



Adobe Cloud Services

Compliance Overview

Overview

At Adobe, the security, privacy and availability of our customers' data is our priority. We believe that a sound compliance and risk management strategy is as important to the success of an organization as the company's product strategy. To this end, our cloud strategy includes a two-pronged approach to keeping your data safer, more secure, and available.

To protect from the physical layer up, we implement a foundational framework of security processes and controls called the Common Controls Framework (CCF) by Adobe. CCF helps protect the Adobe infrastructure, applications and services, as well as helps us comply with a number of industry-accepted best practices, standards, regulations and certifications.

To protect from the software layer down, we use the Adobe Secure Product Lifecycle (SPLC), a rigorous set of several hundred specific security activities spanning software development practices, processes, and tools that are integrated into multiple stages of the product lifecycle.

Table of Contents

- 1 Overview
- 1 Which Standards Does Adobe Focus On?
- 2 Regulatory Compliance
- 3 Our Approach
- 5 Current State
- 6 Third-Party Compliance Audits
- 6 Conclusion

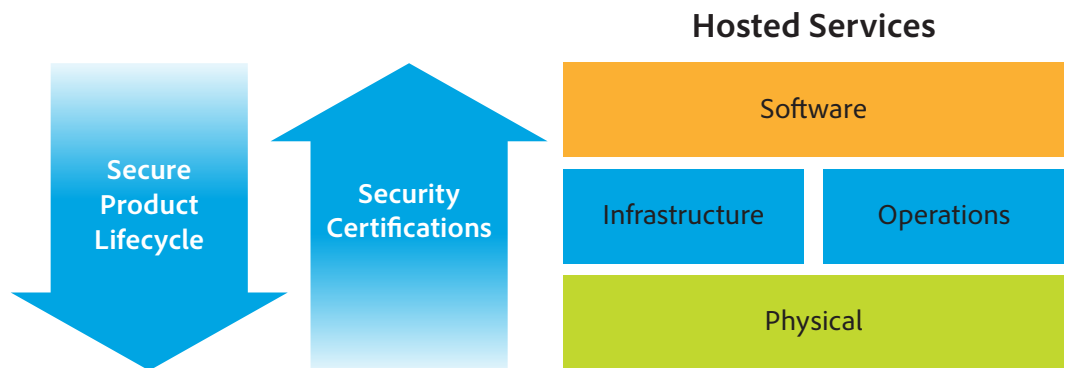


Figure 1: Adobe uses the Secure Product Lifecycle and Common Controls Framework to provide a complete view of compliance with industry standards and regulations.

Which Standards Does Adobe Focus On?

Adobe demonstrates our commitment to security by implementing a range of important industry standards and complying with government regulations concerning the security and privacy of data. While there are numerous industry standards and certifications comprising thousands of different requirements for compliance in the cloud, Adobe determined that significant overlap exists between these requirements and focuses on those that most significantly affect our customers. As new security standards and regulatory requirements are developed and adopted by the industry, Adobe will review them and adopt those with relevance to our customers. Depending on the focus of a particular Adobe service, it may comply with some or all of the following industry and regulatory standards.

Industry Standards

Adobe currently focuses on meeting the compliance requirements for the following primary industry standards.:

- **SOC**—The Service Organization Control (SOC) reporting standard has been established by the American Institute of Public Accountants (AICPA). Adobe currently utilizes the SOC 2 reporting standard. SOC 2 reports are based on a third-party attestation of compliance with AICPA Trust Service Principles (TSPs) relevant to security, availability, confidentiality, privacy, and processing integrity.

- **ISO 27001**—This certification demonstrates a systematic approach towards managing information security risks that affect the confidentiality, integrity, and availability of the service and customer information. ISO 27001 certification includes the establishment of a formal information security management program and demonstration of Adobe’s commitment to providing transparency into its security controls and practices. ISO 27001 is of particular importance outside the United States.
- **FedRAMP**—The Federal Risk and Authorization Management Program (FedRAMP) is a collection of standards established by the U.S. Federal Government for security assessment, authorization, and continuous monitoring for cloud solutions. FedRAMP is mandatory for certain federal agencies. FedRAMP certification determines which cloud solutions can be purchased and deployed by federal agencies and their contractors. FedRAMP requirements are derived from several of the NIST Special Publications including 800-53 system controls.
- **PCI DSS**—The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle payment card information, such as credit card numbers. PCI DSS certification increases controls around cardholder data management. Being a PCI DSS-compliant service provider enables Adobe to help customers meet PCI requirements for the safe handling of personally identifiable data associated with a cardholder.

Regulatory Compliance

Adobe develops technologies and services that help our customers comply with their regulatory obligations. Customers are ultimately responsible for ensuring that their Adobe service is configured and secured in a manner that complies with their legal obligations.

- **GLBA**—The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard their customers’ personal data. A “GLBA-Ready” Adobe service means that the service can be used in a way that enables the customer to help meet its GLBA Act obligations related to the use of service providers.
- **HIPAA**—The Health Insurance Portability and Accountability Act (HIPAA) is legislation that governs the use of electronic medical records, and includes provisions to protect the security and privacy of personally identifiable health-related data called protected health information (PHI). By law, healthcare providers and insurance companies that have any sensitive PHI can only use products that are HIPAA-compliant. Certain Adobe services can be configured to be used in a way that supports HIPAA compliance by a customer that is a “covered entity” under HIPAA and signs Adobe’s Business Associate Agreement (BAA).
- **21 CFR**—The Code of Federal Regulation, Title 21, Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11) establishes the U.S. Food and Drug Administration (FDA) regulations on electronic records and electronic signatures. Being 21 CFR Part 11 compliant means that Adobe services can be configured to be used in a way that allows pharmaceutical customers who engage with the FDA to comply with the 21 CFR Part 11 regulations.
- **FERPA**—The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a “school official” when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.
- **SAFE-BioPharma**—The SAFE-BioPharma standard describes requirements for standardized identity trust for either identity authentication or for digital signing. This certification helps companies provide global high-assurance identity trust for cyber-transactions that rely on service providers.
- **GDPR**—The General Data Protection Regulation (GDPR) is the European Union’s privacy law that harmonizes and modernizes data protection requirements. Adobe complies with industry-accepted standards, regulations and certifications, and has implemented technical and organizational measures (TOMs), as well as hundreds of security processes and controls ([click here for a](#)

[current list](#)). Adobe has updated our Data Processing Agreement to account for the GDPR requirements. Adobe has certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks for customer-related data. This provides our customers with the option of relying on these frameworks or entering into Standard Contractual Clauses (also known as EU Model Clauses) for the transfer of data from the EU to the U.S. You can find [more information on this in our Privacy Center](#), along with information on how to request Standard Contractual Clauses.

Our Approach: The Common Controls Framework by Adobe

The Common Controls Framework (CCF) by Adobe is a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. In creating CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,350 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

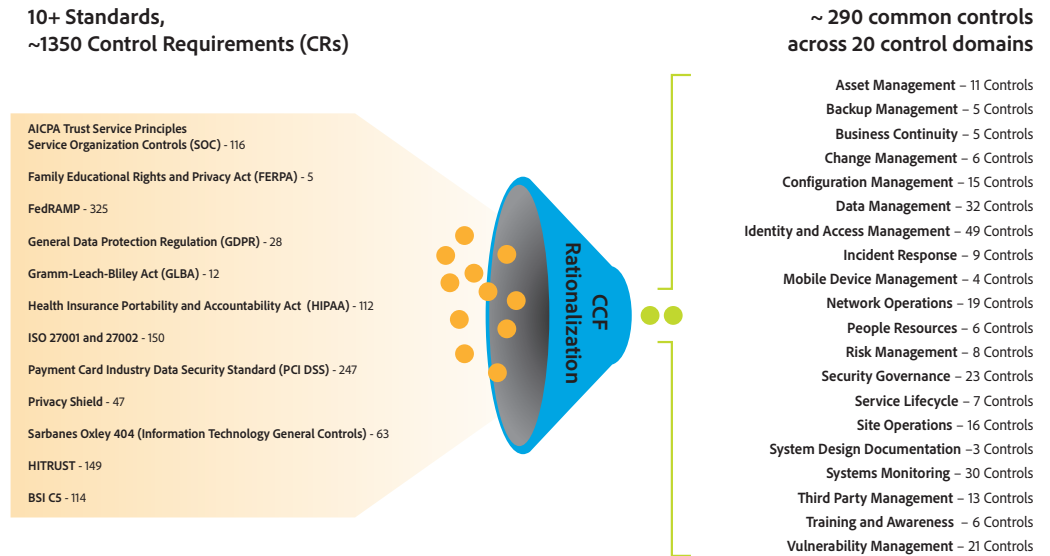


Figure 2: The Common Controls Framework by Adobe

Open Source CCF

As part of our ongoing efforts in knowledge sharing with the broader security community, Adobe has [released a generic version of Common Controls Framework by Adobe](#) through a Creative Commons license to help drive ongoing innovation around compliance in the security industry.

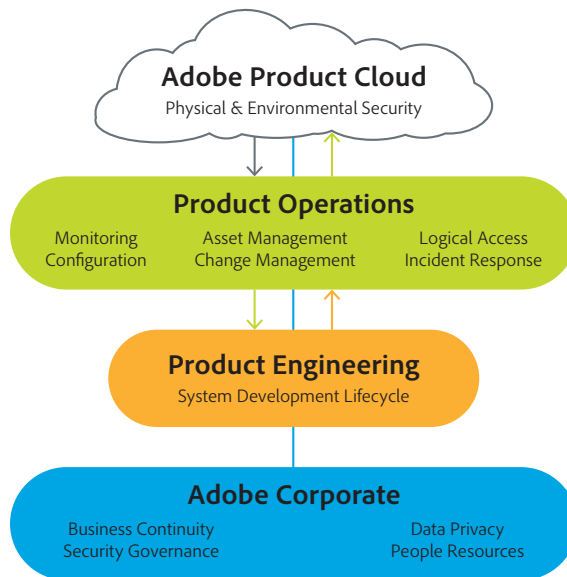


Figure 3: CCF by Adobe Conceptual Model

Realizing that a product-specific, “siloed” compliance approach is neither cost-effective nor efficient, Adobe built the CCF so that teams can inherit control capabilities from other parts of the organization. For example, software engineers are not responsible for data center security, however, they inherit the data center security capabilities from a data center operations team. This strategic simplicity enables the continuous execution of sustainable security controls.

The Adobe SPLC aligns cleanly with CCF as well as industry best practices for software engineering teams to meet compliance requirements. A robust framework, the Adobe SPLC was designed from the ground up to include many controls that are now covered by CCF. Some of these controls include security testing (e.g., static analysis, dynamic analysis, penetration testing, etc.) and annual training of software engineers in secure coding techniques. While the SPLC was already used across all Adobe software engineering teams, the creation of CCF and the need to adhere to compliance requirements now helps ensure that the SPLC is more consistently applied throughout Adobe, thanks to improved process documentation and specificity.

Compliance requirements also impact the Adobe IT/Ops organizations, helping to ensure that key functions within asset management, business continuity management, change management, configuration management, backup management, network operations, data management, identity and access management, and incident response are more rigorous and more consistently applied across the company. Some other areas also positively impacted by compliance requirements include data privacy controls for PII and PHI, logical access control for production and source code control systems, and the company’s network security policy.

All Adobe personnel must participate in annual security awareness training as part of the compliance process. In addition, Adobe offers additional specific security training relevant to each employee’s particular title and responsibilities. The compliance process also requires Adobe to formalize procedures throughout the company by documenting the procedure in advance, following the procedure to completion, and then providing evidence of the procedure’s completion. For example, provisioning user access to a production environment requires a ticketed approval process in which the user’s access to the environment must receive approval prior to provisioning. Adobe documents that procedure and the ticket is evidence of that documentation.

A Continuous Process

Adobe maintains ongoing compliance with periodic reviews. These reviews include assessments of access to production systems, vulnerabilities, and firewall rules. More than 100 teams within the company have been trained in how to conduct a quarterly compliance review, including what to review, the process for a full review, perform remediation activities as needed and how to preserve evidence of the review.

Adobe has established a comprehensive Quarterly Compliance Review (QCR) program to provide a governance model for the compliance program. This program enables automated metrics reporting and dashboarding, auditing, risk assessments, and issues and remediation tracking of compliance controls. In addition, Adobe implements a periodic control, process, and risk self-assessment program that allows corporate management to evaluate compliance risks and certify the operating effectiveness of compliance processes and controls.

The QCR program provides an effective mechanism for management and auditors to establish ownership and accountability over the compliance program and monitor its operating effectiveness on a continuous basis. Adobe's risk assessments are performed in alignment with requirements listed within NIST Special Publication 800-30 Revision 1.

The Adobe Common Controls Framework process doesn't end with the achievement of certifications and compliance with standards. Instead, the CCF is a continuous process that includes periodic internal audits, external assessments and on-going controls improvement. And because it is designed with flexibility in mind, the CCF allows us to quickly and easily adapt to new standards and changing requirements as well as international and regional requirements.

Current State of Adobe Compliance

To help ensure a consistent, company-wide strategy for all cloud offerings and platform services, Adobe has created a comprehensive compliance plan. With this plan, each team across the company documents the security and privacy controls it will implement, then the team implements the documented controls, and conducts regular, ongoing audits to prove compliance.

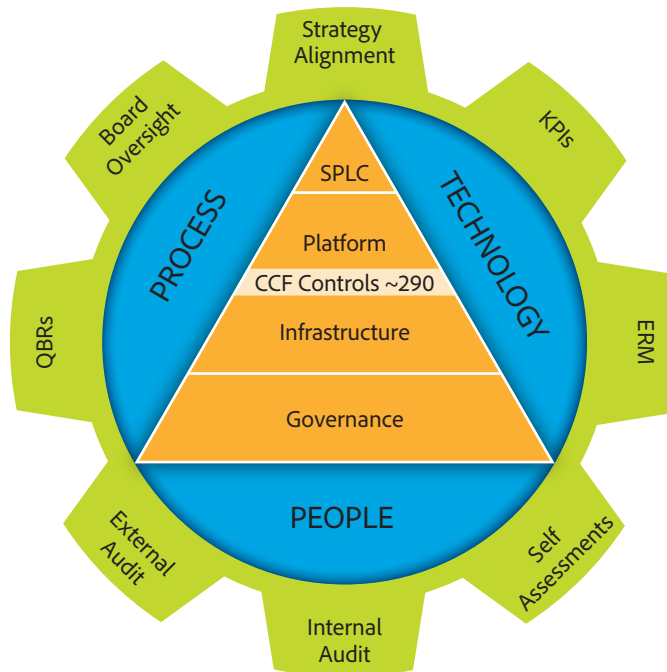


Figure 4: Adobe has created a comprehensive governance model to help ensure that security controls are operative, effective and monitored on an on-going basis.

In addition to the certifications and compliance achievements already in place, additional efforts are in process and at various phases, according to the overall CCF by Adobe implementation. The most current list of all certifications for Adobe products and services [can be found on adobe.com](http://adobe.com).

Third-Party Compliance Audits

SOC 2

A leading accounting firm issued the Service Origination Controls (SOC2) Type 2 report after reviewing the suitability of the design and operating effectiveness of controls over a period of 12 months for Adobe's enterprise clouds relevant to meet the criteria for the Security and Availability principles set forth in TSP section 100, Trust Services Principles, and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA Trust Services Principles and Criteria).

Auditors from the accounting firm conducted their examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Auditor's procedures included testing the operating effectiveness of the required controls to provide reasonable assurance that the application Security and Availability principles were met.

ISO/IEC 27001:2013

The accounting firm also issued ISO/IEC 27001:2013 Information Security Management Certificate of approval after reviewing that Adobe's Information Security Management System (ISMS) is in place in accordance with the requirements of ISO standard ISO/IEC 27001:2013 to appropriately preserve the Confidentiality, Integrity and Availability (CIA) of the platforms, services and applications that are used in processing, transmitting and storing customer assets and/or Personally Identifiable Information within Adobe's enterprise cloud offerings.

SOC 2 reports and ISO/IEC 27001:2013 certificates are available through your Adobe sales representative.

Conclusion

The Common Controls Framework by Adobe is a central part of our company-wide security strategy. With the people, processes and technology, as well as a range of oversight, audit and follow-up mechanisms in place, Adobe ensures that CCF is not just a point in time; it's an ongoing commitment to help protect our customers and their data.

Please visit the [Adobe Trust Center](http://adobe.com/trust-center) for more information about security efforts across our products and services.



Adobe

Adobe
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on Adobe solutions, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 10/2018 Adobe. All rights reserved. Printed in the USA.