Adobe Experience Manager Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience very seriously. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we regularly incorporate advanced security techniques into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to help bolster the security of your data and use of Adobe® Experience Manager.

About Adobe Experience Manager

Adobe Experience Manager is a powerful web content management system for building and managing complex, dynamic, multichannel digital experiences—easily and efficiently. With Adobe Experience Manager, you can manage projects, workflows, assets, integrations, and social communities; build adaptive complex forms; and create websites and mobile apps.

Built on the Java platform, it is powered by open source standards and state-of-the-art frameworks and technologies, including the Java Content Repository (JCR) API, and a solid and structured representational state transfer (REST) architecture.

Customers can either deploy Adobe Experience Manager on-premises using their own network infrastructure or Adobe can host their deployment as a managed service. For more information on the managed service option, see below.

Adobe Experience Manager Application Architecture

The Adobe Experience Manager solution includes the following five (5) capabilities:

Experience Manager Sites — Gives you one place to create, manage, and deliver digital experiences across websites, mobile sites, and on-site screens to make them global in reach, yet personally relevant and engaging.

Experience Manager Assets — Helps you create, manage, and deliver images, video, and other content to virtually any screen or device.

Experience Manager Mobile — Enables you to create and deliver mobile apps for consumers and devices and then integrate these mobile apps into your overall marketing strategy.

Experience Manager Forms — Allows you to make your forms, documents, and their processes paperless, more efficient, and automated. With Experience Manager Forms, you can transform complex transactions into simple, digital experiences on virtually any device.

Experience Manager Communities — Helps you create online community experiences, including forums, user groups, learning resources, and other social features that are valuable to customers, employees, and your brand.

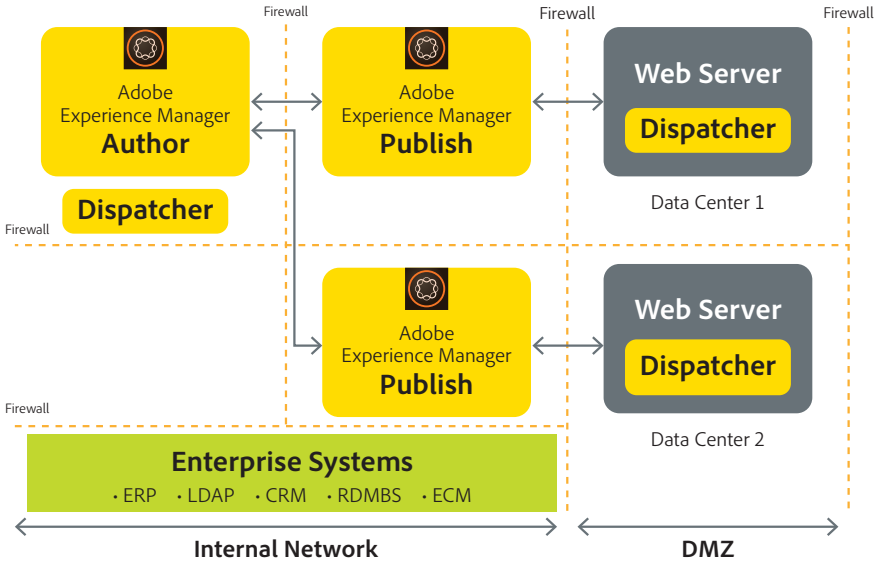


Figure 1: Adobe Experience Manager Application Architecture

Adobe Experience Manager Application Security

Adobe Experience Manager Data Flow Narrative

Before content authors can create and publish content in Adobe Experience Manager, web developers must create the target website using Sightly, an open-source templating language for Adobe Experience Manager. Sightly simplifies the component development process and allows HTML web developers to do programming that historically had to be done by Java/JSP developers. It also includes many built-in security controls. Sightly includes:

- A functional server-side template language;
- Auto-escaping to help ensure secure output by avoiding cross-site scripting (XSS) vulnerabilities, a top security risk according to Open Web Application Security Project (OWASP); and
- Proven technology used on real-life projects to increase development efficiency.

Based on HTML5 core technologies, Sightly turns written code into prebuilt reusable tags that eliminate the need to recreate frequently used elements such as navigation—freeing developers to concentrate on other projects. Also, security features help remove unnecessary data entry when several developers access a project at the same time, which previously exposed systems to possible XSS security breaches.

Once the templates have been created, content authors can use the templates to submit content to the website.

Authors log into the Adobe Experience Manager user interface and upload content to the servers. The document security feature proactively helps protect and control information from theft or misuse, regardless of where the information resides or travels—inside or outside the enterprise. With Adobe Experience Manager Forms Document Security, customers can create personalized PDF documents and allow desktop or mobile users to access them via the website or web portal. Adobe Experence Manager encrypts files and applies persistent and dynamic policies that help maintain confidentiality and control use on fixed or mobile devices.

If the customer has chosen Adobe to host its deployment, all content is protected during upload over the Internet using HTTPS. The content remains protected and private on the Adobe Experience Manager servers until the customer publishes the content, enabling consumers of the website to access it.

User Authentication for Adobe Experience Manager

Typically, customers choose to integrate Adobe Experience Manager into their existing enterprise identity management system. It supports legacy LDAP-compliant systems, SAML-compliant systems, SSO systems, and social integration via OAuth. Custom integrations are also possible.

LDAP Support

Adobe Experience Manager can leverage existing Lightweight Directory Access Protocol (LDAP) implementations, including Microsoft Active Directory, to authenticate user credentials. It also works with sophisticated authentication server deployments, such as synchronized, multi-server environments, to support massive scalability.

SAML Support for Federated Identity Management

Adobe Experience Manager is fully compatible with SAML (Security Assertion Markup Language) and can integrate with any SAML-compliant federated identity provider. SAML provides a standard XML representation for specifying the exchange of security information between a security system, such as an authentication authority, and an application that trusts the security system, and provides interoperable ways to exchange and obtain it. As such,

SAML helps ensure the security of identity information between business partners, keeping federated identity cross-domain transactions more secure.

Adobe Experience Manager ships with a *SAML authentication handler* that provides support for the SAML 2.0 Authentication Request Protocol including support for both Single Sign On and Single Log Out.

SSO Authentication Handler

Adobe Experience Manager includes an SSO Authentication Handler service for organizations that do not implement LDAP or SAML but want to create a federated identity for their users. This service processes the authentication results provided by the trusted authenticator. Single Sign On (SSO) allows a user to access multiple systems after providing authentication credentials (such as a user name and password) once. A separate system (known as the trusted authenticator) performs the authentication and provides Adobe Experience Manager with the user identity, generally in the form of an HTTP header. The SSO Authentication Handler can be used in concert with LDAP, if needed, or as part of a larger integration with bespoke identity management systems.

Social Integration via OAuth

The Social Login feature of Adobe Experience Manager enables organizations to provide a social login option on owned digital properties and then personalize the user experience based on profile information. Marketers can also combine social profile information with data from additional sources, such as a customer relationship management system or a website profile, to create a unified view of the customer.

Adobe Experience Manager includes built-in support for Social Login using Facebook and Twitter. This integration can be extended on a project basis to include other providers that support the OAuth standard. OAuth defines a framework for securing application access to protected resources, such as the identity attributes of a particular user. It allows an application that desires information to send an API query to a resource server hosting the desired information. The server can then authenticate that the client in fact sent the message.

Adobe Experience Manager as a Managed Service

When a customer chooses to have Adobe host its Adobe Experience Manager deployment as a managed service, a single-tenant, virtual container is created to house the customer instance of AEM. A Customer Success Engineer (CSE) works closely with the customer to configure the environment, including access control lists and port restrictions in AMS Enterprise deployments. All components are hosted on a cloud service provider certified by Adobe. Core infrastructure such as web application hosting, redundancy, and storage is enabled through this provider. These providers host services in

accordance with industry-standard practices and undergo regular industry-recognized certifications and audits.

Operational Responsibilities of Adobe Managed Services

Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and Adobe Experience Manager software, as well as the configuration of provided firewalls, and deployment of customer-developed code into production.

Secure Management

Adobe uses secure connections to manage and access customer instances. Multi-factor authentication is required to connect to the cloud infrastructure provider.

Geographic Location of Customer Data

Adobe, by default, stores all customer data in cloud service provider regions within the country of customer operations.

Data replication occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Isolation of Customer Data/Segregation of Customers

Adobe utilizes strong tenant isolation security and control capabilities to maintain the segregation of its customers. Each Managed Services instance is held in a single-tenant ,virtual container, which isolates each customer from other customers. Adobe uses Identity and Access Management (IAM) tools provided by the cloud infrastructure vendors to further restrict access to compute and storage instances.

Intrusion Detection

Adobe actively monitors both the Content Producer Service and the Distribution Service using industry-standard intrusion Detection Systems (IDS). Host-based Intrusion Detection Systems (HIDS) are also deployed on each production server for configuration file monitoring, virus and malware detection, and identification of root kits.

Logging

Adobe conducts server-side logging of customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs do not contain username/password combinations, or other confidential information. A centralized SIEM solution is used to correlate and monitor the events logged. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Data Storage and Backup

By default, Adobe conducts a differential backup of all AEM data on a daily basis and retains this backup information for seven days. The un-needed backup files are deleted, purged from the system, and overwritten by Amazon. This backup procedure can be adjusted, upon customer requestto cover virtually any frequency and retention period. The backup creation snapshot process takes only a few seconds, during which time the repository is in read-only mode. This is targeted for minimum load hours, but has very little impact on normal system operation in any case. This snapshot is then processed and distributed for availability in a second process that takes from 10 to 30 minutes.

Change Management

All changes to production instances of application sub-systems are controlled according to the requirements outlined in the Adobe Managed Services Configuration Management Plan. Only production systems are covered by this change control model; neither development/proof-of-

concept or staging/pre-production systems are covered. Because management and control of customer instance changes are critical to meeting service-level agreement (SLA) commitments, the Adobe Managed Services Change Approval Board (CAB) must review and approve any change prior to implementation, including a technical assessment of the security impact of the proposed change. All qualifying changes are documented prior to implementation, including business justification, timeline, risks, and rollback procedures. Approval archives are maintained for the life of the customer engagement.

Patch Management

Adobe is responsible for patching its guest operating systems (OS), Adobe Experience Manager software, and applications running on provider infrastructure. When patches are required, Adobe supplies a new, pre-hardened instance of the OS and application rather than an actual patch.

Operational Responsibilities of Cloud Infrastructure Providers

Adobe relies upon certified cloud infrastructure providers to operate, manage, and control the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Experience Manager is deployed.

These providers also operate the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. This infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Adobe requires these providers to adhere to industry-standard practices as well as a variety of security compliance standards.

Service Monitoring

Our cloud service providers monitor electrical, mechanical, and life support systems and equipment , and environmental states to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, our cloud providers are required to perform ongoing preventative maintenance.

Physical Environmental Controls

Required physical and environmental controls are specifically outlined in a SOC Report. The following section outlines some of the security measures and controls in place at data centers of our cloud service providers around the world.

Physical Facility Security

Cloud infrastructure partner data centers utilize industry standard architectural and engineering approaches. These data centers are housed in nondescript facilities and partners control physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Our infrastructure partners only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee our partners. All physical access to data centers is logged and audited routinely.

Fire Suppression

Our infrastructure providers provide automatic fire detection and suppression equipment in all data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Controlled Environment

Adobe cloud service providers employ a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. Data centers maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

Data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for data centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster Recovery

Data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters in various global regions, all data centers remain online 24/7/365 to serve customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Secure Network Architecture

Adobe also requires cloud service providers to employ network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic. Adobe works with our cloud providers to enforce the most up-to-date ACLs.

Network Monitoring and Protection

A variety of automated monitoring systems are enabled by our cloud infrastructure providers to help ensure a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points.

These tools provides significant protection against traditional network security issues:

- Distributed Denial Of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

Data Storage and Backup

Adobe stores by default all Adobe Experience Manager data using high durability storage services provided by our cloud infrastructure partners. To help provide durability, PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in a provider region. In addition, providers calculate checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Change Management

The clould service provider is responsible for authorizing, logging, testing, approving, and documenting routine, emergency, and configuration changes to existing infrastructure in accordance with industry norms for similar systems. Providers schedule updates to minimize any customer impact. Adobe maintains a Status Health Dashboard for Adobe Experience Manager, which can be accessed from the Adobe Experience Manager "Welcome" screen.

Patch Management

Adobe cloud infrastructure providers maintain responsibility for patching systems that support the delivery of IaaS services, such as the hypervisor and networking services.

Adobe Risk & Vulnerability Management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can help uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan.

Internally, the Adobe Experience Manager security team performs a risk assessment of all components prior to every release. Conducted by highly trained security staff trusted with creating a secure network topology and infrastructure and Adobe Experience Manager application, the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware as well as application-level vulnerabilities. The security touchpoints include exercises such as threat modeling coupled with vulnerability scanning and static and dynamic analysis of the application. The security team partners with technical operations and development leads to help ensure high-risk vulnerabilities are mitigated prior to each release.

Managed Services conducts penetration testing on a base installation of the solution, however security and penetration testing of customer-developed code or customizations is the responsibility of the customer.

Incident Response and Notification

New vulnerabilities and threats evolve each day and Adobe strives to respond to mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

When a significant announced vulnerability puts Adobe Experience Manager at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the organization to coordinate the mitigation effort.

For cloud-based services, Adobe centralizes incident response, decision-making, and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic Analysis

For incident investigations, the Adobe Experience Manager team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording. Adobe may engage with law enforcement or third-party forensic companies when it determines it is necessary.

The Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe Experience Manager team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.

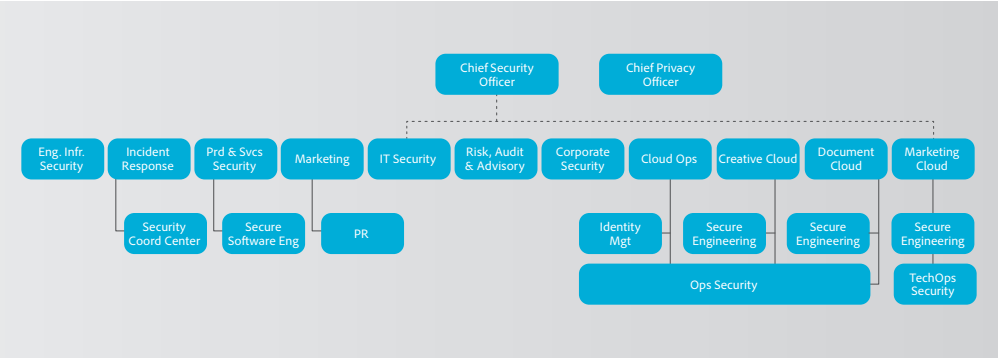


Figure 2: The Adobe Security Organization

Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Experience Manager organization employs the Adobe Software Product Lifecycle (SPLC) process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC activities include, depending on the specific Adobe Experience Manager component, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Experience Manager security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials

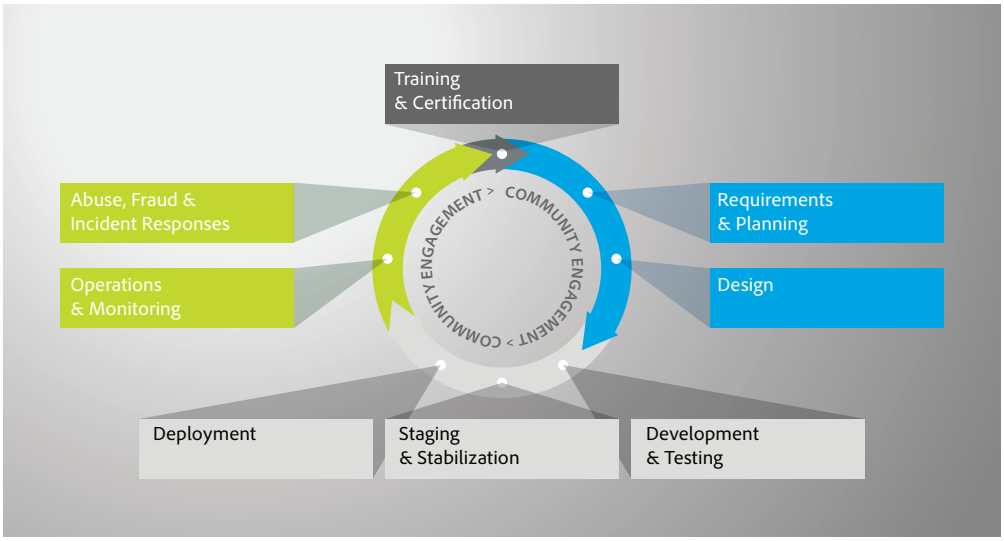


Figure 3: Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

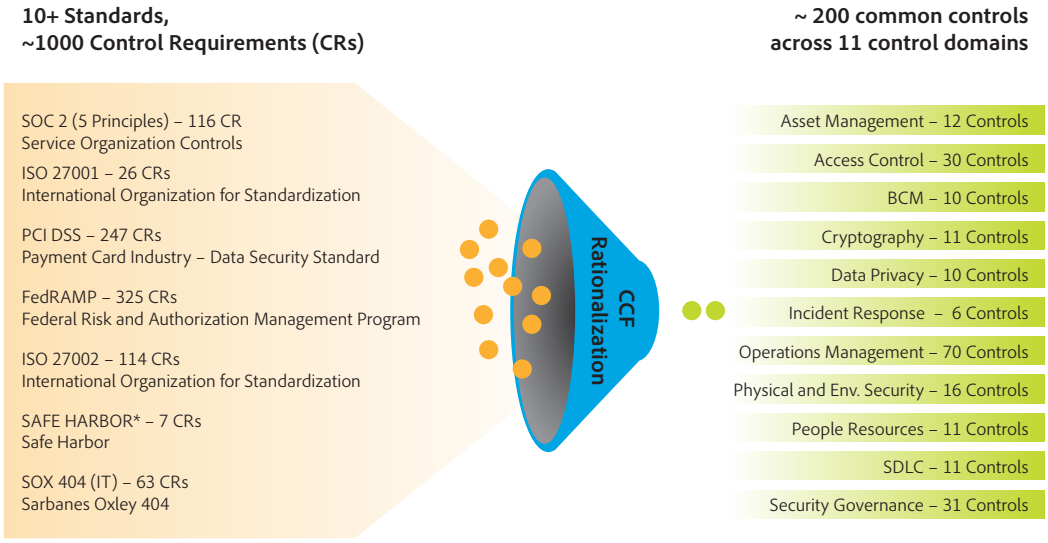
The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams within the Adobe Experience Manager organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.

Adobe Common Controls Framework

To protect from the software layer down, Adobe uses the Adobe Secure Product Lifecycle, which is described in the following section. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company's infrastructure, applications, and services and help Adobe comply with a number of industry accepted best practices, standards, and certifications.

In creating the Adobe Common Controls Framework (CCF), Adobe analyzed the criteria for the most common security certifications and found a number of overlaps. After analyzing more than 1000 requirements from relevant cloud security frameworks and standards, Adobe rationalized these down to approximately 200 Adobe-specific controls. The CCF control owners know exactly what is required to address the expectations of Adobe stakeholders and customers when it comes to implementing controls.



* For information on the recent Safe Harbor developments, visit the Adobe Safe Harbor FAQ.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Physical Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Adobe Experience Manager, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

Background Checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes 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. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee Termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can longer access to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Datacenter Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Customer Data Confidentiality

Adobe always treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

Security compliance

All Adobe services are governed by a comprehensive set of documented security processes and have been subject to numerous security audits to maintain and improve quality. Adobe services are under continuing self review to ISO 27001 standards and the Shared Cloud underlying services infrastructure has a SOC 2 – Security certification.

Adobe complies with several compliance certifications and standards across its product lines. Please refer to the "Adobe Security and Privacy Certifications" white paper for the lastest information on approved certifications for Adobe Experience Manager.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of the Adobe Experience Manager environment and your confidential data. At Adobe, we take the security of your digital experience very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

Adobe

Adobe Systems Incorporated
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 the Adobe solution, 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 Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 04/2018 Adobe Systems Incorporated. All rights reserved. Printed in the USA.