



The Common Controls Framework

BY ADOBE

The Common Controls Framework **by Adobe**

The following table contains the baseline security subset of control activities (derived from the Common Controls Framework by Adobe) that apply to Adobe's enterprise offerings. The control activities help Adobe enterprise offerings meet the requirements of ISO/IEC 27001, AICPA SOC Common Criteria, AICPA SOC Availability as well as the security requirements of GLBA and FERPA. These common activities were identified and developed based on industry requirements and adopted by product operations and engineering teams to achieve compliance with these standards. This information is only to be used as an illustrative example of common security controls that could be tailored to meet minimum security objectives within an organization.

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Asset Management	Device and Media Inventory	Inventory Management	[The organization] maintains an inventory of system devices, which is reconciled [in accordance with an organization-defined frequency].	A.8.1.1				
Asset Management	Device and Media Inventory	Inventory Labels	[The organization's] assets are labeled and have designated owners.	A.8.1.2				
Asset Management	Device and Media Transportation	Asset Transportation Authorization	[The organization] authorizes and records the entry and exit of systems at datacenter locations.	A.11.2.5 A.11.2.6				
Asset Management	Device and Media Transportation	Asset Transportation Documentation	[The organization] documents the transportation of physical media outside of datacenters. Physical media is packaged securely and transported in a secure, traceable manner.	A.11.2.5 A.11.2.6 A.8.3.3				
Asset Management	Component Installation and Maintenance	Maintenance of Assets	Equipment maintenance is documented and approved according to management requirements.	A.11.2.4				
Business Continuity	Business Continuity Planning	Business Continuity Plan	[The organization's] business continuity and disaster recovery plans are reviewed [in accordance with an organization-defined frequency], approved by management, and communicated to authorized personnel.	A.17.1.1 A.17.1.2	CC7.5 CC9.1	A1.2		

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Business Continuity	Business Continuity Planning	Continuity Testing	[The organization] performs business contingency and disaster recovery tests [in accordance with an organization-defined frequency] and ensures the following: <ul style="list-style-type: none"> • tests are executed with relevant contingency teams • test results are documented • corrective actions are taken for exceptions noted • plans are updated based on results 	A.17.12 A.17.13	CC7.5 CC9.1	A1.3		
Backup Management	Backup	Backup Configuration	[The organization] configures redundant systems or performs data backups [in accordance with an organization-defined frequency] to enable the resumption of system operations in the event of a system failure.	A.18.1.3		A1.2		
Backup Management	Backup	Resilience Testing	[The organization] performs backup restoration or failover tests [in accordance with an organization-defined frequency] to confirm the reliability and integrity of system backups or recovery operations.	A.12.3.1		A1.3		
Configuration Management	Baseline Configurations	Baseline Configuration Standard	[The organization] ensures security hardening and baseline configuration standards have been established according to industry standards and are reviewed and updated [in accordance with an organization-defined frequency] or when required due to significant change.		CC7.1 CC7.2		314.4(b)(3)	FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Configuration Management	Baseline Configurations	Configuration Checks	[The organization] uses mechanisms to detect deviations from baseline configurations in production environments.		CC6.1 CC7.1 CC7.2		314.4(b)(3)	FERPA_99.31(a)
Configuration Management	Baseline Configurations	Time Clock Synchronization	Systems are configured to synchronize information system time clocks based on International Atomic Time or Coordinated Universal Time (UTC).	A.12.4.4				
Configuration Management	Approved Software	Software Installation	Installation of software or programs in the production environment is approved by authorized personnel.	A.12.5.1 A.12.6.2 A.9.4.4				
Change Management	Change Management	Change Management Workflow	Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow; notification and approval requirements are also pre-established based on risk associated with change scope and type.	A.12.1.2 A.14.2.2 A.14.2.4	CC2.3 CC8.1			FERPA_99.31(a)
Change Management	Change Management	Change Approval	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: <ul style="list-style-type: none"> • change description • impact of change • test results • back-out procedures 	A.12.5.1 A.14.2.3 A.14.2.4	CC8.1			FERPA_99.31(a)
Change Management	Segregation of Duties	Segregation of Duties	Changes to the production environment are implemented by authorized personnel.	A.14.2.6 A.6.1.2				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Data Management	Data Classification	Data Classification Criteria	[The organization's] data classification criteria are reviewed, approved by management, and communicated to authorized personnel [in accordance with an organization-defined frequency]; management determines the treatment of data according to its designated data classification level.	A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.18.1.3 A.18.1.4			314.3(b)(1)	
Data Management	Choice and Consent	Terms of Service	Consent is obtained for [the organization's] Terms of Service (ToS) prior to collecting personal information and when the ToS is updated.		CC2.3			FERPA_99.31(a)
Data Management	Choice and Consent	Enterprise License Agreements	Consent is obtained for the Enterprise Licensing Agreements (ELA) prior to collecting personal information and when the ELA is renewed.		CC2.3			FERPA_99.31(a)
Data Management	Data Handling	External Privacy Inquiries	In accordance with [the organization] policy, [the organization] reviews privacy-related inquiries, complaints, and disputes.	A.18.1.4				
Data Management	Data Handling	Test Data Sanitization	[Restricted (as defined by the organization's data classification criteria)] data is redacted prior to use in a non-production environment.	A.14.3.1				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Data Management	Data Encryption	Encryption of Data in Transit	[Restricted (as defined by the organization's data classification criteria)] data that is transmitted over public networks is encrypted.	A.13.2.3 A.14.1.2 A.14.1.3 A.18.1.4 A.18.1.5	CC6.7		314.3(b)(1) 314.3(b)(2) 314.3(b)(3)	FERPA_99.31(a)
Data Management	Data Encryption	Encryption of Data at Rest	[Restricted (as defined by the organization's data classification criteria)] data at rest is encrypted.	A.18.1.4 A.18.1.5 A.8.2.3				
Data Management	Data Removal	Secure Disposal of Media	[The organization] securely destroys media containing decommissioned [Restricted (as defined by the organization's data classification criteria)] data and maintains a log of such activities.	A.11.2.7 A.8.3.2	CC6.5			
Identity and Access Management	Logical Access Account Lifecycle	Logical Access Provisioning	Logical user access provisioning to information systems requires approval from authorized personnel based on documented specification of: <ul style="list-style-type: none"> • access privileges granted • account type (e.g., standard, guest, or temporary) • group membership (if applicable) 	A.9.2.1 A.9.2.2 A.18.1.3	CC6.1 CC6.2 CC6.3 CC6.6 CC6.7		314.3(b)(3)	FERPA_99.31(a)
Identity and Access Management	Logical Access Account Lifecycle	Logical Access De-provisioning	Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.	A.7.3.1 A.9.2.1 A.9.2.2 A.9.2.6 A.18.1.3	CC6.2 CC6.3 CC6.6 CC6.7		314.3(b)(3)	FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Identity and Access Management	Logical Access Account Lifecycle	Logical Access Review	[The organization] performs account and access reviews [in accordance with an organization-defined frequency]; corrective action is taken where applicable.	A.9.2.5 A.18.1.3	CC6.2 CC6.3 CC6.7		314.3(b)(3)	FERPA_99.31(a)
Identity and Access Management	Logical Access Account Lifecycle	Shared Logical Accounts	[The organization] restricts the use of shared and group authentication credentials to authorized personnel. Authentication credentials for shared and group accounts are reset [in accordance with an organization-defined frequency].		CC6.1			FERPA_99.31(a)
Identity and Access Management	Authentication	Unique Identifiers	[The organization] creates unique identifiers for user accounts and prevents identifier reuse.	A.9.4.2	CC6.1		314.3(b)(3)	FERPA_99.31(a)
Identity and Access Management	Authentication	Password Authentication	User and device authentication to information systems is protected by passwords that meet [the organization's] password complexity requirements. [The organization] requires system users to change passwords [in accordance with an organization-defined frequency].	A.9.1.2 A.9.4.2 A.9.4.3	CC6.1 CC6.6 CC6.7		314.3(b)(3)	FERPA_99.31(a)
Identity and Access Management	Authentication	Multifactor Authentication	Multi-factor authentication is required for: <ul style="list-style-type: none"> • remote sessions • access to environments that host production systems 	A.11.2.6 A.9.4.2				
Identity and Access Management	Authentication	Authentication Credential Maintenance	Authorized personnel verify the identity of users before modifying authentication credentials on their behalf.	A.9.2.4 A.9.3.1				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Identity and Access Management	Role-Based Logical Access	Logical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with logical access roles are approved by authorized personnel.	A.18.13 A.9.2.3 A.9.4.1	CC6.1 CC6.3 CC6.7		314.3(b)(3)	FERPA_99.31(a)
Identity and Access Management	Role-Based Logical Access	Source Code Security	Access to modify source code is restricted to authorized personnel.	A.9.4.5				
Identity and Access Management	Remote Access	Virtual Private Network	Remote connections to the corporate network are accessed via VPN through managed gateways.	A.11.2.6	CC6.6 CC6.7			FERPA_99.31(a)
Identity and Access Management	End User Authentication	End-user Access to Applications and Data	[The organization's] applications secure user data and maintain confidentiality by default or according to permissions set by the customer; the organization authenticates individuals with unique identifiers and passwords prior to enabling access to: <ul style="list-style-type: none"> • use the application • view or modify their own data 					FERPA_99.33(a)(l)
Identity and Access Management	Key Registration	Key Repository Access	Access to the cryptographic keystores is limited to authorized personnel.	A.10.12 A.18.15	CC6.1 CC6.3			FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Identity and Access Management	Key Registration	Data Encryption Keys	[The organization] changes shared data encryption keys: <ul style="list-style-type: none"> • at the end of an organization-defined lifecycle period • when keys are compromised • upon termination/transfer of employees with access to the keys 	A.10.12 A.18.15				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Incident Response	Incident Response	Incident Response Plan	<p>[The organization] defines the types of incidents that need to be managed, tracked and reported, including:</p> <ul style="list-style-type: none"> • 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, [in accordance with an organization-defined frequency], or when major changes to the organization occur 	<p>A.16.11 A.16.12 A.16.14 A.16.15 A.16.16 A.16.17</p>	<p>CC7.4 CC7.5</p>		<p>314.3(b)(2) 314.4(b)(3)</p>	

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Incident Response	Incident Response	Incident Response	[The organization] responds to confirmed incidents and resolution is tracked with authorized management channels. If applicable, [the organization] coordinates the incident response with business contingency activities.	A.16.1.1 A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7	CC4.2 CC5.1 CC5.2 CC7.4 CC7.5		314.3(b)(2) 314.4(b)(3)	
Incident Response	Incident Communication	External Communication of Incidents	[The organization] defines external communication requirements for incidents, including: <ul style="list-style-type: none"> • information about external party dependencies • criteria for notification to external parties as required by [the organization] policy in the event of a security breach • contact information for authorities (e.g, law enforcement, regulatory bodies, etc.) • provisions for updating and communicating external communication requirement changes 	A.6.1.3				
Incident Response	Incident Communication	Incident Reporting Contact Information	[The organization] provides a contact method for external parties to: <ul style="list-style-type: none"> • submit complaints and inquiries • report incidents 	A.16.1.2	CC2.3			
Network Operations	Perimeter Security	Network Policy Enforcement Points	Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance to identified	A.13.1.1	CC6.6			FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
			security requirements and business justifications.					
Network Operations	Network Segmentation	Network Segmentation	Production environments are logically segregated from non-production environments.	A.12.14 A.13.13 A.14.2.6				
People Resources	On-boarding	Background Checks	New hires are required to pass a background check as a condition of their employment.	A.7.1.1	CC1.1 CC1.4 CC1.5			
People Resources	Off-boarding	Property Collection	Upon employee termination, management is notified to collect [the organization] property from the terminated employee.	A.7.3.1 A.8.1.4 A.9.2.1 A.9.2.2 A.9.2.6				
People Resources	Compliance	Disciplinary Process	Employees that fail to comply with [the organization] policies are subject to a disciplinary process.	A.7.2.3				
Risk Management	Risk Assessment	Risk Assessment	[The organization] management performs a risk assessment [in accordance with an organization-defined frequency]. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.		CC3.1 CC3.2 CC3.3 CC3.4 CC5.1 CC5.2		314.4(b)(1) 314.4(b)(2) 314.4(b)(3)	

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Risk Management	Risk Assessment	Self-Assessments	Management assesses the design and operating effectiveness of internal controls against the established controls framework. Corrective actions related to identified deficiencies are tracked to resolution.	A.12.7.1 A.18.2.2 A.18.2.3	CC1.2 CC3.2 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2			
Risk Management	Internal and External Audit	Internal Audits	[The organization] establishes internal audit requirements and executes audits on information systems and processes [in accordance with an organization-defined frequency].	A.12.7.1 A.18.2.1 A.18.2.2 A.18.2.3	CC1.2 CC3.2 CC3.4 CC4.1 CC4.2 CC5.1 CC5.2		314.4(c)	
Risk Management	Internal and External Audit	ISMS Internal Audit Requirements	Internal audit establishes and executes a plan to evaluate applicable controls in the Information Security Management System (ISMS) at least once every 3 years.					
Risk Management	Controls Implementation	Remediation Tracking	Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.		CC4.2 CC5.1 CC5.2		314.4(c)	
Risk Management	Controls Implementation	ISMS Corrective Action Plans	Management prepares a Corrective Action Plan (CAP) to manage the resolution of nonconformities identified in independent audits.					

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Risk Management	Controls Implementation	Statement of Applicability	Management prepares a statement of applicability that includes control objectives, implemented controls, and business justification for excluded controls. Management aligns the statement of applicability with the results of the risk assessment.	A.18.1.1				
System Design Documentation	Internal System Documentation	System Documentation	Documentation of system boundaries and key aspects of their functionality are published to authorized personnel.		CC2.3			
System Design Documentation	Customer-facing System Documentation	Whitepapers	[The organization] publishes whitepapers that describe the purpose, design, and boundaries of the system and system components.		CC2.3			
Security Governance	Policy Governance	Policy and Standard Review	[The organization's] policies and standards are reviewed, approved by management, and communicated to authorized personnel [in accordance with an organization-defined frequency].	A.5.1.1 A.5.1.2	CC1.4 CC5.3			
Security Governance	Policy Governance	Exception Management	[The organization] reviews exceptions to policies, standards, and procedures; exceptions are documented and approved based on business need and removed when no longer required.	A.5.1.1				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Security Governance	Security Documentation	Information Security Program Content	[The organization] has an established governance framework that supports relevant aspects of information security with policies.	A.10.1.1 A.11.2.9 A.13.2.1 A.5.1.1 A.6.1.1 A.6.1.5 A.6.2.1 A.6.2.2 A.9.1.1	CC1.1 CC1.2 CC1.3 CC2.2 CC2.3 CC3.1 CC3.2 CC5.1 CC5.2		314.3(a)	
Security Governance	Security Documentation	Procedures	[The organization's] key business functions and information security capabilities are supported by documented procedures that are communicated to authorized personnel.	A.12.1.1	CC1.4 CC2.1 CC2.3 CC3.1 CC3.2 CC5.1 CC5.2			
Security Governance	Workforce Agreements	Proprietary Rights Agreement	[Workforce personnel as defined by the organization] consent to a proprietary rights agreement.	A.13.2.4 A.18.1.2				
Security Governance	Workforce Agreements	Review of Confidentiality Agreements	[The organization's] proprietary rights agreement and network access agreement are reviewed [in accordance with an organization-defined frequency].	A.13.2.4 A.18.1.2				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Security Governance	Information Security Management System	Information Security Program	[The organization] has an established security leadership team including key stakeholders in [the organization's] Information Security Program; goals and milestones for deployment of the information security program are established and communicated to the company.				314.4(a)	
Security Governance	Information Security Management System	Information Security Management System Scope	Information Security Management System (ISMS) boundaries are formally defined in an ISMS scoping document.	A.6.1.1 A.6.1.5 A.18.2.1			314.4(b)(3)(e)	
Security Governance	Information Security Management System	Security Roles & Responsibilities	Roles and responsibilities for the governance of information security within [the organization], including the parties responsible for executing the objectives of the Information Security Management System, are formally documented and communicated by management.	A.6.1.1	CC1.1 CC1.4 CC1.5 CC2.2 CC2.3			
Security Governance	Information Security Management System	Information Security Resources	Information systems security implementation and management is included as part of the budget required to support [the organization's] security program.	A.6.1.5				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Security Governance	Information Security Management System	Management Review	The Information Security Management System (ISMS) steering committee conducts a formal management review of ISMS scope, risk assessment activities, control implementation, and audit results [in accordance with an organization-defined frequency].					
Service Lifecycle	Release Management	Service Lifecycle Workflow	<p>System implementations or software releases are subject to the Service Life Cycle (SLC), including documentation and execution of:</p> <ul style="list-style-type: none"> • establishment and segregation of roles and responsibilities (i.e., development, test, approval, and release are performed by specified parties) • details of implementation/release requirements • functional testing of requirements • security testing and approval • legal review and approval • management consideration of test results and approval prior to release/implementation • mechanisms are in place to ensure that the deployed code is the same code that has been approved for deployment 	A.12.5.1 A.14.1.1 A.14.2.1 A.14.2.2 A.14.2.3 A.14.2.5 A.14.2.8 A.14.2.9 A.18.1.4 A.6.1.5	CC8.1			

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Service Lifecycle	Source Code Management	Source Code Management	Source code is managed with [the organization]-approved version control mechanisms.	A.14.2.6				
Systems Monitoring	Logging	Audit Logging	[The organization] logs critical information system activity.	A.12.4.1	CC7.2		314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)
Systems Monitoring	Security Monitoring	Security Monitoring Alert Criteria	[The organization] defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	A.12.4.3	CC3.2 CC3.3 CC3.4 CC5.1 CC5.2 CC7.2		314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)
Systems Monitoring	Security Monitoring	Log-tampering Detection	[The organization] monitors and flags tampering to the audit logging and monitoring tools in the production environment.	A.12.4.2				
Systems Monitoring	Security Monitoring	System Security Monitoring	Critical systems are monitored in accordance to predefined security criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	A.12.4.3	CC3.2 CC3.3 CC3.4 CC4.2 CC5.1 CC5.2 CC6.1 CC7.2 CC7.3		314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Systems Monitoring	Availability Monitoring	Availability Monitoring Alert Criteria	[The organization] defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.	A.12.13 A.17.2.1	CC7.2	A1.1		
Systems Monitoring	Availability Monitoring	System Availability Monitoring	Critical systems are monitored in accordance to predefined availability criteria and alerts are sent to authorized personnel. Confirmed incidents are tracked to resolution.	A.12.13 A.17.2.1	CC7.2	A1.1		
Site Operations	Physical Security	Secured Facility	Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points, and/or manned reception desks.	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1	CC6.4			FERPA_99.31(a)
Site Operations	Physical Security	Physical Protection and Positioning of Cabling	[The organization] power and telecommunication lines are protected from interference, interception, and damage.	A.11.2.3				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Site Operations	Physical Access Account Lifecycle	Provisioning Physical Access	Physical access provisioning to a [the organization] datacenter requires management approval and documented specification of: <ul style="list-style-type: none"> • account type (e.g, standard, visitor, or vendor) • access privileges granted • intended business purpose • visitor identification method, if applicable • temporary badge issued, if applicable • access start date • access duration 	A.11.1.2	CC6.4			FERPA_99.31(a)
Site Operations	Physical Access Account Lifecycle	De-provisioning Physical Access	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 facility.	A.11.1.2	CC6.4			FERPA_99.31(a)
Site Operations	Physical Access Account Lifecycle	Periodic Review of Physical Access	[The organization] performs physical access account reviews [in accordance with an organization-defined frequency]; corrective action is take where applicable.	A.11.1.2	CC6.4			FERPA_99.31(a)
Site Operations	Physical Access Account Lifecycle	Physical Access Role Permission Authorization	Initial permission definitions, and changes to permissions, associated with physical access roles are approved by authorized personnel.	A.11.1.5 A.11.1.6	CC6.4			FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Site Operations	Physical Access Account Lifecycle	Monitoring Physical Access	Intrusion detection and video surveillance are installed at [the organization] datacenter locations; confirmed incidents are documented and tracked to resolution.	A.11.2.1				
Site Operations	Environmental Security	Temperature and Humidity Control	Temperature and humidity levels of datacenter environments are monitored and maintained at appropriate levels.	A.11.1.4 A.11.2.1 A.11.2.2		A1.2		
Site Operations	Environmental Security	Fire Suppression Systems	Emergency responders are automatically contacted when fire detection systems are activated; the design and function of fire detection and suppression systems are maintained [in accordance with an organization-defined frequency].	A.11.1.4 A.11.2.1		A1.2		
Site Operations	Environmental Security	Power Failure Protection	[The organization] employs uninterruptible power supplies (UPS) and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified [in accordance with an organization-defined frequency].	A.11.2.2				
Training and Awareness	General Awareness Training	General Security Awareness Training	[Workforce personnel as defined by the organization] complete security awareness training, which includes 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.	A.16.1.2 A.16.1.3 A.7.2.1 A.7.2.2	CC1.1 CC1.4 CC1.5 CC2.2 CC2.3		314.4(b)(1)	

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Training and Awareness	General Awareness Training	Code of Conduct Training	[Workforce personnel as defined by the organization] complete a code of business conduct training.	A.11.2.8 A.7.1.2 A.7.2.1 A.8.1.3	CC1.1 CC1.4 CC1.5			
Third Party Management	Vendor Assessments	Third Party Assurance Review	[In accordance with an organization-defined frequency], 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 impact the disclosed gaps have on the organization.	A.15.2.1	CC3.2 CC3.3 CC3.4 CC5.1 CC5.2 CC9.2		314.4(d)(1) 314.4(d)(2)	
Third Party Management	Vendor Assessments	Vendor Risk Assessment	[The organization] performs a risk assessment to determine the data types that can be shared with a managed service provider.	A.13.2.2 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.2	CC9.2		314.4(d)(1) 314.4(d)(2)	
Third Party Management	Vendor Agreements	Network Access Agreement: Vendors	Third party entities which gain access to [the organization's] network sign a network access agreement.	A.13.2.4 A.18.1.2				

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Third Party Management	Vendor Agreements	Vendor Non-disclosure Agreements	[Workforce personnel as defined by the organization] consent to a non-disclosure clause.	A.13.2.2 A.14.2.7 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.2			314.4(d)(2)	
Third Party Management	Vendor Agreements	Network Service Level Agreements	Vendors providing networking services to the organization are contractually bound to provide secure and available services as documented in service level agreements.	A.13.1.2				
Vulnerability Management	Production Scanning	Vulnerability Scans	[The organization] conducts vulnerability scans against the production environment; scan tools are updated prior to running scans.	A.12.6.1	CC7.1		314.4(b)(2)	FERPA_99.31(a)
Vulnerability Management	Penetration Testing	Penetration Testing	[In accordance with an organization-defined frequency], [the organization] conducts external penetration tests.	A.12.6.1	CC7.1		314.4(b)(2)	FERPA_99.31(a)
Vulnerability Management	Patch Management	Infrastructure Patch Management	[The organization] installs security-relevant patches, including software or firmware updates; identified end-of-life software must have a documented decommission plan in place before the software is removed from the environment.		CC7.1		314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

The Common Controls Framework by Adobe

Domain	Subdomain	Control Short Name	Common Control Activity	ISO/IEC 27001 Annex A Ref#	SOC – Common Criteria Ref#	SOC – Availability Ref#	GLBA Ref#	FERPA Ref#
Vulnerability Management	Malware Protection	Enterprise Antivirus	If applicable, [the organization] has managed enterprise antivirus deployments and ensures the following: <ul style="list-style-type: none"> • signature definitions are updated • full scans are performed [in accordance with an organization-defined frequency] and real-time scans are enabled • alerts are reviewed and resolved by authorized personnel 	A.12.2.1	CC6.8 CC7.1			FERPA_99.31(a)
Vulnerability Management	Code Security	Code Security Check	[In accordance with an organization-defined frequency], [the organization] conducts source code checks for vulnerabilities.	A.14.2.1 A.14.2.5	CC7.1 CC8.1			
Vulnerability Management	External Advisories and Inquiries	External Information Security Inquiries	[The organization] reviews information-security-related inquiries, complaints, and disputes.		CC7.1			
Vulnerability Management	External Advisories and Inquiries	External Alerts and Advisories	[The organization] reviews alerts and advisories from management approved security forums and communicates verified threats to authorized personnel.	A.16.1.1 A.6.1.4				
Vulnerability Management	Program Management	Vulnerability Remediation	[The organization] assigns a risk rating to identified vulnerabilities and prioritizes remediation of legitimate vulnerabilities according to the assigned risk.	A.12.6.1	CC7.4 CC7.5		314.4(c)	FERPA_99.31(a)

Copyright © 2010-2015 Adobe Systems Incorporated. All rights reserved



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License