Adobe Security and Privacy Certifications

Our Priority for Hosted Services: Protect Our Customers and Their Data
At Adobe, we take the security of your data and digital experience seriously. To protect from the software layer down, we use the Adobe Secure Product Lifecycle—a rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, integrated into multiple stages of the product lifecycle. To protect from the physical layer up, we are implementing a foundational framework of security processes and controls to protect our infrastructure, applications and services and help us comply with a number of industry accepted best practices, standards and certifications.

Common Controls Framework: Clear and Efficient Security
One of the goals of Common Controls Framework is to provide Adobe employees with clear guidance on how to secure our infrastructure and applications. We analyzed the criteria for the most common security certifications and found a number of overlaps. We analyzed over 1000 requirements from relevant cloud security frameworks and standards and rationalized them down to about 200 Adobe-specific controls. The Adobe Common Controls Framework (CCF) control owners know exactly what is required to address expectations of Adobe stakeholders and customers when it comes to implementing controls.

10+ Standards, ~1000 Control Requirements (CRs)

SOC 2 (5 Principles) – 116 CR
Service Organization Controls
ISO 27001 – 26 CRs
International Organization for Standardization
PCI DSS – 247 CRs
Payment Card Industry – Data Security Standard
FedRAMP – 325 CRs
Federal Risk and Authorization Management Program
ISO 27002 – 114 CRs
International Organization for Standardization
SAFE HARBOR – 7 CRs
Safe Harbor
SOX 404 (IT) – 63 CRs
Sarbanes Oxley 404

~ 200 common controls across 11 control domains

Asset Management – 12 Controls
Access Control – 30 Controls
BCM – 10 Controls
Cryptography – 11 Controls
Data Privacy – 10 Controls
Incident Response – 6 Controls
Operations Management – 70 Controls
Physical and Env. Security – 16 Controls
People Resources – 11 Controls
SOLC – 11 Controls
Security Governance – 31 Controls
Common Controls Framework Conceptual Model

We realized that a product-specific, “siloed” compliance approach wouldn’t be cost-effective or efficient to achieve. The CCF is set up to allow teams to inherit control capabilities from other parts of the organization. For example: software engineers are not responsible for datacenter security. However, they inherit, the datacenter security capabilities from a data center operations team. The simplicity of Adobe’s strategy will enable the execution of sustainable security controls going forward.

Adobe Product Cloud
Physical & Environmental Security

Product Operations
Monitoring Configuration
Asset Management Change Management
Logical Access Incident Response

Product Engineering
System Development Lifecycle

Adobe Corporate
Business Continuity
Security Governance
Data Privacy
People Resources

Certification Roadmap

Adobe has several certifications currently in place. Others are in process and at various phases according to the overall Adobe CCF implementation roadmap.

*Shared Cloud is the infrastructure component supporting the Adobe Creative Cloud.

This roadmap provides a summary of our current plans for implementation of the Common Controls Framework and is subject to change.
Current certifications

<table>
<thead>
<tr>
<th>Service</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Products and Services</td>
<td>Adobe Connect Hosted– SOC 2</td>
</tr>
<tr>
<td></td>
<td>Adobe.com e-commerce Website—PCI DSS V3 Level 1 compliant merchant</td>
</tr>
<tr>
<td></td>
<td>Adobe Document Cloud e-Sign Services—PCI DSS V3 Level 1 compliant as a</td>
</tr>
<tr>
<td></td>
<td>merchant and service provider, HIPAA compliant, SOC 2 (Security &amp; Availability)</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>HIPAA; SOC 1/SSAE 16/ISAE 3402 (formerly SAS70); SOC 2, SOC 3, PCI DSS V3 Level</td>
</tr>
<tr>
<td></td>
<td>1, ISO 27001, FedRAMP (SM), DIACAP and FISMA, ITAR, FIPS 140-2, CS, MPAA</td>
</tr>
<tr>
<td>Rackspace</td>
<td>ISO IEC 27001, SOC 2</td>
</tr>
<tr>
<td>Operations</td>
<td>Shared Cloud: SOC 2 – Security</td>
</tr>
<tr>
<td>Privacy</td>
<td>Adobe—Safe Harbor Self Certified.</td>
</tr>
</tbody>
</table>

*Adobe uses Amazon Web Services (AWS) and Rackspace to host certain services

Continuous Controls Improvement

The 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.
On-Going Commitment

But CCF is more than just achieving a set of certifications and renewing them. It’s a central part of our company-wide security strategy. Adobe has the people, process and technology, as well as the various oversight, audit and follow-up mechanisms in place to ensure that CCF is not just a point in time. It’s part of our on-going commitment to help protect our customers and their data.

Please visit Adobe’s security information site (http://www.adobe.com/security) for more information about security efforts across our products and services.