Adobe Cloud Services

Compliance – Überblick

Überblick

Die Sicherheit, der Schutz und die Verfügbarkeit der Kundendaten haben für Adobe höchste Priorität. Eine fundierte Strategie für Compliance und Risiko-Management nimmt einen ebenso hohen Stellenwert für den Erfolg eines Unternehmens ein wie die Produktstrategie. Unsere Cloud-Strategie umfasst daher einen Zwei-Punkte-Plan, um Ihre Daten gleichzeitig sicher und verfügbar zu halten.

Für den Schutz auf der physischen Ebene haben wir das Adobe Common Controls Framework (CCF) als grundlegendes Regelwerk für Sicherheitsprozesse und Kontrollmechanismen implementiert. Es gewährleistet die Sicherheit der Infrastruktur sowie der Anwendungen und Services von Adobe und die Übereinstimmung mit Best Practices, Standards, Normen, Gesetzen und Zertifizierungen der Branche.

Für den Schutz der Software-Ebene werden im Rahmen des Adobe Secure Product Lifecycle-Programms (SPLC) mehrere Hundert Sicherheitsmaßnahmen in den Verfahren, Prozessen und Werkzeugen der Software-Entwicklung umgesetzt. SPLC ist in vielen Phasen des Produktlebenszyklus fest verankert.

Inhalt

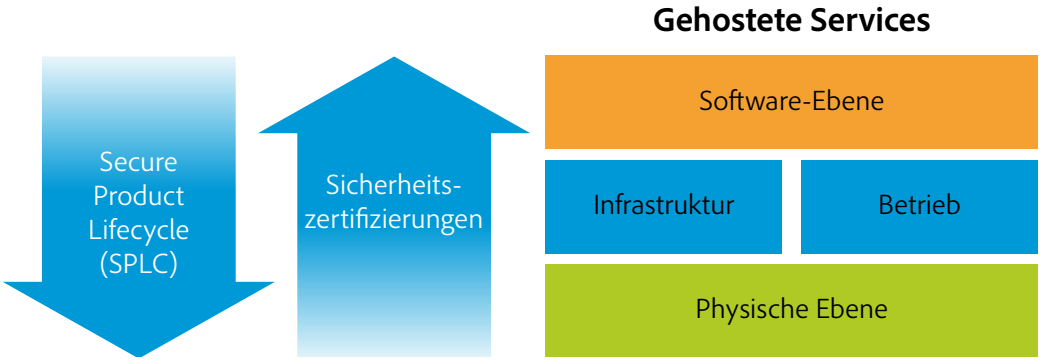

Abb. 1: Adobe Secure Product Lifecycle und Adobe Common Controls Framework regeln die Compliance mit Branchenstandards und Gesetzen.

Welche Standards werden von Adobe unterstützt?

Der hohe Stellenwert, den Adobe der Sicherheit einräumt, wird in den implementierten Branchenstandards und der Einhaltung der gesetzlichen Vorgaben für Datensicherheit und -schutz sichtbar. Für die Cloud gibt es zahlreiche Branchenstandards und Zertifizierungen mit Tausenden unterschiedlicher Compliance-Anforderungen. Da sich diese in wesentlichen Punkten überschneiden, legen wir den Schwerpunkt auf die mit den größten Auswirkungen für unsere Kunden. Sobald neue Sicherheitsstandards und gesetzliche Vorgaben aufgestellt und für die Branche relevant werden, werden sie von Adobe geprüft und übernommen, sofern sie unsere Kunden betreffen. Die Services von Adobe erfüllen je nach Ausrichtung eine oder mehrere der im Folgenden genannten Branchenstandards oder gesetzlichen Auflagen.

Branchenstandards

Die Compliance-Anforderungen der folgenden primären Branchenstandards haben höchste Priorität für Adobe:

- **SOC**: Der SOC-Berichtsstandard (Service Organization Control) wurde vom American Institute of Public Accountants (AICPA, Berufsverband amerikanischer Wirtschaftsprüfer) entwickelt. Adobe verwendet derzeit den SOC 2-Standard. Grundlage für SOC 2-Berichte ist eine unabhängige Zertifizierung, die die Anwendung der Trust Service Principles (TSPs) Sicherheit, Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz bescheinigt.

- **ISO 27001**: Diese Zertifizierung belegt einen systematischen Ansatz im Umgang mit Gefährdungen der Informationssicherheit, insbesondere in Bezug auf die Vertraulichkeit, Integrität und Verfügbarkeit von Services und Kundendaten. Das ISO 27001-Siegel setzt ein formales Programm für Informationssicherheit voraus und bescheinigt Adobes Verpflichtung zu Transparenz in seinen internen Sicherheitsmechanismen und -verfahren. Auf die Erfüllung von ISO 27001 wird besonders in Ländern außerhalb der USA viel Wert gelegt.
- **FedRAMP**: Das Federal Risk and Authorization Management Program (FedRAMP) ist eine Zusammenstellung von Standards der US-Bundesbehörden für die Sicherheitsbewertung, Genehmigung und fortlaufende Überwachung von Cloud-Lösungen. Das FedRAMP ist für bestimmte US-Behörden verpflichtend, da die Zertifizierungen festlegen, welche Cloud-Lösungen von US-Behörden und ihren Vertragspartnern erworben und implementiert werden dürfen.
- **PCI DSS**: Der Payment Card Industry Data Security Standard (PCI DSS) ist ein eigener Standard für Informationssicherheit im Zahlungsverkehr, insbesondere die Abwicklung von Kreditkartentransaktionen. Eine PCI DSS-Zertifizierung erhöht die Sicherheit bei der Verwaltung von Kartendaten und -transaktionen. Als Anbieter von PCI DSS-konformen Services unterstützt Adobe seine Kunden dabei, die PCI-Anforderungen für eine sichere Verwaltung personenbezogener Daten zu erfüllen.

Gesetzliche Auflagen

Adobe entwickelt Technologien und Services, die Kunden die Einhaltung der jeweils geltenden gesetzlichen Vorschriften erleichtern. Letztendlich liegt es in der Verantwortung der Kunden, dass ihre Konfiguration des genutzten Adobe-Diensts in Übereinstimmung mit den gültigen Gesetzen eingerichtet und gesichert ist.

- **GLBA**: Der Gramm-Leach-Bliley Act (GLBA) verpflichtet Finanzdienstleister, die Sicherheit der persönlichen Daten ihrer Kunden zu gewährleisten. Adobe-Services mit dem Siegel „GLBA-Ready" eignen sich für Kunden, die den GLBA-Bestimmungen in Bezug auf die Inanspruchnahme von Dienstleistern unterliegen.
- **HIPAA**: Der Health Insurance Portability and Accountability Act (HIPAA) regelt den Einsatz elektronischer Patientenakten und enthält Sicherheits- und Datenschutzbestimmungen für personenbezogene Gesundheitsdaten (im Englischen als PHI für Protected Health Information = geschützte Gesundheitsdaten bezeichnet). Gesundheitsdienstleister und Versicherungen, die vertrauliche PHI-Daten führen, dürfen in den USA nur HIPAA-konforme Produkte verwenden. Bestimmte Adobe-Dienste können für eine HIPAA-konforme Verwendung durch Benutzer konfiguriert werden, die als Organisation unter HIPAA fallen und ein sogenanntes Business Associate Agreement (BAA) mit Adobe unterzeichnen.
- **21 CFR**: Mit dem Code of Federal Regulations, Title 21, Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11) hat die amerikanische Lebens- und Arzneimittelbehörde FDA (U.S. Food and Drug Administration) die Verwendung elektronischer Datensätze und elektronischer Signaturen geregelt. Adobe-Services nach 21 CFR Part 11 sind so konfiguriert, dass Kunden aus der Pharmaindustrie, die unter die Zuständigkeit der FDA fallen, die 21 CFR Part 11-Vorschriften einhalten können.
- **FERPA**: Der US-amerikanische Family Educational Rights and Privacy Act (FERPA) wahrt die Vertraulichkeit der Daten von Schülern und Studierenden. Für Kunden aus dem Bildungswesen kann Adobe gemäß den FERPA-Richtlinien nach vertraglicher Vereinbarung im Zusammenhang mit gesetzlich geregelten Schüler- und Studentendaten als offizieller Vertreter einer Bildungseinrichtung agieren.

Adobe Common Controls Framework

Das Adobe Common Controls Framework (CCF) umfasst eine Reihe von Sicherheitsmaßnahmen und Compliance-Kontrollen, die in den Produktteams sowie in verschiedenen Teilen der Infrastruktur- und Anwendungsteams im Einsatz sind. Bei der Entwicklung des CCF hat Adobe die Kriterien der gängigsten Sicherheitszertifikate für Cloud-basierte Unternehmen analysiert. Mehr als 1.000 Anforderungen wurden in Adobe-spezifische Kontrollmechanismen umgesetzt, die etwa einem Dutzend Branchenstandards entsprechen.

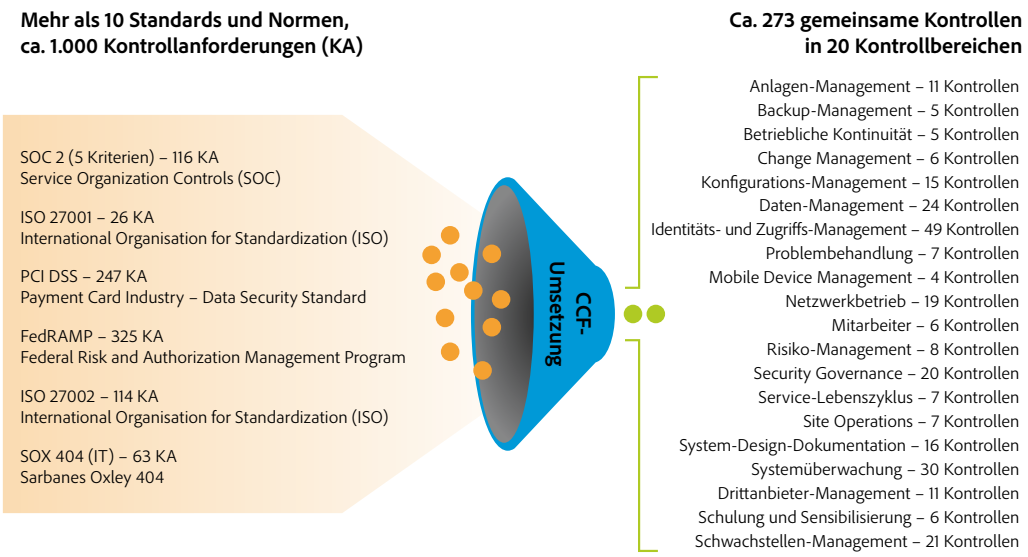

Abb. 2: Adobe Common Controls Framework

Da eine produktspezifische Einzellösung weder kostengünstig noch effizient wäre, wurde das Adobe CCF so konzipiert, dass Teams die Kontrollfunktionen aus anderen Organisationsbereichen übernehmen können. Software-Entwickler sind beispielsweise nicht für die Sicherheit des Rechenzentrums verantwortlich, übernehmen jedoch die Sicherheitskapazitäten des Data Center-Teams. Dieses einfache Prinzip ermöglicht eine kontinuierliche Anwendung nachhaltiger Sicherheitsmechanismen.

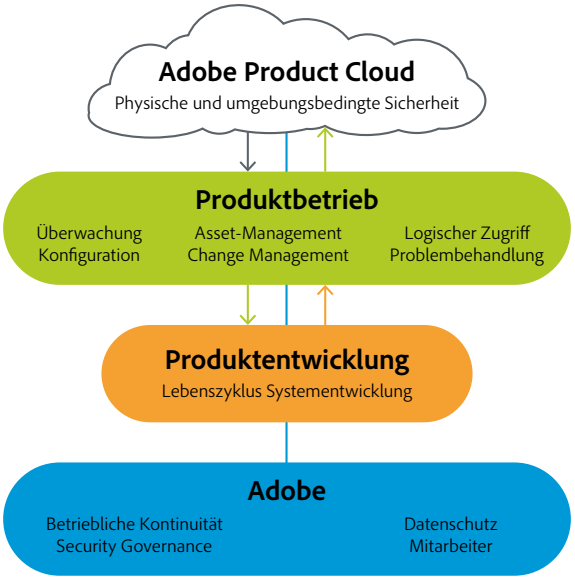

Abb. 3: Konzept des Adobe CCF-Regelwerks

Das SPLC-Programm ist konsequent auf das CCF und etablierte Branchenverfahren für Software-Entwicklungs-Teams abgestimmt, um Compliance zu gewährleisten. Als solides Rahmenwerk konzipiert, enthält es zahlreiche Kontrollmechanismen, die jetzt über das CCF abgedeckt werden, darunter Sicherheitstests (z. B. statische/dynamische Analysen, Penetrationstests usw.) sowie jährliche Schulungen von Software-Entwicklern zu sicheren Programmierverfahren. Das SPLC fand bereits in allen Adobe-Entwickler-Teams Anwendung. Die Einführung des CCF und neue Compliance-Erfordernisse trugen aufgrund der verbesserten Prozessdokumentation und Genauigkeit jedoch zu einem einheitlicheren Einsatz innerhalb Adobes bei.

Das Thema Compliance betrifft auch die operativen und IT-Bereiche von Adobe. Schlüsselfunktionen im Anlagen-Management, betrieblichen Kontinuitäts-Management, Change Management und Netzwerkbetrieb sowie im Daten-, Konfigurations- und Backup-Management, im Identitäts- und Zugriffs-Management und in der Problembehandlung werden strenger und konsistenter im Unternehmen angewendet. Eine positive Auswirkung haben Compliance-Vorgaben außerdem auf die Datenschutzüberwachung für PII und PHI, die logische Zugriffssteuerung für Produktions- und Quell-Code-Kontrollsysteme sowie die Sicherheitsrichtlinien für das Unternehmensnetzwerk.

Alle Adobe-Mitarbeiter müssen einmal jährlich an einer Schulung zum Thema Sicherheit teilnehmen. Zusätzlich bietet Adobe weitere sicherheitsrelevante Schulungen für die jeweiligen Aufgabenbereiche und Zuständigkeiten der einzelnen Mitarbeiter an. Der Compliance-Prozess erfordert außerdem, dass Abläufe unternehmensweit formalisiert werden. Die Prozeduren werden im Vorfeld dokumentiert und in der Ausführung konsequent nachvollzogen. Den Abschluss bildet ein Nachweis über die Fertigstellung. Beispiel: Die Bereitstellung von Benutzerzugriffen auf eine Produktionsumgebung setzt einen Genehmigungsprozess mit Ticket voraus, d. h., der Zugriff des Benutzers auf die Umgebung darf erst nach erfolgter Genehmigung freigeschaltet werden. Adobe dokumentiert dieses Verfahren, und das Ticket bildet den Nachweis für diese Dokumentation.

Die durchgängige Anwendung der Compliance-Vorgaben wird regelmäßig überprüft, normalerweise einmal pro Quartal. Die Prüfungen beinhalten Bewertungen der Zugriffe auf Produktionssysteme, Sicherheitslücken und Firewall-Regeln. Mehr als 40 Teams im Unternehmen wurden für die Durchführung der Quartalsprüfungen geschult. Dazu zählen der Gegenstand der Prüfung, die Vollständigkeit der Prüfung und der Nachweis der Prüfung.

Adobe hat mit einer unternehmensweiten GRC-Lösung (Governance, Risk and Compliance) eine effektives Modell für die Führung und Kontrolle des Compliance-Programms etabliert. Dabei werden automatisch Kennzahlen für Berichte und Dashboards, Audits sowie Risikoeinschätzungen erstellt und Probleme und deren Beseitigung verfolgt. Zusätzlich implementiert Adobe ein periodisches Programm zur Selbstbeurteilung von Kontrollen, Prozessen und Risiken, mit dem die Unternehmensführung die Compliance-Risiken evaluieren und die operative Effektivität der Compliance-Prozesse und -Kontrollmechanismen attestieren kann. Die GRC-Lösung bietet einen wirksamen Mechanismus für Führungskräfte und Auditoren, Verantwortung und Rechenschaft im Compliance-Programm zu etablieren und dessen operative Effektivität kontinuierlich zu überwachen.

Der Adobe Common Controls Framework-Prozess endet jedoch nicht mit Zertifizierungen oder der Einhaltung von Standards und Normen. Das CCF ist vielmehr ein kontinuierlicher Prozess, der regelmäßige interne Audits, externe Beurteilungen und fortlaufende Verbesserungen der Kontrollmechanismen umfasst. Aufgrund seiner flexiblen Auslegung kann das CCF rasch und problemlos an neue Standards und geänderte Anforderungen sowie internationale und regionale Anforderungen angepasst werden.

Adobe und Compliance – Aktueller Status

Zur Sicherstellung einer konsistenten, unternehmensweiten Strategie für alle Cloud-Produkte und Plattform-Services hat Adobe einen umfassenden Compliance-Plan entwickelt. Anhand dieses Plans dokumentiert jedes Team im Unternehmen die Sicherheits- und Datenschutzkontrollen, die implementiert werden sollen. Danach implementiert das Team die dokumentierten Kontrollen und führt kontinuierlich und in regelmäßigen Abständen Audits zum Nachweis der Umsetzung durch.

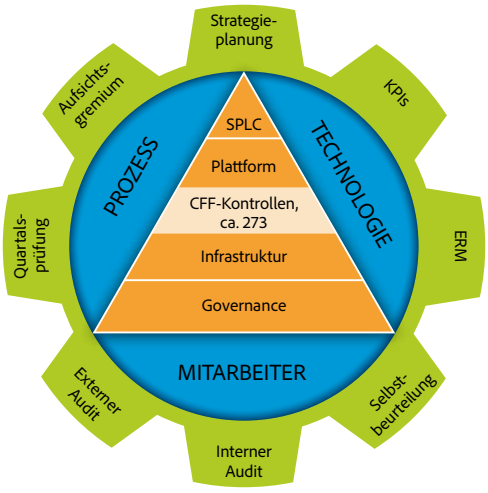

Abb. 4: Adobe hat ein umfassendes Governance-Modell implementiert, das die kontinuierliche Ausführung, Wirksamkeit und Überwachung der Sicherheitsmechanismen gewährleistet.

Adobe und Compliance – Roadmap

Neben den bereits realisierten Zertifizierungen und Compliance-Zielen beinhaltet die allgemeine Roadmap für die CFF-Implementierung weitere Maßnahmen und Aktivitäten, die sich aktuell in verschiedenen Phasen befinden. Die folgende Abbildung zeigt die aktuellen Zertifizierungen und laufenden Projekte zur Implementierung des Common Controls Framework (Änderungen vorbehalten).

	SOC2 – Typ 1		SOC2 – Typ 2						
Adobe Cloud-Produkt/Service	**Sicherheit**	**Verfügbarkeit**	**Sicherheit u. Verfügbarkeit**	**ISO 27001**	**GLBA-Ready***	**FERPA-Ready***	**PCI**	**HIPAA***	**FedRAMP**
Marketing Cloud – On-Demand-Services									
• Adobe Analytics	✓		November 2016		✓				
• Adobe Campaign	✓				✓				
• Adobe Experience Manager**	✓				✓				
• Adobe Media Optimizer	✓				✓				
• Adobe Primetime	✓				✓				
• Adobe Social	✓				✓				
• Adobe Target	✓				✓				
• Adobe Connect	✓				✓				
Marketing Cloud – Managed Services									
• Adobe Experience Manager**	✓	✓		✓	✓	✓		✓	✓
• Adobe Connect	✓	✓		✓	✓	✓		✓	✓
Creative Cloud für Unternehmen (CCE)									
• CCE Shared Services (Öffentlich)			November 2016			✓			
• CCE Managed Services (Privat)						✓			
• Adobe Stock			NICHT ZUTREFFEND				✓		
• E-Commerce							✓		
Document Cloud									
• Adobe Sign	✓	✓	✓	✓	✓	✓	✓	✓	
• PDF-Dienste			November 2016				✓		

Abb. 5: Roadmap für Adobe Compliance

Diese Ansicht zeigt unsere aktuellen Implementierungspläne für das Common Controls Framework (Änderungen vorbehalten). Neu erworbene Unternehmen, die Teil eines Adobe-Services werden, erfüllen die aufgeführten Zertifizierungen und Vorschriften unter Umständen nicht.

*Nach den FERPA-Richtlinien kann Adobe im Rahmen einer gesonderten Vereinbarung für die Abwicklung von gesetzlich geregelten Schüler- und Studentendaten als offizieller Vertreter einer Bildungseinrichtung auftreten, um Kunden aus dem Bildungswesen die Einhaltung von FERPA-Vorgaben zu ermöglichen. Adobe-Services, die als GLBA-Ready, FERPA-Ready oder HIPAA-konform bezeichnet werden, können vom Kunden so genutzt werden, dass er seine gesetzlichen Vorgaben in Bezug auf die Inanspruchnahme von Dienstleistern erfüllt. Letztendlich trägt der Kunde die Verantwortung dafür, dass gesetzliche Auflagen eingehalten werden, der Adobe-Dienst die Compliance-Anforderungen erfüllt und der Service angemessen gesichert ist.

**Mit Ausnahme von AEM Mobile und AEM Livefyre

Fazit

Das Adobe Common Controls Framework ist ein zentraler Bestandteil der unternehmensweiten Sicherheitsstrategie. Mit seinen Mitarbeitern, Prozessen und Technologien sowie verschiedenen Analyse-, Audit- und Folgemechanismen stellt Adobe sicher, dass es sich beim CCF nicht um eine temporäre Maßnahme, sondern um eine beständige Verpflichtung gegenüber der Sicherheit unserer Kunden und ihrer Daten handelt.

Weitere Informationen zu Sicherheitsmaßnahmen für Produkte und Services von Adobe erhalten Sie auf der *Adobe-Website zum Thema Sicherheit*.

Adobe

Adobe Systems GmbH
Georg-Brauchle-Ring 58
D-80992 München
Adobe Systems (Schweiz) GmbH
World Trade Center
Leutschenbachstrasse 95
CH-8050 Zürich
www.adobe.de
www.adobe.at
www.adobe.ch
www.adobe.com

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. Wenn Sie weitere Informationen zu den Lösungen und Kontrollmechanismen von Adobe wünschen, wenden Sie sich bitte an Ihren Adobe-Vertriebsmitarbeiter. Weitere Informationen zu Adobe-Lösungen, z. B. zu SLAs, Änderungsgenehmigungen, Vorgehensweisen zur Zugriffssteuerung und Datenwiederherstellungs-Prozessen, stehen bei Bedarf zur Verfügung.

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.

© 2016 Adobe Systems Incorporated. All rights reserved.

8/16