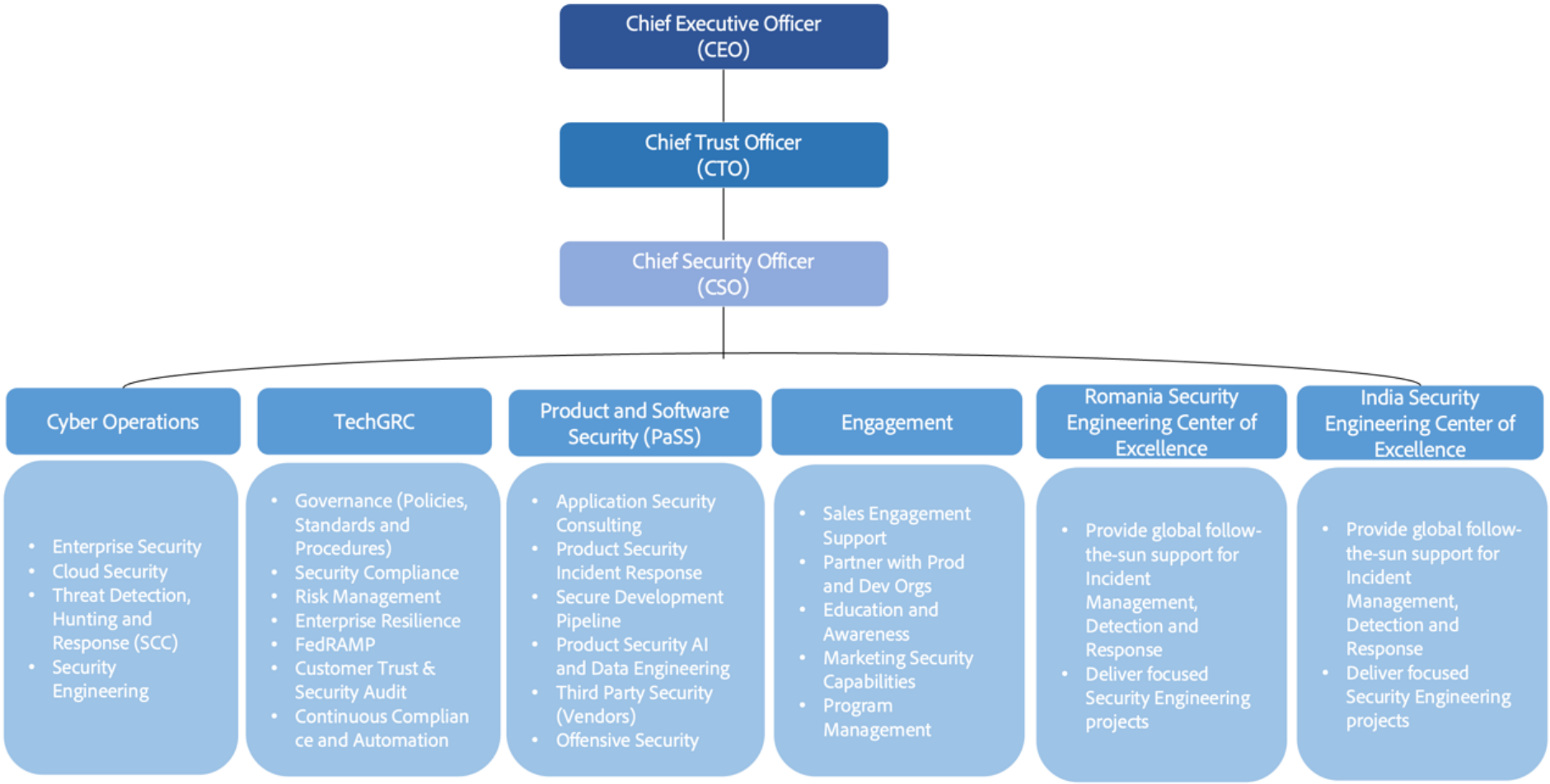
1) North America employees must have their respective background checks completed prior to employment.
2) Europe, the Middle East and Africa, and Asia Pacific employees are subject to a background check that is initiated prior to the beginning of their employment. Background checks in these regions must be completed either prior to an employee's first day of work or shortly after the beginning of their employment, depending on local laws and regulations.

Adobe's Employee Resource Center (ERC) defines standards that outline specific details for background checks performed prior to employment and allows Adobe to periodically repeat the exercise for existing personnel at the discretion of the Adobe PR department.

Adobe's background checks include inquiries regarding educational background, work history, court records (including criminal conviction records), and references obtained from professional and personal associates, each as permitted by applicable law. Background check requirements apply to new hire employees, including those who will be administering systems or have access to customer information.

The combined efforts of these teams enable the release of Document Cloud solutions in controlled operating environments.

Figure 1: Adobe Security Organization Chart



Processes and Procedures

Adobe Document Cloud subscribes to Adobe's corporate policies and standards, which have been developed to provide guidelines for management and employees to ensure security commitments are met. Corporate policies and standards are reviewed annually and made available to all Adobe employees at a central location. Individual teams within Adobe document and implement procedural documentation that supports and adheres to the requirements of corporate policies and standards. Adobe employees that fail to comply with policies and standards are subject to a disciplinary process. Adobe reviews exceptions to policies, standards, and procedures; exceptions are documented and approved based on business need and removed when no longer required.

Policies, standards, and procedures cover the following domains:

- Asset Management
- Business Continuity
- Backup Management
- Change Management
- Configuration Management
- Cryptography
- Data Management
- Entity Management
- Identity and Access Management
- Incident Response
- Network Operations
- People Resources
- Proactive Security
- Risk Management
- Security Governance
- Service Lifecycle
- Site Operations
- System Design Documentation
- Systems Monitoring
- Third-Party Management
- Training and Awareness
- Vulnerability Management

Data

Data, as defined for Adobe's Document Cloud, is inclusive of the information required to operate the services within the Adobe Document Cloud system as well as customer-provided data that these solutions process.

Adobe treats customer data within the Adobe Document Cloud system as confidential and does not use or share the information collected on behalf of a customer except when explicit permission from the customer is granted for support purposes, in the contract with the customer, or as set forth in the Adobe Terms of Use and Adobe Privacy Policy. Customers may choose to move their data outside of Adobe's Document Cloud system.

Description of the Controls Relevant to the Security, Availability, and Confidentiality Trust Services Categories

Control Environment

Adobe's control environment provides the foundation for all components of internal controls, including the ability of Adobe to operate and manage logical and physical access, data security, incident response, change management,

security operations, and monitoring. These are further described in the control activities section below. Adobe's control environment reflects the philosophy of senior management concerning the importance of well-designed security controls operating in environments where computer processing is performed.

Entity Management (CCF EM)

Board of Directors Oversight

Adobe's Board of Directors provides corporate oversight, strategic direction, and review of management. The Board of Directors meets at least quarterly and has three subcommittees:

- Audit Committee
- Executive Compensation Committee
- Governance and Sustainability Committee

Audit Committee

Adobe has an Audit Committee that is governed by a charter. The Audit Committee Charter specifies requirements for independence and oversees the following functions:

- Financial statement quality
- Enterprise risk management
- Regulatory and legal compliance
- Internal audit functions
- Information security functions
- External audit functions

At least on a quarterly basis, the CSO meets with the Audit Committee to review key information security issues, results of continuous monitoring activities, and current security compliance status.

Code of Conduct and Ethics

Adobe is committed to conducting business with the highest ethical standards and integrity. Employees are expected to conduct their work in accordance with governing documentation as defined by Adobe. The Adobe Code of Business Conduct (the Code) addresses the many situations that may raise ethical issues in business transactions, including compliance with law, regulation, and governing documentation. The Code outlines the principles that guide Adobe's interactions with employees, customers, partners, stockholders, and communities.

Training and Awareness (CCF TA)

Code of Business Conduct Training

The Code of Business Conduct mentioned in the previous paragraph is reviewed and acknowledged by each employee during the new hire process and subsequently once every two years within Adobe's Code of Business Conduct training.

General Security Awareness Training

Adobe requires employees to complete a general security awareness training on an annual basis. Training content is aligned with Adobe security policies and standards, reviewed and updated annually, and completely refreshed periodically.

Employees are given 30 days to complete the training once it is delivered. Users begin to receive completion reminders starting at 15 days, with their manager copied on the reminder starting at seven days and continuing through the training's due date. Reminder emails are sent with the user's manager copied for a defined period past the training due date. Management is responsible to ensure that team members complete this mandatory training.

Communication and Information

Internal Communication

Adobe's CSO is responsible for the coordination of development and maintenance of corporate policies and standards that impact information security at Adobe. The policies and standards are reviewed by relevant stakeholders and approved by document owners at least annually. The policies and standards are made available to all Adobe employees on a centralized Adobe intranet site. Additionally, the policies and standards are referenced in annual security and awareness training.

The CCF by Adobe is aligned with Adobe corporate policies and standards. Accordingly, the CSO meets with the Tech GRC team on an ongoing basis to understand operational effectiveness of the CCF implementation. The CCF is used to gauge Adobe's compliance with Adobe policies and standards. If there are any issues relevant to information security, management meets to review information security, availability, and confidentiality priorities, projects, and allocate resources to protect information systems.

External Communication

System Design Documentation (CCF SDD)

Product teams at Adobe are required to document and maintain system functionality, data flow, and boundaries as part of Adobe's internal documentation framework. Product owners are responsible for updating and approving the content of these pages periodically or as the products evolve.

Whitepapers are created and published by Adobe to help customers understand how their data is protected within a given product environment. Once the final review is complete, the whitepaper is published on the Adobe public website.

Risk Assessment

Security Risk Management

Adobe Security Risk Management is governed by the Risk Steering Committee, led by Adobe's CSO. The Risk Steering Committee is supported by a Risk Operating Committee made up of members, and subject matter experts, from across the Adobe Legal, Security, and Policy organization. Adobe has defined a Security Risk Management Framework based on industry best practices and guidance including, but not limited to, NIST 800-30 Revision 1, NIST 800-39, NIST Risk Management Framework, ISO 27005, and Open Factor Analysis of Information Risk (FAIR).

Adobe personnel submit identified security risks via an internal Risk Intake Form. The Risk Operating Committee meets monthly to discuss and review submitted risks for accuracy, likelihood, impact, and inherent risk. Approved risks will be added to, and tracked in, a centralized Security Risk Register. The Risk Operating Committee will analyze the inherent impact of a risk, along with its security posture including, but not limited to, policies, processes, tools, and controls that are in place to mitigate the risk. The inherent risk, less the operating security posture, determines the level of residual risk.

The Risk Steering Committee meets on a quarterly basis to review the Security Risk Register and prioritize risk treatment of high-risk areas. Management leverages insights from the Security Risk Management Program into annual planning and budgeting cycles.

Monitoring Activities

Adobe Document Cloud operates on a global scale, and process-supporting procedures are centrally defined and documented by process owners, who are responsible for the effective operation and remediation of Adobe CCF controls.

Management conducts ongoing monitoring of internal control performance. Monitoring occurs in the course of operations and includes regular management and supervisory activities. Adobe has established the Tech GRC team to monitor and assess the design and operating effectiveness of internal controls of various business units, including Document Cloud services.

The Tech GRC team also performs monitoring controls against established frameworks, establishing internal audit requirements and evaluating information systems and processes according to risk. The Tech GRC team works with the business units and management of operations and engineering teams to remediate and resolve findings identified during continuous monitoring reviews, internal control assessments, and annual risk assessments.

Audit findings are reviewed and prioritized based on risk. Findings are presented to appropriate management members, who design and implement a remediation plan that will sufficiently remediate identified control gaps. Remediation plans are reviewed by Tech GRC prior to implementation and again once the plans have been executed.

Monitoring of the Subservice Organizations

Adobe performs risk assessments of all subservice organizations, in addition to periodically obtaining and reviewing third-party assurance reports to evaluate the impact on the Adobe Document Cloud control environment.

Control Activities

The CCF is a comprehensive set of control requirements that have been rationalized from several different industry information security standards. Adobe reviews this framework on an annual basis to ensure it is aligned with both Adobe's business processes and requirements based on internal company feedback, customer requirements, and guidance from industry and regulatory bodies. The CCF is the main driver of compliance requirements defined in Adobe's corporate security policies and standards. Hence, CCF adoption is required for all Adobe teams.

Although the applicable trust services criteria and related controls are presented in Section IV, Trust Services Criteria, Related Controls, Tests of Controls, and Results of Tests, they are an integral part of Adobe's system description.

Logical and Physical Access

Identity and Access Management (CCF IAM)

Adobe Corporate Network Access Provisioning

A formal process is in place for granting and revoking logical access to Adobe for Adobe personnel, which includes full-time, part-time, temporary, contingent, and contracting vendors. All Adobe personnel who require access to the Adobe corporate network must have a valid, unique AD identifier and password to authenticate to any internally hosted service on the Adobe corporate network. Adobe leverages AD to create and manage personnel identifiers.

Adobe also employs a ZEN platform, with the use of a hardware-based ZEN certificate installed on Adobe-managed employee devices; employees are able to access many secure applications, resources, and data from anywhere without the use of a VPN, or reentry of usernames and passwords. The Adobe ZEN platform checks and validates Adobe-managed device security posture when users attempt to access the corporate resources and applications. All managed devices have unique identifiers that are used for authentication, and, based on the security posture information collected from the device, the ZEN platform determines if it is safe for that device to access the Adobe corporate resources.

The Adobe PR department enters the relevant personnel employment information into the PR system, Workday. Multiple times every day, the PR system sends updates regarding employee additions, updates, transfers, and terminations to the identity management system, SailPoint.

Production System Logical Access Provisioning

Individuals requiring access to the Adobe Document Cloud production environment are required to submit an access request via the Identity and Access Management Portal (IAM Portal). A user must be authenticated to the Adobe corporate network with a valid AD account, and also must authenticate to the IAM Portal via two-factor authentication, prior to submitting their access request. Within the IAM Portal, requesters are required to select the LDAP group for which access is being requested and provide business justification for the request. Each LDAP group is assigned an owner, who is responsible for approving who can have access to that specific group. As a part of the provisioning process, when cryptographic keys are required for authentication, the user uploads their public key within the IAM Portal, which is securely stored within SailPoint on the user's LDAP profile record.

Group owners are managers and supervisors within each respective department who are responsible for reviewing and approving user access requests. LDAP group owners are also able to manage access (i.e., add, modify, remove)

for users within their LDAP groups directly in the IAM Portal. Users who want to authenticate to production systems must have an active Adobe AD account. Users then authenticate to the production environment either via KLAM or multifactor authentication (MFA)-enabled bastion host, or a combination of the two.

Terminations: Logical Access Deprovisioning

For exiting or terminated Adobe personnel, PR or the employee's direct manager sets a termination date in Workday. Every day, an automated job queries user accounts that are scheduled to exit or terminate and disables the associated Adobe AD account. These actions immediately disable all access the exiting or terminated user has to the production systems.

Without an enabled Adobe AD account, a user will not be able to logically access the Adobe corporate network or the Adobe Document Cloud production environment, applications, etc., within Adobe's network. Physical access to Adobe facilities is similarly revoked via automated processes. In addition to logical and physical account disablement, management is notified to collect any Adobe-owned assets held by the exiting user, including physical access badge, office or cabinet keys, proprietary documentation, and Adobe assets including laptops, desktops, and peripherals.

Logical Access Review

Adobe Document Cloud group owners are prompted via email on a quarterly basis to review their group's membership within the IAM Portal. In the review, owners indicate the users whose access is no longer appropriate and certify that the remaining group membership is appropriate. Upon submission, the user accounts that have been selected for removal are immediately revoked as part of an automated workflow. Audit logs of these reviews are maintained within the IAM Portal.

Shared Secrets

Secrets for Adobe Document Cloud consist of shared account credentials (passwords and logical access keys). These secrets are used by authorized personnel to access hosts in the production environment. The service teams manage production secrets and rotate actively used credentials for shared and group accounts periodically (at least every 90 days).

Unique Identifiers

All Adobe personnel with a corporate AD account are provided with unique account identifiers; identifiers are never shared between Adobe personnel. This requirement is driven as part of Adobe's security governance program and is also a technical constraint within AD.

Password Authentication

Password settings are managed by Adobe's AD and within the IAM Portal. Password settings comply with Adobe corporate password standards. When a user updates their password within IAM Portal, the password is synced to their corporate account on the Adobe corporate AD instance.

Virtual Private Network

Remote access to the Adobe corporate network is automatically granted to all Adobe non-contingent workers and granted to contingent workers only when a business need exists. Additionally, remote access to Adobe trusted data

environments is provided through a VPN and requires the user to authenticate with a valid AD username, corporate password, and MFA. All remote connections to trusted data environments are accessed via VPN through managed gateways.

Key Repository Access

When cryptographic keys are required for authentication, the user submits their public key within the IAM Portal, which is stored within SailPoint on the user's LDAP profile record. Access to user public keys within SailPoint is limited to approved administrative staff.

Authentication to Adobe Document Cloud production environments requires the use of Secure Shell Protocol (SSH) and API keys, irrespective of the type of access required. Cryptographic keys are stored in Adobe-authorized repositories such as HashiCorp Vault. Access to the key repositories is governed by access to the Adobe LDAP. Access to the key repositories is restricted to individuals who are authorized and appropriate to have access and are restricted via MFA.

Multifactor Authentication

MFA is required prior to obtaining access to Adobe Document Cloud production systems. In order to access the production environment, the user must first authenticate with their username, private SSH key, and a password or a one-time-use token.

Administrative Consoles

Administrative consoles are the proprietary property of Adobe and are used by Document Cloud teams to provision new customer accounts and assist customers with technical troubleshooting. Access to the administrative console is restricted to only the engineering team.

Asset Management (CCF AM)

Inventory Management

Adobe Document Cloud maintains an inventory of system assets that are ingested into Splunk. Adobe performs periodic asset reconciliation and review as part of the quarterly compliance review process to validate the appropriateness of the cloud system assets and provide signoff.

Asset Transportation

The Adobe Data Center Operations team manages all requests for physical asset transportation between Adobe-owned data center locations. Asset transportation requests are documented in a system of record and include the Configuration Management Database (CMDB) reference to each device requested to be transported, the description of the asset transportation request, and related shipping and tracking information. All changes made to an asset are documented and maintained in the associated asset's history log in CMDB.

The Adobe Data Center Operations team ensures that the asset is packaged and shipped in an appropriate and secure manner during asset transportation.

Asset Maintenance

The Adobe Data Center Operations team manages all requests for physical asset maintenance in Adobe-owned data center locations. Asset maintenance requests are documented in a system of record and include the CMDB reference to each device requested to be maintained and the description of the asset maintenance request.

In addition to physical asset maintenance, the Adobe Data Center Operations team performs supporting system maintenance (e.g., HVAC, uninterruptible power supply [UPS], generator, fire extinguisher, and fire suppression) in Adobe-owned data center locations.

Site Operations (CCF SO) — Physical Access

Adobe-Owned Facilities

Secured Facility

Adobe-owned secured facilities include data centers and data rooms that restrict unauthorized access and are protected via a physical perimeter and secured entry points. All site personnel, including temporary and vendor personnel, must authenticate via a badge reader prior to accessing each facility.

Provisioning Physical Access

For additions and modifications of physical access to the Adobe-owned secured facilities, an access request must be submitted via SAMS. Requesters must first authenticate to the SAMS tool with their AD credentials, choose who they are requesting access for, select the physical site, and then select the appropriate role(s) within the site. If the request is appropriate, the site owner approves the access request, which grants the user physical access to the site using their Adobe-provided badge. Once approved, the user is required to authenticate via badge before being allowed physical access into a data room.

Deprovisioning Physical Access

For Adobe-owned secured facilities, in the event of a terminated or exiting user, the SAMS system receives updates from Workday and will automatically remove physical site and role access for a user whose account has an inactive status in the Workday application.

Periodic Review of Physical Access

On a quarterly basis, individuals with physical access to Adobe-owned facilities are reviewed by the site owner to determine whether the site account access is authorized and appropriate. Site owners use the SAMS application to view access for all active roles within their site. Site owners indicate whether the user should retain access or be removed from the group. Upon submission, all access changes will be immediately updated in the SAMS system via automated backend processes.

Physical Access Role Permission Authorization

Roles are defined and implemented to restrict physical access to the Adobe-owned facilities. All areas of the facility, including restricted areas, require a minimum of badge access prior to entry. Each area of the facility can only be accessed by certain roles, which have been configured in the physical security system to work only with specific

physical badge readers. Within the physical security system, roles are defined and configured. When physical access to the site is requested, the requester must select the role(s) that are desired. Upon approval, that role will grant the access to a user based upon the configuration of those roles. Each role has been created with consideration to least privilege to ensure that physical access can be granted on a granular level.

System Operations

Configuration Management (CCF CFM)

Baseline Configuration Standard

The Adobe Document Cloud is governed by a set of technical documents that specifies a security hardening and baseline configuration to safeguard customer data. Adobe's security hardening and baseline configuration standards are based on industry leading practices defined by the Center for Internet Security (CIS). Security hardening and baseline configuration standards apply to servers and network devices throughout the production environment. These standards are reviewed and updated as part of any significant change to the production environment, which includes the introduction of a new technology that was not previously covered.

Configuration Checks

Network and Host Configuration Changes

The Security team uses various mechanisms to detect whether configurations deviate from security hardening and baseline configuration standards. Hosts are monitored by a configuration management tool, which monitors file integrity and configuration settings of individual hosts. Hosts with configurations that are not compliant with the baseline configuration standard are flagged and an alert is sent to appropriate personnel, who identify the host and remediate the issue. Agents are installed as part of the provisioning process for production hosts. Additionally, the Security team works with solution teams periodically to ensure that their host environments have the appropriate agents running.

Adobe Document Cloud leverages MAVLink to collect available data from public cloud service providers, including access logs, resource configurations, security alerts, and best practice recommendations, into its centralized log repository. This data is consolidated in Splunk and provides the Security team with visibility into asset information, network logs, and identity management. Configurations that deviate from Adobe policy and standard are automatically flagged, and an alert is sent to either the resource owner or the Security Operations Center depending on the criticality of the deviation. Notifications or action requests are filed with appropriate personnel for remediation.

Network Operations (CCF NO)

Network Policy Enforcement Points

Adobe has set up network policy enforcement points (PEPs) within the Adobe production and corporate networks. All inbound traffic to and outbound traffic from the Adobe corporate network as well as the production infrastructure passes through a PEP, which is made up of Adobe firewalls and cloud service provider security groups. PEPs are configured based upon the requirements of the Adobe Perimeter Security Policy, which defines the approved whitelist of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports.

Network segmentation is implemented within the Adobe Document Cloud production environment to restrict access to authorized services, systems, and users. Users can only access the production environment from the Adobe corporate network.

Vulnerability Management (CCF VM)

Vulnerability Assessment

Adobe proactively monitors the production environment to identify and resolve vulnerabilities that could compromise the security of critical data. Vulnerability assessments are performed against the infrastructure, platform, and applications that make up the Adobe Document Cloud.

Network and Host Patch Management

For services hosted at Adobe-owned facilities, Adobe conducts network device vulnerability scanning on a quarterly basis as well as monitors infrastructure patches from vendors. The network engineering team prioritizes and executes the remediation of known network device vulnerabilities according to the risk.

Adobe has developed base configurations of CIS-hardened Amazon Machine Images (AMIs), as well as CIS-hardened Azure Virtual Machine (VM) images, which are deployed within the production environment. These images contain the latest patches as notified by CIS and are available for service teams to use.

In addition to AMI hardening, Adobe also conducts host vulnerability scanning on a scheduled basis via Nexpose. Nexpose is used to query all hosts on the Adobe Document Cloud production network. Completed scans deliver a report that enumerates identified vulnerabilities and assigns them a score. Tickets are created and assigned to appropriate personnel for identified vulnerabilities, which are prioritized based on risk and used to document and track patching. The Nexpose database of known host vulnerabilities is updated on an ongoing basis to ensure the latest known exploitable vulnerabilities are removed from Adobe's environment.

Penetration Testing

Adobe regularly engages approved third-party security firms on an annual basis to perform network and application external penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Testing requirements and criteria vary between each test and product, and usually include all user interfaces, newly implemented features, and unresolved vulnerabilities identified from prior scans. Upon receipt of the scan report provided by the third party, vulnerabilities are documented, assessed, prioritized, and assigned to a remediation plan if necessary. Product teams are responsible for the timely remediation of all findings, which are documented and tracked to remediation in a ticket, following guidance from the Adobe Vulnerability Management and Patch Management Standard.

External Information Security Inquiries

Adobe continuously monitors the threat landscape, shares knowledge with security experts, works to resolve incidents when they occur, and feeds this information back to development teams to promote and increase security for all Adobe products, including Adobe's Document Cloud. Adobe has a public website that details how the security community shares vulnerabilities with the Product Security Incident Response team (PSIRT).

The PSIRT thoroughly analyzes and investigates shared information from these mediums. If a vulnerability is confirmed, it is formally documented and managed by the SCC through a secure and formally defined response process. The PSIRT defines priority and severity ratings based on historical attack patterns in order to help customers prioritize security updates and developers assess the impact of known vulnerabilities.

Audit Logging

Adobe's Document Cloud production systems adhere to the logging requirements documented in the System Security Logging Standard, which is reviewed and updated annually. The standard defines logging requirements such as log attributes, retention, captured events, protection, and the Network Time Protocol (NTP) configuration.

Proactive Security (CCF PS)

Endpoint Detection Response Software

For protection at the server and workstation level, Adobe utilizes CrowdStrike Falcon for EDR. It monitors and records activities taking place on the endpoint, providing real-time and historical visibility necessary to automatically detect malicious activity, enabling Adobe security teams to automatically block activity and/or investigate and resolve incidents.

Systems Monitoring (CCF SM) — Security

Security Monitoring Alert Criteria

Teams responsible for information security monitoring define and implement security monitoring alert criteria, which are used to identify critical security events for the production environment. These criteria are defined and documented within Splunk and are periodically reviewed and updated.

System Security Monitoring

Adobe Document Cloud uses Splunk as a strategic information security monitoring solution. Production hosts are configured to send logs to a secured Splunk indexer as part of their baseline image. Additionally, the Information Security team works with solution teams on a periodic basis to ensure that their host environments are sending logs to an authorized Splunk indexer. The indexers categorize incoming logs so that they may be logically analyzed and reported on within Splunk.

As incoming data is received by Splunk and indexed, the logs are automatically reviewed by the system against the predefined alert criteria. If any of the criteria thresholds are exceeded, an alert is generated and sent to the Security Operations Center. Upon receiving an alert, the root cause is investigated and queued for resolution or flagged as a false-positive. Confirmed incidents are managed by the Security Operations Center, which follows a formally defined process for managing incidents.

Incident Response (CCF IR)

Incident Response Plan

Adobe has a documented and approved Incident Response Plan in place to assist designated response teams with managing incidents that impact Adobe or its customers. The plan is reviewed and approved annually and includes

guidance for identifying, preparing, preventing, prioritizing, managing, resolving, and preserving incidents. The five-step response process is defined within the plan and outlines the incident lifecycle from Planning, to Investigation, Containment, Recovery, and Lessons Learned. The plan also includes pertinent contact information, incident lifecycle flowcharts, and escalation procedures, and defines both roles and responsibilities for key personnel and various incident activities (e.g., event, alert, incident, vulnerability, etc.).

Incidents are reported to the team through human, monitoring, and intelligence channels, described below:

Channel	Description
Human Reports	These reports come from customers, users, and partners in the form of email, phone calls, or instant messaging.
Monitoring Reports	These reports come from Adobe-managed technology including, but not limited to, an intrusion detection system or monitoring log alerts, or via Adobe teams such as the Critical Response Center (CRC).
Intelligence Reports	These reports come from third-party or intracompany communications.

Responding to Incidents

When a reported incident first arrives, the Adobe Security Coordination Center (SCC) thoroughly analyzes and investigates the issue to determine whether it is a confirmed incident or a false positive. Confirmed incidents are manually tracked, and distribution is tightly controlled to protect sensitive information. Confirmed incidents are categorized by type (e.g., security, availability) and severity. The SCC tracks all incidents to resolution. As incidents mature, they are analyzed to determine whether they are evolving into a business continuity crisis. All crisis-declared incidents are managed with extreme caution and scrutiny and may require senior management to initiate business continuity activities.

The SCC works closely with the Adobe Legal team to coordinate any external communication to Adobe external stakeholders, including Adobe customers, law enforcement, and regulatory bodies.

Incident Reporting Contact Information

Adobe customers, personnel and the public may submit security inquiries, complaints, and disputes to Adobe via the publicly facing website and also through the customer support portal. Suspected abuse of personal information or an Adobe product can be reported via email.

Change Management

Service Lifecycle (CCF SLC) Workflow

Adobe Document Cloud products schedule major releases on a controlled basis. These releases are intended for new functionality, major bug fixes, and other significant product updates. These major releases are usually customer-impacting and are subject to the Adobe SLC, which is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. The Adobe SLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

All major releases as part of Adobe's SLC are initiated with a Jira ticket, which accompanies the release from inception to deployment. During the SLC process, the Jira ticket is continuously referenced and updated.

Major software releases are subject to the SLC, which requires business and management acceptance via the Concept Accept and Project Plan Commit phases prior to implementation.

Operational Change Management (CCF CHM) Workflow and Approval

The services constituting Adobe Document Cloud products implement changes outside of the scheduled major release cycle. These changes are intended for bug fixes, configuration changes, server patching, and other operational updates. These changes are tracked within Adobe's change management solutions, SKMS and Jira. Users with a valid AD account can submit a CMR via SKMS and Jira. The change submitter includes key information such as the change description, the scope of the change, the business justification for the change, and the change executor.

Upon submission, the ticket is routed to a predefined approval board for review. The approval board reviews the ticket and the information provided, including testing results and impact, and either approves or rejects the request. Approval may be automated for preapproved change models, where the risk and impact for the change is low and accepted by management. Upon the successful deployment of the change, the ticket is marked as complete in one of two ways:

1) Completed — According to the implementation plan.
2) Completed — Not according to the implementation plan.

If the change was implemented in a way that deviated from the approved plan as documented in the ticket, the change requester must document what was implemented differently and provide a business justification for why the plan was not executed according to the original plan.

Risk Mitigation

Third-Party Management (CCF TPM)

Vendor Security Review

The Vendor Security Review (VSR) Program evaluates a third-party vendor's compliance to Adobe's Vendor Information Security Standard to determine the types of data that can be shared with the vendor. A VSR is required for all third-party vendors that store or process Restricted, Confidential, or Internal Adobe data off-premises. The VSR requirement applies to both adding a new vendor to the Adobe ecosystem and continued engagement with existing vendors. VSRs must be performed on a periodic basis depending on the classification of the data a vendor is handling.

Third-Party Assurance Review

Adobe performs risk assessments of all third-party vendors and, in addition, performs an annual review of vendor assurance reports issued for critical third-party vendors. A listing of all third-party assurance reports, including the period of coverage, is documented and is maintained by the VSR team. The team documents any findings and reviews the vendor's management response to each. The team determines the impact of the findings against Adobe's security posture and risk appetite. If the findings have a critical impact on Adobe, the VSR team initiates a conversation with

the third-party vendors to gain additional understanding of the findings and associated remediation activities. All analysis and conclusions are documented.

Description of the Additional Controls Relevant to the Availability Trust Services Category

Systems Monitoring (CCF SM) — Availability

Adobe uses several commercial-grade tools to monitor its service and help ensure the highest levels of availability. The Adobe Document Cloud also provides a notification portal to inform customers about system downtime.

Availability Monitoring Alert Criteria

The Adobe Document Cloud operations teams define and implement a set of availability monitoring alert criteria, which outline availability thresholds and runbooks for the Adobe Document Cloud production environment. The alert criteria and runbooks are updated during continuing operations and as new system types are introduced to the production environment.

System Availability Monitoring

Monitoring tools used to support Adobe Document Cloud are integrated with the Adobe CRC tool. If the availability is outside of predefined thresholds, an alert will be sent to the Adobe CRC For major level incidents, a war room is auto-launched with appropriate personnel to expedite recovery time, and the issue is tracked through resolution. For lesser level incidents, the issue is resolved through runbook steps defined by the system owner.

Site Operations (CCF SO) — Environmental Controls

Adobe-owned secured facilities are architected to segregate office space, data center racks, utility rooms, storage closets and shipping docks such that each area of the building requires users to authenticate via a badge reader for entry. All restricted areas of the data center facility are protected by walls with non-partitioned ceilings and secured entry points. Additionally, Adobe-owned secured facilities have cameras, HVAC, humidity monitoring, temperature monitoring, fire suppression systems, clean air circulation, emergency power shutoff, universal power supplies, and emergency generators installed and operating. Data rooms utilize secured entry points as well as appropriate environmental safeguards and segregate space within the rooms to protect information assets located therein.

Temperature and Humidity Control

Within Adobe-owned secured facilities, data hall temperature and humidity levels are monitored and controlled against defined minimum and maximum thresholds. When temperature levels are outside the minimum and maximum threshold range, authorized personnel receive alerts. Site personnel investigate received alerts and take the necessary action to remediate the issue.

Fire Suppression Systems

Fire suppression systems are installed at Adobe-owned secured facilities. Upon activation, site personnel and emergency responders are notified and respond to the incident. These systems are maintained in accordance with manufacturer recommendations.

Power Failure Protection

UPS systems are in place at Adobe-owned secured facilities to help ensure uninterrupted power supply in case of a power outage. There are uninterruptible power sources, generators, and emergency lighting in place to support data halls in the event of a power failure. The current operational state of the UPS and generators is monitored, and maintenance is performed on a periodic basis.

Business Continuity (CCF BC)

Office of the CSO

Adobe's Business Continuity and Disaster Recovery Program is governed by the office of the CSO. The office of the CSO drives the adoption of Adobe's Enterprise Resilience Program, reviews the program strategy, and provides oversight of its execution. The office of the CSO meets at least once annually and more frequently as needed to discuss the governance and execution of the Business Continuity and Disaster Recovery Program.

Business Continuity Planning

Adobe is prepared to handle large business disruptions with its corporate business continuity program, which is driven by a Business Continuity Policy (BC Policy) and a Business Continuity Plan (BCP). The BCP provides guidance for managing the safety of personnel, assessing impact and mitigation efforts, escalation and execution of disaster recovery procedures, and event closure. The plan is reviewed and updated on an annual basis.

Individual teams are responsible for documenting a Disaster Recovery Plan (DRP) for each of their identified critical business functions, which are identified via a business impact assessment.

Contingency Testing

Business Continuity Plan Test

Annually, the Adobe BCP undergoes a Business Continuity Test with key personnel that collectively represent cross-functional business units. The BCP Test is structured in a way to ensure important cross-functional business units are engaged. Upon test conclusion, the test results are reviewed and approved, and, if required, necessary updates to the BCP are implemented.

Disaster Recovery Plans Test

Teams perform at least one functional test of a DRP annually. Upon conclusion, the test results are documented and approved by management, including whether the Recovery Time Objective (RTO) was met. DRPs are updated accordingly based on test results or business change.

Business Impact Assessment

Teams perform an initial and annual business impact assessment (BIA) exercise. The purpose of the BIA is to inventory business processes, assign criticality and recovery order, enumerate minimum recovery times, and identify internal and external dependencies. Business processes that are considered a critical business function must adhere to Adobe's disaster recovery requirements.

Capacity Forecasting

Adobe performs budget and capacity planning in order to maintain a stable and available environment for its customers during high-volume and traffic periods (e.g., holiday shopping, worldwide entertainment, or sporting events).

Backup Management (CCF BM)

Backup Configuration

Adobe performs periodic backups or has implemented failover technology of critical operational data and configurations. The purpose of these processes is to restore information to Adobe services in a timely manner should they become unavailable.

System Recovery Testing

Annually, individual teams perform a recovery test of their backup solution. Teams either obtain copies of their data backups and restore them into an operating environment or perform a failover test. Teams are responsible for validating the integrity of the restoration, and ensuring recovery point objectives (RPOs) are met. Upon conclusion, the test results are documented and approved by management.

Description of the Additional Controls Relevant to the Confidentiality Trust Services Category

Cryptography (CCF CRY)

Encryption of Data in Transit and at Rest

Adobe encrypts Adobe Restricted data in transit and at rest. Adobe restricted data is defined within the Adobe Data Classification and Handling Standard and is the most restricted class of data. Adobe restricted data includes, but is not limited to, debit and credit card numbers, bank account information, Social Security or taxpayer identification numbers, passport or driver's license numbers, passwords, digital certificates, and protected health information.

Adobe restricted data is encrypted during transmissions outside of Adobe-owned or Adobe-managed networks. Network communications between customers and Adobe Document Cloud are encrypted until the session is terminated or the user logs out of the session.

Adobe restricted data is encrypted at rest in accordance with Adobe cryptography standards.

Data Management (CCF DM)

Terms of Service

Adobe Document Cloud collects personal information from customers and enterprises only after the customer has accepted the Adobe Terms of Use or the enterprise has accepted the Adobe Enterprise Licensing Terms, which includes security commitments and availability SLAs. Each agreement requires acceptance to the Adobe Privacy Policy, which can be found on the Adobe website. Adobe's Legal team has documented product-specific licensing terms, which may be updated at any time to reflect solution releases and enhancements. All licensing terms are available to the public and can be found on the Adobe website.

Data Classification

All data collected, processed, transmitted, stored, or destroyed by or on behalf of Adobe must be classified and then protected in accordance with its designated classification.

Secure Disposal of Media

Adobe maintains an inventory of system devices, which is reconciled on a periodic basis in a CMDB. When a hosted asset is to be decommissioned, a data center operations custodian will arrange for disposal of the asset with an approved disposal vendor. When the asset has been securely disposed of, the data center operations custodian will update the relevant status fields in the CMDB.

Customer Data Deletion

Adobe deletes or purges data upon customer request. Enterprise customers can initiate the data management request by contacting Adobe's customer care team or respective Customer Service Manager. Adobe responds to customer requests, taking into consideration the urgency specified by the customer.

Complementary Subservice Organization Controls

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements were achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). A list of the subservice organizations and the activities they perform can be found at the beginning of Section III under Scope and Boundaries of the System. The following CSOCs are those controls that Adobe's management assumed, in the design of the system, would be implemented by a subservice organization and are necessary, in combination with controls at Adobe, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Number	CSOC	Applicable Criteria
Amazon Web Services, Inc., and Microsoft Corporation		
1.	Policies and procedures exist to ensure that logical access to production systems is restricted to authorized personnel.	CC6.1, CC6.2, CC6.3
2.	Logical access provisioning to information systems requires approval from appropriate personnel.	CC6.1, CC6.2, CC6.3
3.	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	CC6.1, CC6.2, CC6.3
4.	User and device authentication to information systems is protected by passwords that meet a defined Password Policy.	CC6.1, CC6.2, CC6.3
5.	Logical account and access reviews are conducted on a quarterly basis. Corrective actions are taken where applicable.	CC6.1, CC6.2, CC6.3
6.	Policies and procedures exist to ensure that physical access to facilities housing information systems is restricted to authorized personnel.	CC6.4

Number	CSOC	Applicable Criteria
7.	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks.	CC6.4
8.	Physical access provisioning to facilities housing information systems requires approval from appropriate personnel.	CC6.4
9.	Physical account and access reviews are conducted on a quarterly basis. Corrective actions are taken where applicable.	CC6.4
10.	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance to identified security requirements and business justifications.	CC6.6
11.	Information transmitted over public networks is encrypted.	CC6.6
12.	Vulnerability assessments are performed on the information systems and supporting network on a regular basis.	CC7.2
13.	Vulnerability assessment scan tools are periodically updated to the latest patches/signature definition files.	CC7.2
14.	Change scope, type, roles and responsibilities, and approval requirements are preestablished and documented.	CC8.1
15.	Prior to introducing changes into the production environment, approval from appropriate personnel is required based on the change description, impact of the change, test results, and backout procedures being defined.	CC8.1
16.	Fire detection and suppression systems are implemented and tested at appropriate intervals.	A1.2
17.	Temperature and humidity levels of data halls are monitored and maintained at appropriate levels.	A1.2
18.	Uninterruptible power supplies (UPS) and/or generators to support critical systems are implemented to support critical systems in the event of a power disruption or failure.	A1.2
19.	Contingency and disaster recovery plans exist and are periodically reviewed and approved.	A1.3
20.	Contingency and disaster recovery tests are performed on a periodic basis to ensure the recoverability of information systems and data in a disaster. Corrective actions are taken where applicable.	A1.3
21.	Redundant systems or periodic backups of data to resume system operations in the event of a failure are performed.	A1.3
22.	Annual backup restoration or failover and failback tests are performed to confirm reliability and integrity of system backups and redundancy.	A1.3

User Entity Responsibilities

User entities must perform specific activities in order to benefit from Adobe's services. These activities may affect the user entity's ability to effectively use Adobe's services but do not affect the ability of Adobe to achieve its service commitments and system requirements. These activities may be specified in agreements between user entities and Adobe, user manuals, and/or other communications. These activities are referred to as user entity responsibilities (UERs).

UERs are listed in the following table. They are the responsibility of the user entities of the system and are expected to be in operation at user entities to complement Adobe's controls. The list of UERs does not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

Number	UER
1.	Controls should be established to ensure user access provisioned to the customer's enterprise account is authorized and appropriate.
2.	Controls should be established to ensure user access to the customer's enterprise account that is no longer required (either in the case of a terminated employee or for other reasons) is removed appropriately.
3.	Controls should be established to ensure customers review and validate account access within their environments. Adobe provides customers with tools to view accounts that have access to their environment, including what role is assigned to each account.
4.	Controls should be established to ensure the security configurations of customer systems that transfer data or sensitive information to Adobe are appropriate.
5.	Controls should be established to ensure that data is retained or deleted accordingly.

IV. Trust Services Criteria, Related Controls, Tests of Controls, and Results of Tests

Trust Services Criteria, Related Controls, Tests of Controls, and Results of Tests

This report is intended to provide information to the management of Adobe, user entities of Adobe's Document Cloud system, and prospective user entities, independent auditors, and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information, including information about the controls implemented by the user entities. This report is intended to provide information about the suitability of the design and operating effectiveness of controls implemented to achieve the service commitments and system requirements based on the 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,* in AICPA *Trust Services Criteria*, throughout the period November 1, 2022 to October 31, 2023.

The examination was performed in accordance with attestation standards established by the AICPA, specifically, AT-C Sections 105 and 205 and the guidance contained in the AICPA Guide, *SOC 2 Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. It is each user entity's responsibility to evaluate this information in relation to its own system of internal control in order to assess its system of internal control. If an effective system of internal control is not in place at user entities, Adobe's controls may not compensate for such weaknesses.

This description is intended to focus on Adobe's controls surrounding the system throughout the period November 1, 2022 to October 31, 2023; it does not encompass all aspects of the services provided or controls performed by Adobe. Unique processes or control situations not described in the report are outside the scope of this report.

Tests of Controls

Our examination of the description of the service organization's system and the suitability of the design and operating effectiveness of controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria stated in the description, involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements, based on the applicable trust services criteria stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the applicable trust services criteria stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the applicable trust services criteria stated in the description were achieved throughout the period November 1, 2022 to October 31, 2023.

Our tests of controls were designed to cover a representative number of activities throughout the period November 1, 2022 to October 31, 2023 for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the applicable trust services criteria. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

BDO USA, P.C.'s testing of controls was restricted to the controls specified by Adobe in Section IV and was not extended to controls in effect at user entities or other controls that were not documented as tested under each control criteria listed in Section IV. The description of BDO USA, P.C.'s tests of controls and the results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of BDO USA, P.C. and should be considered information provided by BDO USA, P.C.

The basis for all tests of operating effectiveness includes inquiry of the individual(s) responsible for the control. As part of our testing of each control, we inquired of the individual(s) to determine the fairness of the description of the control and to evaluate the design and implementation of the control. As part of our inquiries, we also gained an understanding of the knowledge and experience of the personnel managing the control(s) and corroborated evidence obtained as part of other testing procedures. While inquiries were performed for every control, our inquiries were not listed individually for every control activity tested and shown in Section IV.

Additional testing of the control activities may have been performed using the following methods:

Method	Description
Inquiry	Inquired of appropriate personnel and corroborated responses with management.
Observation	Observed the application, performance, or existence of the specific control(s), as represented by management.
Inspection	Inspected documents and records indicating performance of the control.
Reperformance	Reperformed the control or processing application to ensure the accuracy of its operation.

When using information produced by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Presentation of Controls

Controls presented in the following tables may appear more than once if a control supports the achievement of multiple criteria. When a control is presented to support additional criteria, it will be presented in alpha-numeric order with the other controls for that criteria.

Security, Availability, and Confidentiality Categories, Related Criteria, and Controls Overview

Purpose and Content

The following matrix depicts the security, availability, and confidentiality categories, related criteria, and controls related to Adobe's Document Cloud.

Content	Description	
Criteria	The criteria represent the individual requirements for the in-scope categories of security, availability and confidentiality within the Trust Services Criteria issued by the AICPA.	
Controls	The controls included in the matrix depict Adobe Incorporated's controls related to each applicable criterion for the security, availability, and confidentiality categories. Control domains are identified as follows:	
	AM	Asset Management
	BC	Business Continuity
	BM	Backup Management
	CFM	Configuration Management
	CHM	Change Management
	CRY	Cryptography
	DM	Data Management
	EM	Entity Management
	IAM	Identity and Access Management
	IR	Incident Response
	NO	Network Operations
	PR	People Resources
	PS	Proactive Security
	RM	Risk Management
	SDD	System Design Documentation
	SG	Security Governance
	SLC	Service Lifecycle
	SM	Systems Monitoring
	SO	Site Operations
	TA	Training and Awareness
	TPM	Third-Party Management
	VM	Vulnerability Management

Security Category

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise its information or systems and affect the entity's ability to meet its objectives.

Availability Category

Information and systems are available for operation and use to meet the entity's objectives.

Confidentiality Category

Information designed as confidential is protected to meet the entity's objectives.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	EM-01-01	The Board of Directors provides corporate oversight, strategic direction, and review of management for Adobe. The Board of Directors is scheduled to meet at least quarterly and has three subcommittees: • Audit Committee • Executive Compensation Committee • Governance and Sustainability Committee	Inspected Adobe's Corporate Governance documents on Adobe's public Corporate Governance website and a selected Board of Directors quarterly presentation, and inquired of management, to determine whether the Board of Directors: • Has three subcommittees • Provides corporate oversight, strategic direction, and review of management for Adobe • Meets at least quarterly	No exceptions noted.
		PR-05-01	Adobe has documented the Code of Business Conduct, which is reviewed, updated if applicable, and approved by senior management periodically.	Inspected Adobe's Code of Business Conduct to determine whether it was reviewed and approved by senior management and addressed Adobe personnel conduct (including employees, independent contractors, and vendors).	No exceptions noted.
		TA-01-02	Biannually, Adobe full-time and temporary employees and interns complete a Code of Business Conduct training.	Inspected Adobe's Code of Business Conduct training material to determine whether it included Adobe full-time and temporary employees' responsibilities for adhering to the Code of Business Conduct.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
				Inspected Code of Business Conduct training completion records for a selection of new and current employees to determine whether new hires and existing employees completed the Code of Business Conduct training when they were onboarded or biannually thereafter.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	EM-01-02	The Audit Committee is governed by a charter, is independent from Adobe management, is composed of outside directors, and is scheduled to meet at least quarterly. The Audit Committee oversees: • Financial statement quality • Enterprise risk management • Regulatory and legal compliance • Internal audit functions • Information security functions • External audit functions	Inspected the committee assignments and charter documents on Adobe's public Corporate Governance website and a selected Audit Committee quarterly presentation, and inquired of management, to determine whether the Audit Committee is independent from management, is composed of outside directors, and is scheduled to meet at least quarterly to oversee risk management and compliance functions.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	SG-02-01	The CSO conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Inspected the CSO staff meeting agenda for a selection of quarters to determine whether the CSO staff meeting was held to communicate and align on relevant security threats, program performance, and resource prioritization.	No exceptions noted.
		SG-04-01	Adobe has an established security leadership team including key stakeholders in the Adobe Information Security Program; goals and milestones for deployment of the Information Security Program are established and communicated to the Company through the periodic security all-hands meeting.	Inspected Adobe's Information Security Management Standard to determine whether it established Adobe's Information Security Program, including the leadership team, key stakeholders, goals, and milestones.	No exceptions noted.
				Inspected the annual Information Security Management Standard Steering Committee meeting minutes to determine whether the security leadership team established and communicated security goals and milestones.	No exceptions noted.
		SG-04-03	Roles and responsibilities for the governance of information security within Adobe are formally documented within the Information Security Management Standard and communicated on the Adobe intranet.	Inspected Adobe's Information Security Management Standard to determine whether it was reviewed and defined information security roles and responsibilities for the governance of information security within Adobe.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
				Observed Adobe's corporate intranet to determine whether the Information Security Management Standard is communicated to the Company.	No exceptions noted.
		TPM-04-01	Adobe has documented a Vendor Information Security Standard that defines the responsibilities and governance requirements regarding vendor information security engagements. Contractual agreements are entered into with vendors that process or store Adobe data that define information security terms and SLAs.	Inspected Adobe's Vendor Information Security Standard to determine whether responsibilities and governance requirements regarding vendor information security engagements are defined.	No exceptions noted.
				Inspected the contract for a selection of third parties that process or store Adobe data to determine whether information security terms and SLAs are defined.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	PR-01-01	New hires are required to pass a background check as a condition of their employment.	Inspected background check results for a selection of new hires to determine whether background checks were performed in a timely manner for new hires.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
		PR-01-02	Adobe has established a check-in performance management process for ongoing dialogue between managers and employees. Quarterly reminders are sent to managers to perform their regular check-in conversation.	Inspected the check-in performance management process dashboard for a selection of quarters and departments, and the quarterly email reminder, to determine whether Adobe has established a performance process and managers are reminded quarterly.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	PR-01-02	Adobe has established a check-in performance management process for ongoing dialogue between managers and employees. Quarterly reminders are sent to managers to perform their regular check-in conversation.	Inspected the check-in performance management process dashboard for a selection of quarters and departments, and the quarterly email reminder, to determine whether Adobe has established a performance process and managers are reminded quarterly.	No exceptions noted.
		PR-03-01	Employees that fail to comply with Adobe policies are subject to a disciplinary process.	Inspected Adobe's Compliance Investigations Standard and various policies and procedures to determine whether a disciplinary process was defined for individuals who fail to comply with Adobe policies.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Environment					
				Inspected the noncompliance log and the case results for a selection of cases related to noncompliance with Information Security Policies and Procedures to determine whether employees that fail to comply with Adobe policies went through the disciplinary process.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	RM-02-02	The design and operating effectiveness of internal controls are continuously evaluated against the established CCF by Adobe. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected Tech Governance Risk and Compliance internal readiness results and QCR tickets to determine whether control owners have assessed the design and operating effectiveness of controls and corrective actions are tracked to resolution as appropriate.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	PR-03-03	Adobe has a business ethics hotline for employees and external parties to report ethical misconduct. Allegations are investigated and Adobe will take appropriate action for confirmed violations.	Inspected Adobe's public-facing website to determine whether employees and external parties are able to report ethical misconduct.	No exceptions noted.
				Inspected the Hotline Case Summary and EthicsPoint Incident Management Report and the case results for a selection of allegations to determine whether reported ethical misconduct(s) were investigated and appropriate action was taken, as appropriate.	No exceptions noted.
		SDD-01-01	Documentation of system boundaries and key aspects of their functionality are published to authorized Adobe personnel on the Adobe intranet.	Inspected wiki documentation for a selection of in-scope environments to determine whether they contained a description of the operating environment and its boundaries, including high-level design and implementation, for internal users of the system.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
		SG-01-01	Adobe's policies and standards are periodically reviewed, approved by management, and communicated to Adobe personnel.	Inspected a selection of Adobe's security, availability, and confidentiality policies and standards to determine whether they are documented, periodically reviewed, and approved by management.	No exceptions noted.
				Inspected Adobe's corporate intranet to determine whether Adobe's policies and standards are published and available to Adobe personnel.	No exceptions noted.
		TA-01-01	Adobe personnel complete security awareness training, which includes annual updates about relevant policies and how to report security events to the authorized response team. Records of training completion are documented and retained for tracking purposes.	Inspected Adobe's security awareness training material to determine whether it detailed: • Annual updates about relevant policies and standards. • How to report security events to the appropriate response team.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
				Inspected security awareness training completion records for a selection of Adobe full-time and temporary employees, the learning manager notification configuration, and an automated reminder email to determine whether Adobe personnel are reminded to complete security awareness training.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	CHM-03-01	Customer-impacting product and system changes are publicly communicated on the company website.	Inspected Adobe's public-facing website to determine whether customer-impacting product and system changes are publicly communicated.	No exceptions noted.
		EM-06-01	When customers sign up to Adobe's product and services, the customer is required to acknowledge a service agreement that includes considerations for protecting security, availability, and confidentiality and indicates the responsibilities of the user's and Adobe's responsibilities and commitments.	Observed a user create a new Adobe account to determine whether users are required to acknowledge the terms of services, which includes considerations for protecting security, availability, and confidentiality and indicates the responsibilities of the user's and Adobe's responsibilities and commitments.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
		IR-02-01	Adobe defines and updates external communication requirements for incidents, including: • Information about external party dependencies. • Criteria for notification to external parties as required by Adobe policy in the event of a security breach. • Contact information for authorities (e.g., law enforcement, regulatory bodies, etc.).	Inspected the Incident Legal Communications Requirements Standard to determine whether the following is defined: • Information about external party dependencies. • Criteria for notification to external parties as required by Adobe policy in the event of a security breach. • Contact information for authorities (e.g., law enforcement, regulatory bodies, etc.).	No exceptions noted.
		IR-02-02	Adobe provides a contact method to: • Submit complaints and inquiries • Report incidents	Inspected Adobe's public website to determine whether Adobe provides a contact method for external parties to submit complaints and inquiries, and report incidents.	No exceptions noted.
		IR-02-03	Adobe communicates a response to external stakeholders as required by the Incident Response Plan.	Inspected incident tickets and inquired of Adobe management for a selection of confirmed incidents to determine whether Adobe communicates a response to external stakeholders as required by the Incident Response Plan.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Communication and Information					
		SDD-02-01	Adobe publishes whitepapers to its public website that describe the purpose, design, and boundaries of the system and system components.	Inspected Adobe's public website to determine whether whitepapers for a selection of services (describing the purpose, design, and boundaries of the system and system components) were published.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	BC-02-01	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections, purchases are made against the established budget, and plans are updated on a quarterly basis.	Inspected infrastructure budgets to determine whether the budgets are established based on historical business activity and future growth projections, and plans were updated on a quarterly basis.	No exceptions noted.
		EM-06-01	When customers sign up to Adobe's product and services, the customer is required to acknowledge a service agreement that includes considerations for protecting security, availability, and confidentiality and indicates the responsibilities of the user's and Adobe's responsibilities and commitments.	Observed a user create a new Adobe account to determine whether users are required to acknowledge the terms of services, which includes considerations for protecting security, availability, and confidentiality and indicates the responsibilities of the user's and Adobe's responsibilities and commitments.	No exceptions noted.
		SG-02-01	The CSO conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	Inspected the CSO staff meeting agenda for a selection of quarters to determine whether the CSO staff meeting was held to communicate and align on relevant security threats, program performance, and resource prioritization.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		SM-03-01	Adobe defines availability monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected availability monitoring tool and system configurations for a selection of services to determine whether availability monitoring rules are defined and implemented to flag events and notify authorized personnel.	No exceptions noted.
		SM-03-02	Critical systems are monitored in accordance with predefined availability criteria, and alerts are sent to authorized personnel.	Inspected availability incident tickets for a selection of alerts generated to determine whether the alerts are triaged and resolved by authorized personnel.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	DM-01-01	Adobe's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	Inspected Adobe's Data Classification and Handling Standard to determine whether Adobe's data classification criteria are periodically reviewed, approved by management, communicated to authorized personnel, and used to determine the treatment of data.	No exceptions noted.
				Inspected the data classification tickets for a selection of services to determine whether Adobe reviewed and confirmed the data classification associated for the service.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		RM-01-01	A Security Risk Management Framework is documented which defines the security risk management methodology.	Inspected the Security Risk Management Framework to determine whether the framework is documented and defines the security risk management methodology.	No exceptions noted.
		RM-01-02	A comprehensive security risk register is maintained that incudes risks both internal and external to Adobe.	Inspected the security risk register findings and associated remediation to determine whether a comprehensive security risk register is maintained that includes risks both internal and external to Adobe.	No exceptions noted.
		RM-02-01	Adobe management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	Inspected the Security Risk Register, Security Risk Summary report, and a quarterly Risk Steering Committee calendar invite and inquired of management to determine whether management performed an annual risk assessment and identified risks had an overall residual risk ranking that was reviewed and approved.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
		SG-01-02	Adobe reviews exceptions to policies and standards; exceptions are documented and approved based on business need and removed when no longer required.	Inspected the GRC tool (used for policy management) for a selection of policy and standard exceptions to determine whether the exception was documented, approved based on business need, and removed when no longer required.	No exceptions noted.
		TPM-01-01	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address the impact the disclosed gaps have on the organization.	Inspected the VSR documentation for a selection of third parties to determine whether management obtained the third-party assurance reports, reviewed the controls and results, and took action on control gaps, as applicable.	No exceptions noted.
		VM-01-01	Adobe conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	Inspected vulnerability scan tool system configuration, vulnerability ticket automation, and vulnerability tickets to determine whether the vulnerability scanning tool was updated prior to running scans against the Adobe production environment, and tickets are automatically created when a vulnerability is identified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
				Inspected the vulnerability tracking tickets for a selection of vulnerabilities identified from the vulnerability scans to determine whether identified vulnerabilities were assigned a risk rating and were tracked through to remediation.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	RM-02-01	Adobe management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	Inspected the Security Risk Register, Security Risk Summary report, and a quarterly Risk Steering Committee calendar invite and inquired of management to determine whether management performed an annual risk assessment that took into consideration fraudulent behavior, such as theft of assets or inappropriate action to data and resources that could lead to financial and brand/reputational risk to Adobe.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Assessment					
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	RM-02-01	Adobe management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	Inspected the Security Risk Register, Security Risk Summary report, and a quarterly Risk Steering Committee calendar invite and inquired of management to determine whether management performed an annual risk assessment and identified risks had an overall residual risk ranking that was reviewed and approved.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	RM-02-02	The design and operating effectiveness of internal controls are continuously evaluated against the established CCF by Adobe. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected Tech Governance Risk and Compliance internal readiness results and QCR tickets to determine whether control owners have assessed the design and operating effectiveness of controls and corrective actions are tracked to resolution as appropriate.	No exceptions noted.
		TPM-01-01	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address the impact the disclosed gaps have on the organization.	Inspected the VSR documentation for a selection of third parties to determine whether management obtained the third-party assurance reports, reviewed the controls and results, and took action on control gaps, as applicable.	No exceptions noted.
		VM-02-01	Adobe conducts penetration tests periodically.	Inspected penetration testing results for a selection of services to determine whether penetration tests are performed periodically.	No exceptions noted.
				Inspected remediation tickets for a selection of vulnerabilities identified through penetration tests to determine whether the vulnerabilities are tracked through to remediation.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Monitoring Activities					
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	EM-04-02	Information security compliance results are reported to the Audit Committee by the CSO on a quarterly basis and support information security compliance certifications.	Inspected the Audit Committee presentations for a selection of quarters to determine whether information security compliance results including deficiencies are discussed.	No exceptions noted.
		RM-02-02	The design and operating effectiveness of internal controls are continuously evaluated against the established CCF by Adobe. Corrective actions related to identified deficiencies are tracked to resolution.	Inspected Tech Governance Risk and Compliance internal readiness results and QCR tickets to determine whether control owners have assessed the design and operating effectiveness of controls and corrective actions are tracked to resolution as appropriate.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	EM-05-01	Adobe maintains a CCF that is used in the implementation of control measures as a risk mitigation strategy to support Adobe operations, technology infrastructure, and security management activities.	Inspected Adobe's CCF to determine whether control measures have been selected and/or developed as a risk mitigation strategy to support Adobe operations, technology infrastructure, and security management activities.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	EM-05-01	Adobe maintains a CCF that is used in the implementation of control measures as a risk mitigation strategy to support Adobe operations, technology infrastructure, and security management activities.	Inspected Adobe's CCF to determine whether control measures have been selected and/or developed as a risk mitigation strategy to support Adobe operations, technology infrastructure, and security management activities.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	SG-01-01	Adobe's policies and standards are periodically reviewed, approved by management, and communicated to Adobe personnel.	Inspected a selection of Adobe's security, availability, and confidentiality policies and standards to determine whether they are documented, periodically reviewed, and approved by management.	No exceptions noted.
				Inspected Adobe's corporate intranet to determine whether Adobe's policies and standards are published and available to Adobe personnel.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Control Activities					
		SG-01-02	Adobe reviews exceptions to policies and standards; exceptions are documented and approved based on business need and removed when no longer required.	Inspected the GRC tool (used for policy management) for a selection of policy and standard exceptions to determine whether the exception was documented, approved based on business need, and removed when no longer required.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AM-01-01	Adobe maintains an inventory of system devices, which is reconciled on a periodic basis.	Observed the inventory of system devices to determine whether Adobe maintains the inventory in a system of record.	No exceptions noted.
				Inspected reconciliation documentation to determine whether system devices are reconciled on a periodic basis.	No exceptions noted.
		AM-01-02	Adobe assets are labeled and have designated owners.	Observed the asset repositories to determine whether the assets are labeled and have a designated owner.	No exceptions noted.
		CHM-02-01	Changes to the production environment are implemented by authorized personnel.	Inspected branch protection settings for a selection of services to determine whether branch protection rules were defined and implemented.	No exceptions noted.
				Inspected implementer names and their associated job titles for a selection of changes to determine whether the changes are implemented by authorized personnel and are different than the change approver.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CRY-02-01	Adobe restricted data that is transmitted over public networks is encrypted.	Observed the encryption certificate during the logon process for Adobe services to determine whether encryption is enabled.	No exceptions noted.
				Inspected the encryption expiration notification configuration to determine whether Adobe is informed of expiring or expired encryption certifications.	No exceptions noted.
		CRY-02-02	Adobe restricted data at rest is encrypted.	Inspected the database encryption configuration for a selection of services to determine whether the Adobe restricted data at rest is encrypted.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		CRY-03-01	Access to the cryptographic keystores is limited to authorized personnel.	Inspected the Adobe user access reviews for the cryptographic keystores for a selection of quarters to determine whether access to the keystores is limited to authorized personnel.	No exceptions noted.
				Inspected the secret storage tool authentication mapping for a selection of services to determine whether Adobe restricts the use of shared and group authentication credentials.	No exceptions noted.
		DM-01-01	Adobe's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	Inspected Adobe's Data Classification and Handling Standard to determine whether Adobe's data classification criteria are periodically reviewed, approved by management, communicated to authorized personnel, and used to determine the treatment of data.	No exceptions noted.
				Inspected the data classification tickets for a selection of services to determine whether Adobe reviewed and confirmed the data classification associated for the service	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAM-01-04	Adobe restricts the use of shared and group authentication credentials. Authentication credentials for shared and group accounts are reset every 90 days.	Inspected the secret storage tool authentication mapping for a selection of services to determine whether Adobe restricts the use of shared and group authentication credentials.	No exceptions noted.
				Inspected tickets for a selection of services and quarters to determine whether authentication credentials are rotated every 90 days.	No exceptions noted.
		IAM-02-01	Adobe requires unique identifiers for user accounts and prevents identifier reuse.	Inspected the Active Directory user account names to determine whether there were any duplicate (non-unique) accounts.	No exceptions noted.
		IAM-02-02	User and device authentication to privileged information systems is protected by passwords that meet Adobe's password complexity requirements.	Inspected corporate Active Directory group policy and IAM Portal/SailPoint system configuration to determine whether the password complexity requirements have been implemented as per the standard.	No exceptions noted.
		IAM-02-03	MFA is required for: • Remote VPN sessions • Access to trusted data environments	Observed a user remotely VPN to the Adobe corporate network and log in for a selection of production systems (e.g., trusted data environments) to determine whether MFA is required.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAM-04-01	Remote connections to the corporate network are accessed via VPN through managed gateways.	Observed a user remotely access the corporate network to determine whether remote access is accessed via VPN through managed gateways.	No exceptions noted.
		NO-02-01	Production environments are logically segregated from non-production environments.	Observed account names to determine whether separate accounts are created for production and non-production.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	IAM-01-01	Logical access provisioning to information systems requires approval from appropriate personnel.	Inspected the access management system workflow and provisioning details for a selection of new hires to determine whether approval is required prior to access being provisioned to in-scope systems.	No exceptions noted.
				Inspected a list of approvers and their associated job roles for a selection of new hires to determine whether approvers are appropriate.	No exceptions noted.
		IAM-01-02	Logical access is revoked timely.	Inspected the configuration between Workday and the IAM Portal/SailPoint to determine whether Active Directory accounts are automatically disabled.	No exceptions noted.
				Inspected termination details for a selection of terminations to determine whether the access is revoked timely.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAM-01-03	Adobe performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	Inspected the access review dashboard and QCR tickets for a selection of quarters to determine whether account and access reviews are performed on a quarterly basis and corrective action was taken where applicable.	No exceptions noted.
				Observed an approver update a user's access in SailPoint to determine whether access is automatically disabled by the system when revoked as a part of the quarterly access review.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	IAM-01-01	Logical access provisioning to information systems requires approval from appropriate personnel.	Inspected the access management system workflow and provisioning details for a selection of new hires to determine whether approval is required prior to access being provisioned to in-scope systems.	No exceptions noted.
				Inspected a list of approvers and their associated job roles for a selection of new hires to determine whether approvers are appropriate.	No exceptions noted.
		IAM-01-02	Logical access is revoked timely.	Inspected the configuration between Workday and the IAM Portal/SailPoint to determine whether Active Directory accounts are automatically disabled.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
				Inspected termination details for a selection of terminations to determine whether the access is revoked timely.	No exceptions noted.
		IAM-01-03	Adobe performs account and access reviews on a quarterly basis; corrective action is taken where applicable.	Inspected the access review dashboard and QCR tickets for a selection of quarters to determine whether account and access reviews are performed on a quarterly basis and corrective action was taken where applicable.	No exceptions noted.
				Observed an approver update a user's access in SailPoint to determine whether access is automatically disabled by the system when revoked as a part of the quarterly access review.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	SO-01-01	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	Observed the Adobe-owned data center facility to determine whether the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		SO-02-01	Physical access provisioning to an Adobe data center or data room requires management approval and documented specification of: • Account type (e.g., visitor, vendor, or regular) • Access privileges granted • Intended business purpose • Visitor identification method, if applicable • Temporary badge issued, if applicable • Access start date • Access duration	Inspected the physical security system workflow to determine whether requests for physical access required management approval and required documented specification of: • Account type (e.g., visitor, vendor, or regular) • Access privileges granted • Intended business purpose • Visitor identification method, if applicable • Temporary badge issued, if applicable • Access start date • Access duration	No exceptions noted.
				Inspected physical access request documentation for a selection of new physical access requests to the Adobe-owned data center and data rooms to determine whether access is approved.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		SO-02-02	Physical access that is no longer required in the event of a termination or role change is revoked. If applicable, temporary badges are returned prior to exiting the facility.	Inspected Adobe's Worldwide Badging Policy to determine whether it contains the requirement for temporary badges to be returned prior to exiting the facility.	No exceptions noted.
				Inspected the system configuration of the automated feed from the HR system to the badging system to determine whether it is configured to automatically revoke access to the Adobe-owned data center when access is no longer required as a result of a termination.	No exceptions noted.
				Inspected access removal evidence for a selection of terminated Adobe full-time or temporary employees and role changes to determine whether their physical access to Adobe-owned data centers and data rooms is removed in a timely manner.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		SO-02-03	Adobe performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.	Inspected physical access review documentation for a selection of data centers (Adobe-owned), data rooms, and quarters to determine whether the access reviews are completed and corrective actions are documented and resolved for any access that should be revoked.	No exceptions noted.
		SO-02-05	Intrusion detection and video surveillance are installed at Adobe data center locations; confirmed incidents are documented and tracked to resolution.	Observed the Adobe data center intrusion detection and video surveillance system to determine whether intrusion detection and video surveillance systems are installed at Adobe data centers.	No exceptions noted.
				Inspected the event logs and inquired of management and determined that there were no events that escalated to an incident at Adobe-owned data centers.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this control could not be tested.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		TPM-01-01	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address the impact the disclosed gaps have on the organization.	Inspected the VSR documentation for a selection of third parties to determine whether management obtained the third-party assurance reports, reviewed the controls and results, and took action on control gaps, as applicable.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	DM-01-01	Adobe's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	Inspected Adobe's Data Classification and Handling Standard to determine whether Adobe's data classification criteria are periodically reviewed, approved by management, communicated to authorized personnel, and used to determine the treatment of data.	No exceptions noted.
				Inspected the data classification tickets for a selection of services to determine whether Adobe reviewed and confirmed the data classification associated for the service.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		DM-06-01	Media that are flagged for disposal are sent to a third party for destruction. Adobe obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.	Inspected media decommissioning tickets and/or third-party destruction certificate for a selection of decommissioned media to determine whether the media was securely erased by a third party or was maintained in a secure facility pending erasure.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	IAM-02-03	MFA is required for: • Remote VPN sessions • Access to trusted data environments	Observed a user remotely VPN to the Adobe corporate network and log in for a selection of production systems (e.g., trusted data environments) to determine whether MFA is required.	No exceptions noted.
		IAM-02-10	Adobe users are authenticated against a Zero Trust model prior to gaining access to Adobe resources.	Inspected baseline compliance policy, missing certificate check and an example device to determine whether ZEN certificate authentication solution is available for devices, prior to gaining access to Adobe resources.	No exceptions noted.
		NO-01-01	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance with	Inspected the monitoring configuration for cloud services (i.e., AWS and Azure) to determine whether security rules are monitored for open ports.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
			identified security requirements and business justifications.	Inspected network device configurations for firewall and load balancer devices to determine whether traffic is restricted.	No exceptions noted.
				Inspected tickets for a selection of security rule deviations to determine whether the identified deviations from network security requirements are researched and resolved.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	AM-02-01	Adobe authorizes and records the entry and exit of systems at data center locations.	Inspected the tickets for a selection of moved assets to determine whether movement of assets within and outside the facilities is documented.	No exceptions noted.
		CRY-02-01	Adobe restricted data that is transmitted over public networks is encrypted.	Observed the encryption certificate during the logon process for Adobe services to determine whether encryption is enabled.	No exceptions noted.
				Inspected the encryption expiration notification configuration to determine whether Adobe is informed of expiring or expired encryption certifications.	No exceptions noted.
		CRY-02-02	Adobe restricted data at rest is encrypted.	Inspected the database encryption configuration for a selection of services to determine whether the Adobe restricted data at rest is encrypted.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		IAM-04-01	Remote connections to the corporate network are accessed via VPN through managed gateways.	Observed a user remotely access the corporate network to determine whether remote access is accessed via VPN through managed gateways.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CFM-01-01	Adobe ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	Inspected Adobe's standards and baseline images to determine whether security hardening and baseline configuration requirements have been established, reviewed, and updated periodically.	No exceptions noted.
		CFM-01-02	Adobe uses mechanisms to detect deviations from baseline configurations on production environments.	Inspected baseline deviation tool configurations to determine whether they are configured to detect deviations from security hardening and baseline configuration standards in the production environment.	No exceptions noted.
				Inspected tickets and meeting agendas for a selection of configuration management deviations to determine whether the detected deviations are tracked to resolution.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		PS-01-01	EDR software is deployed to continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity.	Inspected baseline workstation policy, an example workstation, and auto-install configurations to determine whether the EDR software is deployed on workstations and is configured to monitor, detect, and respond to security threats and malicious behavior and activity in the production environment.	No exceptions noted.
				Inspected baseline server policy, system logs for a selection of production accounts, and configuration for detecting hosts with missing EDR to determine whether EDR is deployed on servers and configured to monitor, detect, and respond to security threats and malicious behavior and activity in the production environment.	No exceptions noted.
				Inspected access review tickets of CrowdStrike administrators for a selection of quarters to determine whether ability to make changes to configurations is restricted to authorized personnel.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Logical and Physical Access					
		SLC-02-01	Source code is managed with Adobe-approved version control mechanisms.	Inspected the source code repository tools for a selection of services to determine whether Adobe-approved version control mechanisms/systems are utilized.	No exceptions noted.
		SM-02-02	Critical systems are monitored in accordance with predefined security criteria, and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Inspected the security monitoring tool for a selection of production accounts to determine whether critical information system activity is monitored.	No exceptions noted.
				Inspected alert resolution for a selection of security events to determine whether the events are triaged and resolved by authorized personnel as applicable.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	CFM-01-01	Adobe ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	Inspected Adobe's standards and baseline images to determine whether security hardening and baseline configuration requirements have been established, reviewed, and updated periodically.	No exceptions noted.
		CFM-01-02	Adobe uses mechanisms to detect deviations from baseline configurations on production environments.	Inspected baseline deviation tool configurations to determine whether they are configured to detect deviations from security hardening and baseline configuration standards in the production environment.	No exceptions noted.
				Inspected tickets and meeting agendas for a selection of configuration management deviations to determine whether the detected deviations are tracked to resolution.	No exceptions noted.
		SM-01-01	Adobe logs critical information system activity.	Inspected system logging configurations for a selection of production accounts to determine whether critical information system activity is logged.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
				Inspected missing log notification configuration, tickets, and results to determine whether Adobe has a process to detect and remediate if logs are not received.	No exceptions noted.
		SM-02-01	Adobe defines security monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected security monitoring tool configuration for a selection of alert rules to determine whether security monitoring rules are defined and implemented to flag events and notify authorized personnel.	No exceptions noted.
				Inspected the Splunk QCR access review for a selection of quarters to determine whether users that can add, modify, and delete alerts are limited to authorized personnel.	No exceptions noted.
		VM-01-01	Adobe conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	Inspected vulnerability scan tool system configuration, vulnerability ticket automation, and vulnerability tickets to determine whether the vulnerability scanning tool was updated prior to running scans against the Adobe production environment, and tickets are automatically created when a vulnerability is identified.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
				Inspected the vulnerability tracking tickets for a selection of vulnerabilities identified from the vulnerability scans to determine whether identified vulnerabilities were assigned a risk rating and were tracked through to remediation.	No exceptions noted.
		VM-02-01	Adobe conducts penetration tests periodically.	Inspected penetration testing results for a selection of services to determine whether penetration tests are performed periodically.	No exceptions noted.
				Inspected remediation tickets for a selection of vulnerabilities identified through penetration tests to determine whether the vulnerabilities are tracked through to remediation.	No exceptions noted.
		VM-03-01	Adobe installs security-relevant patches, including software or firmware updates.	Inspected Adobe's hardening standards and base images to determine whether AMIs and Azure VM images are reviewed and updated periodically.	No exceptions noted.
				Inspected vulnerability remediation tracking tickets for a selection of vulnerabilities to determine whether security-relevant patches are identified and tracked through to remediation.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	SM-02-02	Critical systems are monitored in accordance with predefined security criteria, and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Inspected the security monitoring tool for a selection of production accounts to determine whether critical information system activity is monitored.	No exceptions noted.
				Inspected alert resolution for a selection of security events to determine whether the events are triaged and resolved by authorized personnel as applicable.	No exceptions noted.
		SM-03-01	Adobe defines availability monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected availability monitoring tool and system configurations for a selection of services to determine whether availability monitoring rules are defined and implemented to flag events and notify authorized personnel.	No exceptions noted.
		SM-03-02	Critical systems are monitored in accordance with predefined availability criteria, and alerts are sent to authorized personnel.	Inspected availability incident tickets for a selection of alerts generated to determine whether the alerts are triaged and resolved by authorized personnel.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	SM-02-01	Adobe defines security monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected security monitoring tool configuration for a selection of alert rules to determine whether security monitoring rules are defined and implemented to flag events and notify authorized personnel.	No exceptions noted.
				Inspected the Splunk QCR access review for a selection of quarters to determine whether users that can add, modify, and delete alerts are limited to authorized personnel.	No exceptions noted.
		SM-02-02	Critical systems are monitored in accordance with predefined security criteria, and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	Inspected the security monitoring tool for a selection of production accounts to determine whether critical information system activity is monitored.	No exceptions noted.
				Inspected alert resolution for a selection of security events to determine whether the events are triaged and resolved by authorized personnel as applicable.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	IR-01-01	Adobe defines the types of incidents that need to be managed, tracked, and reported, including: • Procedures for the identification and management of incidents. • Procedures for the resolution of confirmed incidents. • Key incident response systems. • Incident coordination and communication strategy. • Contact method for internal parties to report incidents. • Support team contact information. • Notification to relevant management in the event of a security breach. • Provisions for updating and communicating the plan. • Provisions for training of support team. • Preservation of incident information.	Inspected Adobe's Incident Response Plan and Computer Security Incident Response Standard to determine whether Adobe defined the types of incidents that needed to be managed, tracked, and reported, including: • Procedures for the identification and management of incidents. • Procedures for the resolution of confirmed incidents. • Key incident response systems. • Incident coordination and communication strategy. • Contact method for internal parties to report incidents. • Support team contact information. • Notification to relevant management in the event of a security breach. • Provisions for updating and communicating the plan. • Provisions for training of support team. • Preservation of incident information.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
			• Management review and approval annual or when major changes to organization occur.	• Management review and approval annual or when major changes to organization occur.	
		IR-01-02	Confirmed incidents are assigned a priority level and managed to resolution. If applicable, Adobe coordinates the incident response with business contingency activities.	Inspected incident tickets for a selection of confirmed incidents to determine whether the incidents are tracked to resolution and, if necessary, incidents involved business contingency activities.	No exceptions noted.
		IR-02-01	Adobe defines and updates external communication requirements for incidents, including: • Information about external party dependencies. • Criteria for notification to external parties as required by Adobe policy in the event of a security breach. • Contact information for authorities (e.g., law enforcement, regulatory bodies, etc.).	Inspected the Incident Legal Communications Requirements Standard to determine whether the following is defined: • Information about external party dependencies. • Criteria for notification to external parties as required by Adobe policy in the event of a security breach. • Contact information for authorities (e.g., law enforcement, regulatory bodies, etc.).	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	BC-01-01	Adobe's business contingency plan is periodically reviewed, approved by management, and communicated to relevant team members.	Inspected Adobe's Business Continuity Plan to determine whether Adobe has established recovery steps and phases, and recovery capabilities, and identified personnel responsible to execute recovery procedures, and that the plan is periodically reviewed and approved.	No exceptions noted.
				Inspected Adobe's corporate intranet and email communication to determine whether Adobe's Business Continuity Plan is communicated to relevant team members.	No exceptions noted.
		BC-01-02	Adobe performs business contingency and disaster recovery tests on a periodic basis and ensures the following: • Tests are executed with relevant contingency teams. • Test results are documented. • Corrective actions are taken for exceptions noted. • Plans are updated based on results.	Inspected the business contingency and disaster recovery test results for a selection of services to determine whether: • Tests are executed with relevant contingency teams. • Test results are documented. • Corrective actions are taken for exceptions noted. • Plans are updated based on results.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		BC-01-03	Adobe identifies the business impact of relevant threats to assets, infrastructure, and resources that support critical business functions. Recovery objectives are established for critical business functions.	Inspected the Business Impact Analysis for a selection of services to determine whether the threats to assets, infrastructure, and resources are identified and the recovery objectives are established.	No exceptions noted.
		BM-01-01	Adobe configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	Inspected the data replication and/or data backup configuration for a selection of services to determine whether Adobe configured redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	No exceptions noted.
		BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Inspected business contingency and disaster recovery test results for a selection of services to determine whether Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
		IR-01-01	Adobe defines the types of incidents that need to be managed, tracked, and reported, including: • Procedures for the identification and management of incidents. • Procedures for the resolution of confirmed incidents. • Key incident response systems. • Incident coordination and communication strategy. • Contact method for internal parties to report incidents. • Support team contact information. • Notification to relevant management in the event of a security breach. • Provisions for updating and communicating the plan. • Provisions for training of support team. • Preservation of incident information.	Inspected Adobe's Incident Response Plan and Computer Security Incident Response Standard to determine whether Adobe defined the types of incidents that needed to be managed, tracked, and reported, including: • Procedures for the identification and management of incidents. • Procedures for the resolution of confirmed incidents. • Key incident response systems. • Incident coordination and communication strategy. • Contact method for internal parties to report incidents. • Support team contact information. • Notification to relevant management in the event of a security breach. • Provisions for updating and communicating the plan. • Provisions for training of support team. • Preservation of incident information.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to System Operations					
			• Management review and approval annual or when major changes to organization occur.	• Management review and approval annual or when major changes to organization occur.	

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CFM-01-01	Adobe ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	Inspected Adobe's standards and baseline images to determine whether security hardening and baseline configuration requirements have been established, reviewed, and updated periodically.	No exceptions noted.
		CHM-01-01	Change scope, change type, and roles and responsibilities are preestablished and documented in a change control workflow; notification and approval requirements are also preestablished based on risk associated with change scope and type.	Inspected Adobe's Change Management Standard to determine whether the change scope, change type, and roles and responsibilities are preestablished.	No exceptions noted.
				Inspected the change management ticketing and tracking tools to determine whether the change control workflow defines the notification and approval requirements.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Change Management					
		CHM-01-02	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: • Change description • Impact of change • Test results • Backout plan	Inspected change tickets for a selection of changes to in-scope systems to determine whether approval from appropriate personnel is obtained prior to the implementation of the change, and the following are documented and performed: • Change description • Impact of the change • Testing was required and performed • Backout plan	No exceptions noted.
		SLC-01-01	Major software releases are subject to the SLC, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	Inspected SLC tickets for a selection of major releases to determine whether it required an acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	No exceptions noted.
		SLC-02-01	Source code is managed with Adobe-approved version control mechanisms.	Inspected the source code repository tools for a selection of services to determine whether Adobe-approved version control mechanisms/systems are utilized.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Mitigation					
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	BM-01-01	Adobe configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	Inspected the data replication and/or data backup configuration for a selection of services to determine whether Adobe configured redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	No exceptions noted.
		BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Inspected business contingency and disaster recovery test results for a selection of services to determine whether Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	No exceptions noted.
		EM-02-03	Adobe purchases cybersecurity insurance to mitigate risk of material financial impact that could result from a cybersecurity event.	Inspected the insurance policy to determine whether Adobe purchased insurance to mitigate risk of material financial impact that could result from a cybersecurity event.	No exceptions noted.

Common Criteria Related to Security, Availability, and Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
Common Criteria Related to Risk Mitigation					
		RM-02-01	Adobe management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	Inspected the Security Risk Register, Security Risk Summary report, and a quarterly Risk Steering Committee calendar invite and inquired of management to determine whether management performed an annual risk assessment and identified risks had an overall residual risk ranking that was reviewed and approved.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	TPM-01-01	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address the impact the disclosed gaps have on the organization.	Inspected the VSR documentation for a selection of third parties to determine whether management obtained the third-party assurance reports, reviewed the controls and results, and took action on control gaps, as applicable.	No exceptions noted.
		TPM-02-02	Agency temporary workers, independent contractors, and third-party entities consent to a non-disclosure clause.	Inspected the signed agreements for a selection of agency temporary workers, independent contractors, and third-party entities to determine whether they contained a non-disclosure clause.	No exceptions noted.

Additional Criteria Related to Availability

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	BC-02-01	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections, purchases are made against the established budget, and plans are updated on a quarterly basis.	Inspected infrastructure budgets to determine whether the budgets are established based on historical business activity and future growth projections, and plans were updated on a quarterly basis.	No exceptions noted.
		SM-03-01	Adobe defines availability monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	Inspected availability monitoring tool and system configurations for a selection of services to determine whether availability monitoring rules are defined and implemented to flag events and notify authorized personnel.	No exceptions noted.
		SM-03-02	Critical systems are monitored in accordance with predefined availability criteria, and alerts are sent to authorized personnel.	Inspected availability incident tickets for a selection of alerts generated to determine whether the alerts are triaged and resolved by authorized personnel.	No exceptions noted.
A1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	AM-03-01	Equipment maintenance is documented and approved according to management requirements.	Inspected Jira tickets for a selection of equipment maintenances to determine whether equipment maintenance is documented and approved.	No exceptions noted.

Additional Criteria Related to Availability

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		BM-01-01	Adobe configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	Inspected the data replication and/or data backup configuration for a selection of services to determine whether Adobe configured redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	No exceptions noted.
		BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Inspected business contingency and disaster recovery test results for a selection of services to determine whether Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	No exceptions noted.
		SM-03-02	Critical systems are monitored in accordance with predefined availability criteria, and alerts are sent to authorized personnel.	Inspected availability incident tickets for a selection of alerts generated to determine whether the alerts are triaged and resolved by authorized personnel.	No exceptions noted.

Additional Criteria Related to Availability

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		SO-03-01	Temperature and humidity levels of data center environments are monitored and maintained at appropriate levels.	Inspected the temperature and humidity monitoring system and configurations at the Adobe-owned data center to determine whether temperature and humidity levels are monitored and configured to alert appropriate personnel when temperature or humidity levels exceed set limits.	No exceptions noted.
				Inspected the temperature and humidity alarms generated over the threshold and determined that there were no instances of alarms being triggered during the examination period.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this control could not be tested.
		SO-03-02	Emergency responders are automatically contacted when fire detection systems are activated; the design and function of fire detection and suppression systems are maintained at appropriate intervals.	Observed the fire detection/suppression systems in use at the Adobe-owned data center to determine whether they are in place.	No exceptions noted.
				Inspected the fire detection system monitoring contract in place to determine whether Adobe has contracted with a third party to monitor fire detection systems for the Adobe-owned data center.	No exceptions noted.

Additional Criteria Related to Availability

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
				Inspected fire suppression/detection certifications at the Adobe-owned data center to determine whether the design and function of these systems are tested at appropriate intervals.	No exceptions noted.
		SO-03-03	Adobe employs UPSs and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	Observed the UPS and generators at a selection of Adobe-owned data center and data rooms to determine whether they are employed to support critical systems in the event of a power disruption or failure.	No exceptions noted.
				Inspected UPS and generator certifications for in-scope Adobe-owned data center and data rooms to determine whether the equipment is certified at appropriate intervals.	No exceptions noted.
				Inquired of management and determined that there were no instances of power disruption or failure that caused the UPS and generators to be initiated.	The circumstances that warrant the operation of this control did not occur during the examination period and, as a result, this control could not be tested.

Additional Criteria Related to Availability

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	BC-01-02	Adobe performs business contingency and disaster recovery tests on a periodic basis and ensures the following: • Tests are executed with relevant contingency teams. • Test results are documented. • Corrective actions are taken for exceptions noted. • Plans are updated based on results.	Inspected the business contingency and disaster recovery test results for a selection of services to determine whether: • Tests are executed with relevant contingency teams. • Test results are documented. • Corrective actions are taken for exceptions noted. • Plans are updated based on results.	No exceptions noted.
		BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Inspected business contingency and disaster recovery test results for a selection of services to determine whether Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	No exceptions noted.

Additional Criteria Related to Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	BM-01-01	Adobe configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	Inspected the data replication and/or data backup configuration for a selection of services to determine whether Adobe configured redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	No exceptions noted.
		BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	Inspected business contingency and disaster recovery test results for a selection of services to determine whether Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	No exceptions noted.
		DM-01-01	Adobe's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	Inspected Adobe's Data Classification and Handling Standard to determine whether Adobe's data classification criteria are periodically reviewed, approved by management, communicated to authorized personnel, and used to determine the treatment of data.	No exceptions noted.

Additional Criteria Related to Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
				Inspected the data classification tickets for a selection of services to determine whether Adobe reviewed and confirmed the data classification associated for the service.	No exceptions noted.
		DM-06-02	Adobe purges data according to customer requests.	Observed a customer account in a test environment to determine whether customers can delete their own data via an API.	No exceptions noted.
				Inspected the customer request tickets for a selection of requests related to data deletion to determine whether Adobe purges data according to customer requests.	No exceptions noted.
		PRIV-03-04	In accordance with Adobe policy, Adobe provides notice to individuals regarding legally required disclosures of personal information.	Inspected Adobe's public-facing website to determine whether Adobe provides notice to individuals regarding legally required disclosures related to personal information.	No exceptions noted.
		TPM-02-02	Agency temporary workers, independent contractors, and third-party entities consent to a non-disclosure clause.	Inspected the signed agreements for a selection of agency temporary workers, independent contractors, and third-party entities to determine whether they contained a non-disclosure clause.	No exceptions noted.

Additional Criteria Related to Confidentiality

Criteria	Trust Services Criteria	Control Number	Controls Specified by Adobe Incorporated	Tests of Controls Performed by BDO USA, P.C.	Results of Tests
		TPM-04-01	Adobe has documented a Vendor Information Security Standard that defines the responsibilities and governance requirements regarding vendor information security engagements. Contractual agreements are entered into with vendors that process or store Adobe data that define information security terms and SLAs.	Inspected Adobe's Vendor Information Security Standard to determine whether responsibilities and governance requirements regarding vendor information security engagements are defined.	No exceptions noted.
				Inspected the contract for a selection of third parties that process or store Adobe data to determine whether information security terms and SLAs are defined.	No exceptions noted.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	DM-06-01	Media that are flagged for disposal are sent to a third party for destruction. Adobe obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.	Inspected media decommissioning tickets and/or third-party destruction certificate for a selection of decommissioned media to determine whether the media was securely erased by a third party or was maintained in a secure facility pending erasure.	No exceptions noted.
		DM-06-02	Adobe purges data according to customer requests.	Observed a customer account in a test environment to determine whether customers can delete their own data via an API.	No exceptions noted.
				Inspected the customer request tickets for a selection of requests related to data deletion to determine whether Adobe purges data according to customer requests.	No exceptions noted.

V. Other Information Provided by Adobe Incorporated That Is Not Covered by the Independent Service Auditor's Report on a SOC 2 Examination

Other Information Provided by Adobe Incorporated That Is Not Covered by the Independent Service Auditor's Report on a SOC 2 Examination

Adobe Controls Included in the Scope of the Report that Map to NIST Cybersecurity Framework, AUS CPS 234, BSI C5, HKMA-TechRM, MAS, and HITRUST CSF Security

The table below demonstrates alignment between the controls described in this report and the National Institute of Standards and Technology Cybersecurity Framework (NIST Cybersecurity Framework), Australian Prudential Regulation Authority's Prudential Standard CPS 234 Information Security (AUS CPS 234), Germany's Federal Office for Information Security - Cloud Computing Compliance Controls Catalogue (BSI C5), the Hong Kong Monetary Authority Technology Risk Management (HKMA-TechRM) frameworks, the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines (TRM), and the HITRUST CSF Security Certification Criteria (HITRUST CSF Security).

Additionally, some of the NIST Cybersecurity, AUS CPS 234, BSI C5, HKMA-TechRM, MAS TRM, and HITRUST CSF Security requirements are not in scope for the Adobe Document Cloud and are not represented in this table. This information is provided by Adobe to assist readers in understanding the relationship between the Adobe controls and the NIST Cybersecurity, AUS CPS 234, BSI C5, HKMA-TechRM, MAS TRM, and HITRUST CSF Security requirements.

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
AM-01-01	Adobe maintains an inventory of system devices, which is reconciled on a periodic basis.	ID.AM-1 ID.AM-2		AM-01 AM-06	5.3.1	3.3	07.A
AM-01-02	Adobe assets are labeled and have designated owners.			AM-01 AM-03 AM-06	3.1.1	3.3	07.A
AM-02-01	Adobe authorizes and records the entry and exit of systems at data center locations.	ID.AM-4 PR.DS-3					09.o
AM-03-01	Equipment maintenance is documented and approved according to management requirements.	PR.DS-8 PR.MA-1		PS-06		7.3	08.j

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
BC-01-01	Adobe's business contingency plan is periodically reviewed, approved by management, and communicated to relevant team members.	RC.IM-2		BCM-01 BCM-02 BCM-03 BCM-04	5.4.1 7.1.1	8.2	12.c 12.d
BC-01-02	Adobe performs business contingency and disaster recovery tests on a periodic basis and ensures the following: • Tests are executed with relevant contingency teams. • Test results are documented. • Corrective actions are taken for exceptions noted. • Plans are updated based on results.	ID.SC-5 PR.IP-9 PR.IP-10 PR.PT-5 RC.IM-2		BCM-03 BCM-04 OPS-08 PS-02	5.4.1 7.1.1	8.2 8.3	12.c 12.d
BC-01-03	Adobe identifies the business impact of relevant threats to assets, infrastructure, and resources that support critical business functions. Recovery objectives are established for critical business functions.	ID.BE-5 PR.IP-9		BCM-02 BCM-03 BCM-04 OPS-06 OPS-08	5.4.1	8.2	12.b
BC-02-01	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections, purchases are made against the established budget, and plans are updated on a quarterly basis.		15	BCM-01 OPS-01	5.2.1 5.2.2	8.1	12.b

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
BM-01-01	Adobe configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.	PR.IP-4		OPS-06 OPS-07 OPS-09 PS-02	5.1.2	8.1 8.4	09.l 12.c
BM-01-02	Adobe performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.	PR.IP-4		OPS-06 OPS-08 OPS-09 PS-02		8.4	09.l 12.c
CFM-01-01	Adobe ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated periodically.	PR.IP-1 PR.PT-3 DE.AE-1		AM-03 COS-03 OPS-04 OPS-05 OPS-18 OPS-23	3.4.1 6.1.1	7.2 11.3 12.2	10.a
CFM-01-02	Adobe uses mechanisms to detect deviations from baseline configurations on production environments.			AM-03 COS-03 OIS-04 OPS-04 OPS-05 OPS-18 OPS-23	3.4.1	7.2 11.3 12.2	01.l
CHM-01-01	Change scope, change type, and roles and responsibilities are preestablished and documented in a change control workflow; notification and approval requirements are also preestablished based on risk associated with change scope and type.	PR.IP-3		DEV-01 DEV-03 DEV-05 DEV-07	3.4.1 4.3.1	5.4 7.5	09.b 09.k 10.k

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
CHM-01-02	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: • Change description • Impact of change • Test results • Backout plan			AM-03 DEV-05 DEV-06 DEV-07 DEV-09 OIS-04 PSS-02 PSS-09	4.2.4 4.3.1	5.5 5.7 5.8 6.3 7.4 7.5	03.d 09.b 09.k 10.a 10.k
CHM-02-01	Changes to the production environment are implemented by authorized personnel.	PR.AC-4		DEV-07 OIS-04	3.3.2 4.3.1	6.3 7.6	09.c
CRY-02-01	Adobe restricted data that is transmitted over public networks is encrypted.	PR.DS-2 PR.DS-5		COS-08 CRY-01 CRY-02 OPS-14 OPS-24 PI-01		11.1	06.d 09.s 09.v 09.x
CRY-02-02	Adobe restricted data at rest is encrypted.	PR.DS-1 PR.DS-5		COS-08 CRY-01 CRY-03 IDM-08 OPS-14 OPS-24 PSS-07		8.4 11.1	06.d
CRY-03-01	Access to the cryptographic keystores is limited to authorized personnel.			CRY-01 CRY-03 CRY-04	3.1.4	9.2 10.2	01.c 10.f

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
DM-01-01	Adobe's data classification criteria are periodically reviewed, approved by management, and communicated to authorized personnel; the data security management team determines the treatment of data according to its designated data classification level.	ID.AM-5	20	AM-06 CRY-01	3.1.1 3.1.2	3.3 11.1	06.c 09.q 09.s
DM-06-01	Media that are flagged for disposal are sent to a third party for destruction. Adobe obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.	PR.IP-6		AM-01 AM-04	3.1.3	11.1	08.l 09.p
DM-06-02	Adobe purges data according to customer requests.			PI-03		11.1	06.c 08.l 09.p
EM-01-01	The Board of Directors provides corporate oversight, strategic direction, and review of management for Adobe. The Board of Directors is scheduled to meet at least quarterly and has three subcommittees: • Audit Committee • Executive Compensation Committee • Governance and Sustainability Committee		13			3.1	00.a 02.d

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
EM-01-02	The Audit Committee is governed by a charter, is independent from Adobe management, is composed of outside directors, and is scheduled to meet at least quarterly. The Audit Committee oversees: • Financial statement quality • Enterprise risk management • Regulatory and legal compliance • Internal audit functions • Information security functions • External audit functions					3.1	00.a 05.a
EM-02-03	Adobe purchases cybersecurity insurance to mitigate risk of material financial impact that could result from a cybersecurity event.					4.4	
EM-04-02	Information security compliance results are reported to the Audit Committee by the CSO on a quarterly basis and support information security compliance certifications.					3.1 4.5 15.1	00.a 03.d 06.g
EM-06-01	When customers sign up to Adobe's product and services, the customer is required to acknowledge a service agreement that includes considerations for protecting security, availability, and confidentiality and indicates the responsibilities of the user's and Adobe's responsibilities and commitments.			COM-01 OIS-02 OIS-03 PI-02			

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
IAM-01-01	Logical access provisioning to information systems requires approval from appropriate personnel.	PR.AC-1		DEV-07 IDM-01 IDM-02 IDM-06 OIS-04 OPS-16	3.2.3 3.3.1	9.1 11.4	01.b 01.c 01.v 05.j
IAM-01-02	Logical access is revoked timely.	PR.AC-1		IDM-01 IDM-02 IDM-03 IDM-04 OIS-04	3.3.1	9.1	01.b 02.i
IAM-01-03	Adobe performs account and access reviews on a quarterly basis; corrective action is taken where applicable.			IDM-01 IDM-02 IDM-03 IDM-04 IDM-05 IDM-06 OIS-04 OIS-07	3.3.1	9.1	01.b 01.c 01.e
IAM-01-04	Adobe restricts the use of shared and group authentication credentials. Authentication credentials for shared and group accounts are reset every 90 days.			CRY-01			
IAM-02-01	Adobe requires unique identifiers for user accounts and prevents identifier reuse.			IDM-01	3.2.1	9.1	01.b 01.q

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
IAM-02-02	User and device authentication to privileged information systems is protected by passwords that meet Adobe's password complexity requirements.			COS-05 IDM-01 IDM-08 IDM-09	3.2.1	9.1 9.3	01.d 01.q
IAM-02-03	MFA is required for: • Remote VPN sessions. • Access to trusted data environments	PR.AC-7		COS-05 IDM-01 IDM-08 IDM-09 OPS-14 OPS-16	3.2.2 3.4.1	9.1 9.3	01.d 01.q
IAM-02-10	Adobe users are authenticated against a Zero Trust model prior to gaining access to Adobe resources.			IDM-01 IDM-09			
IAM-04-01	Remote connections to the corporate network are accessed via VPN through managed gateways.			COS-02 COS-04 COS-05 COS-08 IDM-09 OPS-14		9.3	01.j 09.v 09.x

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
IR-01-01	Adobe defines the types of incidents that need to be managed, tracked, and reported, including: • Procedures for the identification and management of incidents. • Procedures for the resolution of confirmed incidents. • Key incident response systems. • Incident coordination and communication strategy. • Contact method for internal parties to report incidents. • Support team contact information. • Notification to relevant management in the event of a security breach. • Provisions for updating and communicating the plan. • Provisions for training of support team. • Preservation of incident information. • Management review and approval, annual or when major changes to organization occur.	ID.RA-4 PR.IP-9 RS.RP-1 RS.CO-1 RS.CO-2 RS.CO-3 RS.AN-2 RS.AN-4 RS.IM-1 RS.MI-1 RC.IM-1 RC.RP-1	23 24 25	COS-01 SIM-01 SIM-05	3.3.1 3.3.3	7.7 7.8 12.3	11.a 11.c 11.d

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
IR-01-02	Confirmed incidents are assigned a priority level and managed to resolution. If applicable, Adobe coordinates the incident response with business contingency activities.	DE.DP-3 DE.DP-5: RC.CO-3 RS.CO-4 RS.MI-2 RS.IM-2		COS-01 OPS-20 SIM-01 SIM-02 SIM-03 SIM-05		7.7 12.3	11.c
IR-02-01	Adobe defines and updates external communication requirements for incidents, including: • Information about external party dependencies. • Criteria for notification to external parties as required by Adobe policy in the event of a security breach. • Contact information for authorities (e.g., law enforcement, regulatory bodies, etc.).	RC.CO-2	35 36	OIS-03 OPS-21 SIM-05		12.1 12.3	11.a
IR-02-02	Adobe provides a contact method for external parties to: • Submit complaints and inquiries • Report incidents			OIS-05 SIM-04		7.7	11.a
IR-02-03	Adobe communicates a response to external stakeholders as required by the Incident Response Plan.	RS.CO-5		OPS-21 SIM-03		7.7 12.3	

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
NO-01-01	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance with identified security requirements and business justifications.	PR-PT-4		COS-01 COS-02 COS-03 COS-04 COS-05 COS-06 COS-08 OPS-24	6.1.2 6.1.4 6.2.1	11.2	01.n 01.o 09.m 09.n
NO-02-01	Production environments are logically segregated from non-production environments.	PR.AC-5 PR.DS-7		COS-05 DEV-10	6.2.2	5.7 5.8 11.2	01.m 01.w 09.m 09.n
PR-01-01	New hires are required to pass a background check as a condition of their employment.	PR.AC-6 PR.IP-11		HR-01	3.6.3	3.5	
PR-03-01	Employees that fail to comply with Adobe policies are subject to a disciplinary process.			HR-04			02.f 06.e
PRIV-03-04	In accordance with Adobe policy, Adobe provides notice to individuals regarding legally required disclosures of personal information.			IDM-07			06.d
PS-01-01	EDR software is deployed to continuously monitor, detect, and respond to cyber threats and patterns of malicious behavior and activity			OPS-04 OPS-05	3.5.3	11.3	

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
RM-01-01	A Security Risk Management Framework is documented which defines the security risk management methodology.	ID.GV-4 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3		COM-03 OIS-04 OIS-06		3.1 4.1 4.2 4.3	03.b 03.c 03.d 12.b
RM-01-02	A comprehensive security risk register is maintained that includes risks both internal and external to Adobe.	ID.GV-4 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3		COM-03 OIS-04 OIS-06 OIS-07 SSO-05		3.1 4.1 4.2 4.3	03.b 03.c 03.d 12.b
RM-02-01	Adobe management performs an annual risk assessment. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.	ID.GV-4 ID.RA-6 ID.RM-1 ID.RM-2 ID.RM-3		COM-03 OIS-04 OIS-06 OIS-07 OPS-20 SSO-05		3.1 4.1 4.2 4.3	03.b 03.c 03.d 12.b
RM-02-02	The design and operating effectiveness of internal controls are continuously evaluated against the established CCF by Adobe. Corrective actions related to identified deficiencies are tracked to resolution.		21 27 30 31 32 33 34	COM-02 COM-03	4.2.3	3.2 4.1 15.1	03.b 03.c 03.d 06.g 06.h
SDD-01-01	Documentation of system boundaries and key aspects of their functionality are published to authorized Adobe personnel on the Adobe intranet.			COS-07 COS-08 PI-01		5.6	

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
SDD-02-01	Adobe publishes whitepapers to its public website that describe the purpose, design, and boundaries of the system and system components.			COS-07 COS-08 OIS-03 PI-01 PSS-01			
SG-01-01	Adobe's policies and standards are periodically reviewed, approved by management, and communicated to Adobe personnel.	ID.AM-6 ID:GV-1	18	AM-02 COM-01 COM-02 COM-03 COS-08 CRY-01 DEV-01 DEV-03 IDM-01 OIS-02 OIS-06 OPS-04 OPS-06 OPS-10 OPS-11 OPS-18 SP-01 SP-02	6.3.1 7.1.1	3.1 3.2 4.4 5.1 5.4 7.1	01.h 01.x 01.y 02.d 04.a 04.b 06.e 07.c 10.a 10.f
SG-01-02	Adobe reviews exceptions to policies and standards; exceptions are documented and approved based on business need and removed when no longer required.			SP-03		3.2	04.b

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
SG-02-01	The CSO conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.	ID.AM-3 PR.IP-8		HR-03 OIS-05 SIM-04 SP-01			04.a 05.a
SG-04-01	Adobe has an established security leadership team including key stakeholders in the Adobe Information Security Program; goals and milestones for deployment of the Information Security Program are established and communicated to the Company through the quarterly security all-hands meeting.	ID.BE-2 ID.BE-3		AM-02 BCM-01 COM-01 COM-04 HR-03 OIS-01 OIS-02 OIS-06 SP-01		3.1	05.a
SG-04-03	Roles and responsibilities for the governance of information security within Adobe are formally documented within the Information Security Management Standard and communicated on the Adobe intranet.	ID.AM-6 ID.BE-2 ID.BE-3 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1	14 19	BCM-01 COM-01 COM-04 HR-03 OIS-01 OIS-02 OIS-06		3.1 4.1	04.a 05.a 11.c
SLC-01-01	Major software releases are subject to the SLC, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.	PR.IP-2		DEV-01	4.1.1 4.2.1 4.2.2 4.2.4	5.1 5.2 5.4 5.7	10.h

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
SLC-02-01	Source code is managed with Adobe-approved version control mechanisms.			DEV-08		5.7 6.3 7.6	
SM-01-01	Adobe logs critical information system activity.	DE.AE-3		DEV-07 OIS-04 OPS-10 OPS-11 OPS-17	6.2.3	9.2 12.2	09.ad
SM-02-01	Adobe defines security monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	DE.AE-5 DE.CM-2		COS-01 IDM-06 OPS-10 OPS-13 OPS-17	3.4.1 7.1.1	6.4 7.7 12.2	09.ab
SM-02-02	Critical systems are monitored in accordance with predefined security criteria, and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	DE.CM-1 DE.CM-7 DE.DP-2 RS.AN-1		COS-01 COS-03 OPS-10 OPS-13 PSS-04 SIM-05 SSO-04	5.2.1 6.1.5	7.7	09.ab
SM-03-01	Adobe defines availability monitoring alert criteria and how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	DE.AE-5 PR.DS-4		OPS-01 OPS-02 OPS-09 OPS-17 PS-02	5.2.1	8.1	

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
SM-03-02	Critical systems are monitored in accordance with predefined availability criteria, and alerts are sent to authorized personnel.	DE.CM-1 DE.DP-2		OPS-01 OPS-02 OPS-09 OPS-17 PS-06 SSO-04		8.1	
SO-01-01	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	PR.AC-2 PR.IP-5		PS-01 PS-03 PS-04 PS-05 PS-06	3.6.1	8.5	09.ab
SO-02-01	Physical access provisioning to an Adobe data center or data room requires management approval and documented specification of: • Account type (e.g., visitor, vendor, or regular) • Access privileges granted • Intended business purpose • Visitor identification method, if applicable • Temporary badge issued, if applicable • Access start date • Access duration			PS-04	3.6.1 3.6.3	8.5	08.b
SO-02-02	Physical access that is no longer required in the event of a termination or role change is revoked. If applicable, temporary badges are returned prior to exiting the facility.			PS-04		8.5	08.b

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
SO-02-03	Adobe performs physical account and access reviews on a quarterly basis; corrective action is taken where applicable.			PS-04		8.5	08.b
SO-02-05	Intrusion detection and video surveillance are installed at Adobe data center locations; confirmed incidents are documented and tracked to resolution.			PS-01 PS-03 PS-04		8.5	08.b
SO-03-01	Temperature and humidity levels of data center environments are monitored and maintained at appropriate levels.			PS-05 PS-06 PS-07	3.6.2	8.5	08.d
SO-03-02	Emergency responders are automatically contacted when fire detection systems are activated; the design and function of fire detection and suppression systems are maintained at appropriate intervals.			PS-05 PS-07	3.6.2	8.5	08.d
SO-03-03	Adobe employs UPSs and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.	ID.BE-4		PS-01 PS-06 PS-07	3.6.2 5.3.1	8.5	08.d
TA-01-01	Adobe personnel complete security awareness training, which includes annual updates about relevant policies and how to report security events to the authorized response team. Records of training completion are documented and retained for tracking purposes.	PR.AT-1		AM-05 DEV-04 HR-02 HR-03 SIM-04 SP-01		3.6	11.a

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
TA-01-02	Biannually, Adobe full-time and temporary employees and interns complete a Code of Business Conduct training.			AM-05 HR-02 HR-04			
TPM-01-01	On a periodic basis, management reviews controls within third-party assurance reports to ensure that they meet organizational requirements; if control gaps are identified in the assurance reports, management takes action to address the impact the disclosed gaps have on the organization.	ID.SC-1 ID.SC-3 ID.SC-4.	16 22 28 34	OIS-03 OIS-07 PS-01 PS-03 SSO-01 SSO-02 SSO-03 SSO-04 SSO-05	7.2.1	3.4 6.4	05.i 09.e 09.f 10.l
TPM-02-02	Agency temporary workers, independent contractors, and third-party entities consent to a non-disclosure clause.	DE.CM-6		AM-05 HR-02 HR-05 SP-01			05.k
TPM-04-01	Adobe has documented a Vendor Information Security Standard that defines the responsibilities and governance requirements regarding vendor information security engagements. Contractual agreements are entered into with vendors that process or store Adobe data that define information security terms and SLAs.	ID.BE-1 ID.SC-3 PR.AT-3		AM-05 COM-01 HR-02 HR-06 OIS-02 OIS-03 SIM-04 SP-01 SSO-01 SSO-02		3.4	05.k 10.l

Adobe Control ID	Adobe Control Activity	NIST Cybersecurity Framework	AUS CPS 234	BSI C5	HKMA-TechRM	MAS TRM	HITRUST CSF Security
VM-01-01	Adobe conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	ID.RA-1 PR.IP-12 DE.CM-8	17	COS-03 OPS-18 OPS-20 OPS-22 PSS-02 PSS-03 PSS-09	6.1.5	11.3 13.1	06.h 09.j 10.m
VM-02-01	Adobe conducts penetration tests periodically.		17	OIS-05 OPS-18 OPS-19 OPS-20 PSS-02		13.2 13.3	06.h
VM-03-01	Adobe installs security-relevant patches, including software or firmware updates.			OPS-22	3.4.1	7.3 7.4 11.4	