The Common Controls Framework

BY ADOBE

The following table contains the baseline security subset (derived from The Common Controls Framework by Adobe) of control activities that apply to Adobe's enterprise service offerings. The control activities help Adobe enterprise offerings meet the requirements of ISO/IEC 27001, AICPA Trust Service Criteria - Common Criteria (TSC - CC), AICPA Trust Service Criteria - Availability ("TSC - A"), FedRAMP Tailored baseline ("Fedramp Tailored"), PCI DSS, as well as the security requirements of GLBA, FERPA, and HIPAA Security Rule. 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.

Following are the requirements that are not mapped to CCF:
HIPAA Security Rule: 164.308(a)(4)(ii)(A) - Adobe is not a health care Clearing house
FedRAMP Tailored: PE-15, SC-20, SA-4(10) - Adobe's FedRAMP certified services have aditional control activities to meet with these requirements.

Control Family	Control Sub-Family	Control Short Name	Common Control Activity	ISO/IEC 27001 ISMS Ref#	ISO/IEC 27001 Annex A Ref#	TSC - Common Criteria	TSC - Availability	FedRAMP Tailored Ref#	PCI DSS V3.2.1 Ref#	GLBA Ref#	FERPA Ref#	BSI CS	HIPPA Security
Asset Management	Device and Media Inventory	Inventory Management	[The organization] maintains an inventory of system devices, which is reconciled [in accordance with the organization-defined frequency].		A.8.1.1	CC6.1		CM-8	9.6.1 9.7 9.7.1			AM-01	
Asset Management	Device and Media Inventory	Inventory Management: Payment Card Systems	[The organization's] asset inventory includes in-scope cardholder related systems, devices, and media.						11.1.1 12.3.4 2.4 9.6.1 9.7 9.9.1				
Asset Management	Device and Media Inventory	Inventory Labels	[The organization's] assets are labelled and have designated owners.		A.8.1.2	CC6.1			12.3.3 9.6.1			AM-02 AM-06	
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	CC6.5		MA-2 PE-8				AM-08 AM-04	164.310(d)(1) 164.310(d)(2)(iii)
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	CC6.5		MA-2	9.5 9.6 9.6.2 9.6.3 9.6.3 9.7				164.310(d)(1) 164.310(d)(2)(iii)
Asset Management	Device and Media Transportation	Use of Portable Media	The use of portable media in [the organization] datacenters is prohibited unless explicitly authorized by management.			CC6.7							
Asset Management	Component Installation and Maintenance	Maintenance of Assets	Equipment maintenance is documented and approved according to management requirements.		A.11.2.4		A1.2	MA-2 MA-4				PS-04 PS-05 BCM-05	164.310(a)(2)(iv)
Asset Management	Component Installation and Maintenance	Tampering of Payment Card Capture Devices	Devices that physically capture payment card data are inspected for evidence of tampering [in accordance with the organization-defined frequency].						9.9 9.9.2 A2.1				
Business Continuity	Business Continuity Planning	Business Continuity Plan	[The organization's] business contingency plan is reviewed, approved by management and communicated to relevant team members [in accordance with the organization-defined frequency].		A.17.1.1 A.17.1.2	CC7.4 CC7.5 CC9.1	A1.2		12.10.1			BCM-01 BCM-02 BCM-03 BCM-04 BCM-05	164.308(a)(7)(i) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C)
Business Continuity	Business Continuity Planning	Business Continuity Plan: Personal Health Information	[The organization] Business Contingency Plan addresses how to access facilities and obtain data during an emergency.										164.308(a)(7)(i) 164.310(a)(2)(i) 164.312(a)(2)(ii)

Business Continuity	Business Continuity Planning	Business Continuity Plan: Roles and Responsibilities	Business contingency roles and responsibilities are assigned to individuals and their contact information is communicated to authorized personnel.					IA-2					
Business Continuity	Business Continuity Planning	Continuity Testing	[The organization] performs business contingency and disaster recovery tests [in accordance with the organization-defined frequency] and ensures the following: • 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.17.1.2 A.17.1.3	CC7.4 CC7.5 CC9.1	A1.2 A1.3					BCM-01 BCM-02 BCM-04 BCM-05	164.308(a)(7)(i) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i)
Business Continuity	Business Continuity	Business Impact Analysis	[The organization] identifies the business impact of relevantthreats to assets, infrastructure,and resources that supportcritical business functions.Recovery objectives areestablished for critical businessfunctions.		A.17.1.1 A.17.1.2	CC7.4 CC7.5 CC9.1	A1.2	CP-9				BCM-01 BCM-02 BCM-03	164.308(a)(7)(ii)(E)
Business Continuity	Capacity Management	Capacity Forcasting	Budgets for infrastructure capacity are established based on analysis of historical business activity and growth projections; purchases are made against the established budget and plans are updated on a [in accordance with the organization-defined frequency].		A.12.1.3			SA-2				RB-01	
Backup Management	Backup	Backup Configuration	[The organization] configures redundant systems or performs data backups [in accordance with the organization-defined frequency] to resume system operations in the event of a system failure.		A.18.1.3	CC7.5 CC9.1	A1.2	CP-9	12.10.1			RB-06 RB-07 RB-08	164.308(a)(7)(ii)(A) 164.310(d)(2)(iv)
Backup Management	Backup	Resilience Testing	[The organization] performs backup restoration or failover tests [in accordance with the organization-defined frequency] to confirm the reliability and integrity of system backups or recovery operations.		A.12.3.1	CC7.4 CC7.5 CC9.1	A1.2 A1.3		12.10.1			RB-06 RB-07 RB-08 RB-09	164.308(a)(7)(ii)(B)
Backup Management	Backup	Alternate Storage	[The organization] backups are securely stored in an alternate location from source data.						9.5.1				
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 the organization-defined frequency].		A.12.5.1	CC6.8 CC7.1 CC7.5 CC8.1		CA-3 CM-2 CM-6	1.1 1.1.4 1.1.6 1.2 1.2.2 2.1 2.1.1 2.2 2.2.2 2.2.3 2.2.4 2.2.5 5.3	314.4(b)(3)	FERPA_99.31(a)	RB-22	164.306(a)(2)
Configuration Management	Baseline Configurations	Default "Deny- all" Settings	Where applicable, the information system default access configurations are set to "deny-all."						7.2 7.2.1 7.2.3				
Configuration Management	Baseline Configurations	Configuration Checks	[The organization] uses mechanisms to detect deviations from baseline configurations in production environments.		A.9.4.4 A.12.5.1	CC6.8		CM-6 CM-7	1.2.2 10.4.2 11.4 11.5 11.5.1 5.3	314.4(b)(3)	FERPA_99.31(a)	IDM-12 KOS-01 RM-22	164.306(a)(2)

Configuration Management	Baseline Configurations	Configuration Checks Reconciliation: CMDB	[The organization] reconciles the established device inventory against the enterprise log repository [in accordance with the organization-defined frequency]; devices which do not forward security configurations are remediated.							314.4(b)(3)	FERPA_99.31(a)		164.306(a)(2)
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			AU-5 AU-6	10.4 10.4.1 10.4.2 10.4.3				
Configuration Management	Baseline Configurations	Time Clock Configuration Access	Access to modify time data is restricted to authorized personnel.						10.4 10.4.2				
Configuration Management	Baseline Configurations	Default Device Passwords	Vendor-supplied default passwords are changed according to [the organization] standards prior to device installation on the [the organization] network or immediately after software or operating system installation.					IA-5	2.1 2.1.1				
Configuration Management	Baseline Configurations	Process Isolation	[The organization] implements only one primary function per server within the production environment; the information system maintains a separate execution domain for each executing process.						2.2.1				
Change Management	Change Management	Change Management Workflow	Change scope, change type, and roles and responsibilities are pre-established and control workflow; notification and approval requirements are also pre-established based on risk associated with change scope and type.		A.12.1.2 A.12.6.2 A.14.2.1 A.14.2.2 A.14.2.4	CC2.2 CC6.8 CC7.1 CC8.1		SA-3	1.1.1 10.4.2 6.4 6.4.5 6.4.5.1 6.4.5.2 6.4.5.3 6.4.5.4 6.4.6		FERPA_99.31(a)	BEI-01 BEI-02 BEI-03 BEI-04 BEI-05 BEI-06 BEI-07 BEI-08 BEI-09 BEI-10 BEI-11 BEI-12	
Change Management	Change Management	Change Approval	Prior to introducing changes into the production environment, approval from authorized personnel is required based on the following: • change description • impact of change • test results • back-out procedures		A.12.5.1 A.14.2.3 A.14.2.4 A.14.2.8 A.14.2.9	CC7.1 CC8.1		CA-9 CM-4 CM-6	1.1.1 10.4.2 6.3.2 6.4 6.4.5 6.4.5.1 6.4.5.2 6.4.5.3 6.4.5.4 6.4.6		FERPA_99.31(a)	BEI-01 BEI-02 BEI-07 BEI-08	
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	CC5.1 CC6.3 CC6.8			6.4.2 6.4.6			IDM-06 BEI-11 BEI-12	
Change Management	Change Communication	Communication of Maintenance and Downtime	Customer-impacting product and system changes are publicly communicated on the company website.			CC2.2 CC2.3							
Data Management	Data Classification	Data Classification Criteria	[The organization's] data classification criteria are reviewed, approved by management, and communicated to authorized the organization-defined frequency]; the data security 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	CC3.2 CC6.1 CC6.5 CC8.1		MP-6 RA-2 SI-1 SI-12	9.6.1	314.3(b)(1)		AM-05 AM-06 AM-07	
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.								FERPA_99.31(a)		
Data Management	Choice and Consent	Notice of Personal Information Disclosure	In accordance with [the organization] policy, [the organization] provides notice to individuals regarding legally-required disclosures of personal information.			CC2.3							

Data Management	Data Handling	External Privacy Inquiries	In compliance 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				6.4.3				
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		IA-5(1) IA-7 SC-12 SC-13	2.3 4.1 4.1.1 8.2.1 A2.3	31.4.3(b)(1) 31.4.3(b)(2) 31.4.3(b)(3)	FERPA_99.31(a)	AM-08 BEI-01 COM-01 KOS-07 KRY-01 KRY-02 KRY-03 KRY-04 PI-04 PI-05	164.306(a)(1) 164.306(a)(2) 164.306(a)(3) 164.312(a)(2)(iv) 164.312(c)(1) 164.312(c)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii)
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.8.2.3 A.18.1.4 A.18.1.5	CC6.1 CC6.7		SC-12 SC-13	3.4 3.5 3.5.3 3.6 3.6.3 8.2.1			KRY-01 KRY-02 KRY-03	164.306(a)(1) 164.306(a)(2) 164.306(a)(3) 164.312(a)(2)(iv) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(ii)
Data Management	Data Encryption	Approved Cryptographic Technology	Where applicable, strong industry standard cryptographic ciphers and keys with an effective strength greater than 112 bits are required for cryptographic security operations.					SC-12 SC-13	2.3 3.6 3.6.1 4.3 8.2.1 A2.2				
Data Management	Data Storage	Credit Card Data Restrictions	[The organization] does not store full track credit card data, credit card authentication information, credit card verification code, or credit personal identification number (PIN) which [the organization] processes for payment.						3.2 3.2.1 3.2.2 3.2.3				
Data Management	Data Storage	Personal Account Number Data Restrictions	[The organization] restricts personal account number (PAN) data such that only the first six and last four digits are displayed; authorized users with a legitimate business need may be provided the full PAN.						3.3				
Data Management	Data Integrity	Changes to Data at Rest	[The organization] uses mechanisms to detect direct changes to the integrity of customer data and personal information; [the organization] takes action to resolve confirmed unauthorized changes to data.						11.5				
Data Management	Data Removal	Secure Disposal of Media	[The organization] securely erases media containing decommissioned [Restricted organization's data classification criteria)] data and obtains a certificate or log of erasure; media pending erasure are stored within a secured facility.		A.8.3.2 A.11.2.7	CC6.5		MA-2 MP-6	9.8 9.8.1 9.8.2			AM-07 PI-05	164.310(d)(2)(i)
Data Management	Data Removal	Customer Data Retention and Deletion	[The organization] purges or archives data according to customer requests or legal and regulatory mandates.						3.1			PI-02	164.310(d)(2)(i)
Data Management	Data Removal	Removal of PHI from Media	[The organization] removes electronic protected health information from electronic media if the media is made available for re-use.										164.310(d)(2)(ii)
Data Management	Social Media	Social Media	Sharing [the organization] [restricted (as defined by the organization's data classification criteria)] data via messaging technologies, social media, and public websites is prohibited.						4.2				

Entity Management	Board of Directors	Board of Directors Structure and Purpose	The Board of Directors provides corporate oversight, strategic direction, and review of management for [the organization] The Board of Directors meets at least [organization-defined frequency] and has 3 sub-committees: - Audit Committee - Executive Compensation and Nominating Committee - Governance Committee	5.1		CC1.1 CC1.2 CC1.5 CC2.2							
Entity Management	Board of Directors	Audit Committee	The Audit Committee is governed by a Charter, is independent from [the organization] Management, is composed of outside directors (Industry Experts), and meets [organization-defined frequency] . The Audit Committee oversees: -Financial Statement Quality -Enterprise Risk Management -Regulatory & Legal Compliance -Internal Audit Functions -Information Security Functions -External Audit Functions	5.1 5.3		CC1.2 CC1.5 CC2.1 CC2.2							
Entity Management	Strategic Planning	Organizational Structure	[The organization] Management ensures that its organization is aligned with the corporate strategy by assigning key managers with responsibilities to execute the corporate strategy.	5.1a		CC1.1 CC1.2 CC1.3 CC1.5 CC2.2							
Entity Management	Strategic Planning	Operating Plans	Annual operating plans are aligned with Corporate Objectives, which are established on an annual basis during the Company's planning process. Priorities are set and plans are communicated appropriately.	5.1a 7.1		CC1.5							
Entity Management	Strategic Planning	Cyber Security Insurance	[The organization] purchases cyber security insurance to mitigate risk of material financial impact that could result from a cyber security event.	7.1		CC9.1							
Entity Management	Internal Audit Oversight	Internal Audit Function	[Organization-defined frequency] , the Chief Audit Executive meets with the Audit Committee to review key risk issues. The Audit Committee approves the annual Internal Audit Plan. Results of [organization-defined frequency] audits and subsequent issue tracking summaries are presented to the Audit Committee.	9.2		CC1.5 CC2.1 CC2.2 CC3.1 CC4.1							
Entity Management	Internal Audit Oversight	Financial Control Review	Internal financial control assessment results are reported to the Audit Committee by the Chief Audit Executive on a [in accordance with the organization-defined frequency] and support the CEO/CFO 302/404 certifications.	9.2		CC3.1							
Entity Management	Internal Audit Oversight	Anti-fraud Program	[The organization]'s anti-fraud program encompasses both entity-level (Code of Conduct, Hotline, Background Checks, AC oversight, etc.) and process-level controls (including IT controls) embedded with [The organization]'s process design of ICOFR			CC1.5 CC3.3							
Entity Management	Information Security Oversight	Information Security Function	[In accordance with the organization-defined frequency], the Chief Security Officer meets with the Audit Committee to review key Information Security issues. Results of continuous monitoring activities and current security compliance status are presented to the Audit Committee and the Board of Directors.	9.3		CC2.2 CC2.3						SPN-01	
Entity Management	Information Security Oversight	Information Security Compliance Review	Information Security compliance results are reported to the Audit Committee by the Chief Security Officer on a [in accordance with the organization-defined frequency] and support information security compliance certifications			CC3.1 CC4.1 CC4.2						SPN-01	

Identity and Access Management	Logical Access Account Lifecycle	Logical Access Provisioning	Logical access provisioning to information systems requires approval from appropriate personnel.		A.9.2.1 A.9.2.2 A.9.2.3 A.9.4.1 A.12.5.1 A.18.1.3	CC6.1 CC6.2 CC6.3 CC8.1		AC-17 AC-2 CP-9 IA-4 IA-5 MP-2 PS-4	7.1.4 8.1.2	314.3(b)(3)	FERPA_9931(a)	IDM-01 IDM-02 IDM-03 IDM-05 IDM-06 IDM-09 IDM-10 IDM-11 IDM-12 IDM-13	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(1)
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.9.2.3 A.9.4.1 A.9.2.6 A.18.1.3	CC6.1 CC6.2 CC6.3 CC9.2		AC-2 AC-17 PS-4	8.1.2 8.1.3 8.1.4	314.3(b)(3)	FERPA_9931(a)	HR-05 IDM-04	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(ii)(C)
Identity and Access Management	Logical Access Account Lifecycle	Terminations: People Resources Notification	The People Resources system sends a notification to relevant personnel in the event of a termination of an information system user.					PS-4					
Identity and Access Management	Logical Access Account Lifecycle	Logical Access Review	[The organization] performs account and access reviews [in accordance with the organization-defined frequency]; corrective action is taken where applicable.		A.9.2.3 A.9.4.1 A.9.2.5 A.18.1.3	CC6.1 CC6.2 CC6.3		AC-2 IA-5 PS-5	7.1	314.3(b)(3)	FERPA_9931(a)	IDM-05	164.308(a)(1)(ii)(D) 164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(ii)(C)
Identity and Access Management	Logical Access Account Lifecycle	Role Change: Access De- provisioning	Upon notification of an employee reassignment or transfer, management reviews the employee's access for appropriateness. Access that is no longer required is revoked and documented.					PS-5	8.1.2				
Identity and Access Management	Logical Access Account Lifecycle	Shared Logical Accounts	[The organization] restricts the use of shared and group authentication credentials. Authentication credentials for shared and group accounts are reset [in accordance with the organization-defined frequency].								FERPA_9931(a)		
Identity and Access Management	Logical Access Account Lifecycle	Shared Account Restrictions	Where applicable, the use of generic and shared accounts to administer systems or perform critical functions is prohibited; generic user IDs are disabled or removed.						8.5				
Identity and Access Management	Authentication	Unique Identifiers	[The organization] requires unique identifiers for user accounts and prevents identifier reuse.		A.9.4.1 A.9.4.2	CC6.1		IA-4 IA-5	8.1.1 8.6	314.3(b)(3)	FERPA_9931(a)	IDM-08 IDM-10	164.312(a)(2)(i) 164.312(d)
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 the organization-defined frequency].		A.9.1.2 A.9.4.1 A.9.4.2 A.9.4.3	CC6.1		IA-4 IA-5 IA-5 (1)	8.2 8.2.3 8.2.4 8.2.5 8.2.6 8.6	314.3(b)(3)	FERPA_9931(a)	IDM-11	164.308(a)(5)(ii)(d)
Identity and Access Management	Authentication	Multifactor Authentication	Multi-factor authentication is required for: • remote sessions • access to environments that host production systems		A.9.4.1 A.9.4.2 A.11.2.6	CC6.1 CC6.6		AC-2 AC-20 IA-2 (1) IA-2(12) IA-5 IA-5(11) IA-8 IA-8(1) IA-8(2) IA-8(3) IA-8(4) MA-4	8.3 8.3.1 8.3.2			IDM-08 IDM-11	164.312(d)

Identity and Access Management	Authentication Maintenance	Authentication Credential	Authorized personnel verify the identity of users before modifying authentication credentials on their behalf.		A.9.2.4 A.9.3.1	CC6.1		IA-5 IA-5(1)	8.2.2			IDM-07 IDM-08	164.308(a)(5)(ii)(D)
Identity and Access Management	Authentication	Session Timeout	Information systems are configured to terminate inactive sessions after [the organization-defined duration] or when the user terminates the session.					MA-4	12.3.8 8.1.8				164.312(a)(2)(iii)
Identity and Access Management	Authentication	Session Limit	Information systems are configured to limit concurrent login sessions and the inactive user interface is not displayed when the session is terminated.					AC-7					
Identity and Access Management	Authentication	Account Lockout: Cardholder Data Environments	Users are locked out of information systems after [the organization-defined number] of invalid attempts for a minimum of [the organization- defined duration], or until an administrator enables the user ID.						8.1.6 8.1.7				
Identity and Access Management	Authentication	Account Lockout	Users are locked out of information systems after multiple, consecutive invalid attempts within a defined period; Accounts remain locked for a defined period.					AC-2					
Identity & Access Management	Authentication	Privileged Session Management	Privileged logical access to trusted data environments is enabled through an authorized session manager; session user activity is recorded and tunnelling to untrusted data environments is restricted.			CC6.7 CC7.1		IA-2(12) IA-5(11) IA-8 IA-8(1) IA-8(2) IA-8(3) IA-8(4)					
Identity and Access Management	Authentication	Full Disk Encryption	Where full disk encryption is used, logical access must be managed independently of operating system authentication; decryption keys must not be associated with user accounts.						3.4.1				
Identity and Access Management	Authentication	Login Banner	Systems leveraged by the U.S. Federal Government present a login screen that displays the following language: • users are accessing a U.S. Government information system • system usage may be monitored, recorded, and subject to audit • unauthorized use of the system is prohibited and subject to criminal and civil penalties • use of the system indicates consent to monitoring and recording					AC-7					
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.						7.1 7.1.1 7.1.2 7.1.3 7.2 7.2.1 7.2.2 7.2.3 8.7				

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	Role-Based Logical Access	Service Account Restrictions	Individual user or administrator use of service accounts for O/S, applications, and databases is prohibited.						8.7				
Identity and Access Management	Role-Based Logical Access	PCI Account Restrictions	[The organization] clients with access to the cardholder data environment (CDE), as users or processes, are assigned unique accounts that cannot modify shared binaries or access data, server resources, or scripts owned by another CDE or [the organization]; application processes are restricted from operating in privileged-mode.						A.1 A.1.1 A.1.2				
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	CC6.1		AC-20 MA-4			FERPA_99.31(a)		164.312(d)
Identity and Access Management	Remote Access	Ability to Disable Remote Sessions	[The organization] has a defined process and mechanisms in place to expeditiously disable or disconnect remote access to information systems within a defined time frame based on business need.						12.3 12.3.8				
Identity and Access Management	Remote Access	Remote Maintenance: Authentication Sessions	Vendor accounts used for remote access are enabled only during the time period needed, disabled when not in use, and monitored while in use.						12.3.9 8.1.5				
Identity and Access Management	Remote Access	Remote Maintenance: Unique Authentication Credentials for each Customer	Where applicable, Service providers with remote access to customer premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.						8.5.1				
Identity and Access Management	End-user Authentication	End-user Environment Segmentation	Where applicable, processes that run as part of an [the organization] shared hosting platform will run under unique credentials that permit access to only one customer environment.						A.1.1 A.1.2				
Identity and Access Management	End-user Authentication	End-user Access to Applications and Data	[The organization] applications secure user data and maintain confidentiality by default or according to permissions set by the individual; [the organization] authenticates individuals with unique identifiers and passwords prior to enabling access to: • use the application • view or modify their own data								FERPA_99.33(a)(1)		
Identity and Access Management	Key Management	Key Repository Access	Access to the cryptographic keystores is limited to authorized personnel.		A.10.1.2 A.18.1.5	CC6.1 CC6.7			3.5 3.5.2 3.6 3.6.2 3.6.3		FERPA_99.31(a)	KRY-02 KRY-04	

Identity and Access Management	Key Management	Data Encryption Keys	[The organization] changes shared data encryption keys - at the end of the [organization-defined lifecycle period] - when keys are compromised - upon termination/transfer of employees with access to the keys		A.10.1.2 A.18.1.5	CC6.1 CC6.7		PS-4 PS-5	3.6 3.6.4 3.6.5 3.6.7				
Identity and Access Management	Key Management	Key Maintenance	Cryptographic keys are invalidated when compromised or at the end of their defined lifecycle period.						3.6 3.6.4 3.6.5 3.6.7				
Identity and Access Management	Key Management	Clear Text Key Management	If applicable, manual clear-text cryptographic key- management operations must be managed using split knowledge and dual control.						3.6 3.6.6				
Identity and Access Management	Key Storage and Distribution	Key Store Review	Management reviews and authorizes key store locations.						3.5 3.5.4				
Identity and Management	Key Storage and Distribution	Storage of Data Encryption Keys	Storage of data encryption keys that encrypt or decrypt cardholder data meet at least one of the following: • the key-encrypting key is at least as strong as the data encrypting key and is stored separately from the data encrypting key • stored within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of interaction device) • keys are stored as at least two full-length key components or key shares						3.5 3.5.3 3.6 3.6.1 3.6.3				
Identity and Access Management	Key Storage and Distribution	Clear Text Distribution	[The organization] prohibits the distribution of cryptographic keys in clear text.						3.6 3.6.2				
Incident Response	Incident Response	Incident Response Plan	[The organization] defines the types of incidents that need to be managed, tracked and reported, including: • 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 frequency], or when major changes to the organization occur		A.16.1.1 A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7	CC2.2 CC7.2 CC7.3 CC7.4 CC7.5 CC8.1		IR-4 IR-6 IR-7 IR-8	11.1.2 11.5.1 12.10 12.10.1 12.10.4 12.10.5 12.10.6	31.4.3(b)(2) 31.4.4(b)(3)		SIM-03 SIM-04 SIM-05 SIM-06 SIM-07 SPN-01	164.306(a)(1) 164.306(a)(2) 164.308(a)(1)(ii)(B) 164.308(a)(6)(i) 164.308(a)(7)(i)

Incident Response	Incident Response	Incident Response Testing	[The organization] tests incident response processes [in accordance with the organization-defined frequency]. Results from the tests are documented.						12.10.2 12.10.6				
Incident Response	Incident Response	Incident Response	Confirmed incidents are assigned a priority level and managed to resolution. 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	CC2.2 CC7.3 CC7.4 CC7.5		IR-4 IR-5 IR-9	10.6.3 10.8.1 12.10.3	314.3(b)(2) 314.4(b)(3)		SIM-01 SIM-02 SIM-03 SIM-04 SIM-05 SIM-06 SIM-07 SPN-01	164.308(a)(1)(ii)(D) 164.308(a)(6)(i) 164.308(a)(6)(ii) 164.308(a)(7)(i)
Incident Response	Incident Communication	External Communication of Incidents	[The organization] defines external communication requirements for incidents, including: • 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	CC2.2 CC2.3 CC7.3 CC7.4 CC7.5			12.10.1			HR-04 KOS-01 OIS-05 RB-10 RB-11 RB-13 SIM-01 SIM-02 SIM-03 SIM-04 SIM-05 SIM-06 SIM-07 SPN-01	164.308(a)(7)(i) 164.314(b)(2)(iv)
Incident Response	Incident Communication	Incident Reporting Contact Information	[The organization] provides a contact method for external parties to: • submit complaints and inquiries • report incidents		A.16.1.2	CC2.2 CC2.3			12.10.3			HR-04 RB-10 RB-11 RB-17 RB-19 RB-20 RB-21 SIM-04 SIM-05 SIM-06 SIM-07	164.308(a)(7)(i)
Incident Response	Incident Communication	Incident External Communication	[The organization] communicates a response to external stakeholders as required by the Incident Response Plan.			CC2.3			12.10.1			RB-20	164.308(a)(7)(i) 164.314(b)(2)(iv)
Mobile Device Management	Mobile Device Security	Mobile Device Enrollment	Where applicable, authorized [the organization] personnel must enrol mobile devices with the enterprise Mobile Device Management (MDM) solution prior to obtaining access to [the organization] network resources on mobile devices.					MP-7					
Mobile Device Management	Mobile Device Security	Configuration Management: Mobile Devices	Where applicable, portable and mobile devices are configured to ensure unnecessary hardware capabilities and functionalities are disabled, and management defined security features are enabled.						1.4				

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 security requirements and business justifications.		A.13.1.1	CC6.6		CA-3 CM-7 SC-5	1.1.4 1.2 1.2.1 1.2.3 1.3 1.3.1 1.3.2 1.3.3 1.3.4		FERPA_99.31(a)	KOS-01 KOS-02 KRY-02 PI-04	164.306(a)(2)
Network Operations	Perimeter Security	Inbound and Outbound Network Traffic: DMZ Requirements	Network traffic to and from untrusted networks passes through a Demilitarized Zone (DMZ).			CC6.1 CC6.7 CC6.8 CC8.1			1.1.4 1.2 1.2.1 1.2.3 1.3 1.3.1 1.3.2 1.3.3				
Network Operations	Perimeter Security	Ingress and Egress Points	[The organization] maintains an inventory of ingress and egress points on the production network and performs the following for each: · inventory is reduced to the minimum possible level · permitted ports, protocols and services are inventoried and validated · documents security features that are implemented for insecure protocols						1.1.6 1.3.6				
Network Operations	Perimeter Security	Non-disclosure of Routing Information	[The organization] does not disclose private IP addresses and routing information to unauthorized parties.						1.3.7				
Network Operations	Perimeter Security	Dynamic Packet Filtering	Where applicable, [the organization] enables dynamic packet filtering on the network.					SC-5	1.3.5				
Network Operations	Perimeter Security	Firewall Rule Set Review	Network infrastructure rule sets are reviewed [in accordance with the organization-defined frequency].					SC-5	1.1.7				
Network Operations	Perimeter Security	Trusted Connections	All trusted connections are documented and approved by authorized personnel; management ensures the following documentation is in place prior to approval: · agreement with vendor · security requirements · nature of transmitted information					CA-3 SC-7 SC-21 SC-22					
Network Operations	Network Segmentation	Network Segmentation	Production environments are logically segregated from non- production environments.		A.12.1.4 A.13.1.3 A.14.2.6	CC6.1 CC6.7 CC6.8 CC8.1		SC-39	6.4.1			BEI-11 KOS-04 RB-23	
Network Operations	Network Segmentation	Card Processing Environment Segmentation	Where applicable, [the organization] segregates the Personal Account Number (PAN) infrastructure including payment card collection devices; [the organization] limits access to the segregated environment to authorized personnel.						1.3.6 9.1.2				
Network Operations	Wireless Security	Disable Rogue Wireless Access Points	[The organization] employs mechanisms to detect and disable the use of unauthorized wireless access points.						12.10.5				

Network Operations	Wireless Security	Wireless Access Points	[The organization] maintains an inventory of authorized wireless access points including a documented business justification.						11.1.1				
Network Operations	Wireless Security	Rogue Wireless Access Point Mapping	[In accordance with the organization-defined frequency], [the organization] performs an access point mapping exercise to identify and remove unauthorized wireless access points.						11.1 11.1.2				
Network Operations	Wireless Security	Authentication: Wireless Access Points	[The organization] restricts access to network services via wireless access points to authenticated users and services; approved wireless encryption protocols are required for wireless connections.						4.1 4.1.1				
People Resources	On-boarding	Background Checks	New hires are required to pass a background check as a condition of their employment.	7.2	A.7.1.1	CC1.4 CC5.3		PS-3	12.7			HR-01	
People Resources	On-boarding	Performance Management	[The organization] has established a check-in performance management process for on-going dialogue between managers and employees. [In accordance with the organization-defined frequency] reminders are sent to managers to perform their regular check-in conversation.			CC1.1 CC1.4 CC1.5							
People Resources	On-boarding	Hiring Process	Job candidates apply for roles that are listed on the [the organization] career portal; candidates are interviewed to determine their knowledge and competence for their prospective roles and compatability with [the organization] values.			CC1.4							
People Resources	Off-boarding	Organization 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			PS-4					
People Resources	Off-boarding	Exit Interviews	Upon employee termination, management conducts exit interviews for the terminated employee.					PS-4					
People Resources	Compliance	Disciplinary Process	Employees that fail to comply with [the organization] policies are subject to a disciplinary process.	7.3(c)	A.7.2.3	CC1.1 CC1.5		PS-8				HR-04	164.306(a) 164.308(a)(1)(ii)(C)
People Resources	Business Ethics	Code of Ethics	[The organization] has a Code of Ethics for Senior Officers. The Senior Officers and CEO certify that they understand the Code on a an annual basis.			CC1.2		PL-4					
People Resources	Business Ethics	Business Ethics Hotline	[The organization] has a business ethics hotline for employees and external parties to report ethical misconduct. Allegations are investigated and [the organization] will take appropriate action for confirmed violations. Hotline reports are reported to the Audit Committee on a [in accordance with the organization-defined frequency].			CC1.1 CC1.5 CC2.2 CC2.3							

People Resources	Personnel Screening	National Security Clearance	[The organization] conducts screening and rescreening of authorized personnel for roles that require national security clearances. For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. In addition, for law enforcement and high impact public trust level, a reinvestigation is required during the 5th year.					PS-3					
Risk Management	Risk Assessment	Risk Assessment	[The organization] management performs a risk assessment [in accordance with the organization-defined frequency]. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks	4.1 8.1 8.2 8.3 10.2 6.1.1 6.1.2 6.1.3 6.2(c) 9.1		CC3.1 CC3.2 CC3.3 CC3.4 CC4.1 CC5.1 CC7.4		RA-3	12.2	314.4(b)(1) 314.4(b)(2) 314.4(b)(3)		OIS-06 OIS-07	164.306(a)(2) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)
Risk Management	Risk Assessment	Risk Assessment: HIPAA Criteria	[The organization]s periodic risk assessment for systems that process, transmit or store Protected Health Information (PHI) includes the following: · identify and classify assets · identify threats · identify vulnerabilities · identify controls · perform threat likelihood analysis · perform threat impact analysis · identify residual risk · identify appropriate safeguards										164.308(a)(1)(ii)(A) 164.308(a)(8)
Risk Management	Risk Assessment	Continuous Monitoring	The design and operating effectiveness of internal controls are continuously evaluated against the established [organization-defined controls framework] by [the organization]. Corrective actions related to identified deficiencies are tracked to resolution.	9.1 9.3 10.1	A.12.7.1 A.18.2.2 A.18.2.3	CC1.5 CC2.1 CC2.2 CC2.3 CC3.2 CC3.3 CC3.4 CC4.1 CC4.2 CC5.1 CC5.3 CC7.5		CA-5 CA-7				COM-02 COM-03 KOS-06 OIS-01 PI-01 RB-02 RB-03 RB-04 RB-11 RB-12	164.306(e) 164.308(a)(1)(i) 164.308(a)(8)
Risk Management	Risk Assessment	Self- Assessments	[In accordance with the organization-defined frequency], reviews shall be performed with approved documented specification to confirm personnel are following security policies and operational procedures pertaining to: · log reviews [in accordance with the organization-defined frequency] · firewall rule-set reviews · applying configuration standards to new systems · responding to security alerts · change management processes						12.11 12.11.1				

Risk Management	Risk Assessment	Service Risk Rating Assignment	[In accordance with the organization-defined frequency], [the organization] prioritizes the frequency of vulnerability discovery activities based on an assigned service risk rating.	4.1 8.1 8.2 8.3 10.2 6.1.1 6.1.2 6.1.3 6.2(c) 9.1		CC3.2 CC4.1 CC5.1 CC7.4		CA-7	12.2	314.4(b)(1) 314.4(b)(2) 314.4(b)(3)			164.306(a)(2) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)
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 the organization-defined frequency].	9.2	A.12.7.1 A.18.2.1 A.18.2.2 A.18.2.3	CC2.2 CC1.5 CC4.1 CC4.2		CA-5 CA-7		314.4(c)		COM-02 COM-03 OIS-01 SPN-02 SPN-03	164.306(e) 164.308(a)(8)
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.	9.2		CC4.1							
Risk Management	Controls Implementation	Remediation Tracking	Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	8.3 10.1 10.2		CC4.2 CC5.1 CC5.3 CC7.4 CC7.5				314.4(c)		COM-03 OIS-01 SPN-02	
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.	10.1 10.2									
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.	6.1.3(c) 6.1.3(d)	A.18.1.1	CC5.1							
System Design Documentation	Internal System Documentation	System Documentation	Documentation of system boundaries and key aspects of their functionality are published to authorized personnel.			CC2.2		CA-3 CA-9 SA-5				IDM-01	
System Design Documentation	Internal System Documentation	System Documentation: Cardholder Environment	Information systems and interfaces of the Cardholder Data Environment (CDE) are diagrammed.						1.1.2 1.1.3				
System Design Documentation	Customer- facing System Documentation	Whitepapers	[The organization] publishes whitepapers to its public website that describe the purpose, design, and boundaries of the system and system components.			CC2.3						IDM-01	

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 the organization-defined frequency].	5.1(d) 5.2(e) 5.2(g) 7.3(a) 7.3(b) 7.3(c) 7.5.1(b) 7.5.2(a) 7.5.2(b) 7.5.2(c) 7.5.3(a) 7.5.3(b) 7.5.3(c) 7.5.3(d) 7.5.3(e) 7.5.3(f)	A.5.1.1 A.5.1.2 A.12.1.1 A.12.5.1 A.12.6.2	CC1.4 CC2.2 CC5.3		PS-6	1.5 2.5 3.5 3.5.1 3.5.2 3.5.3 3.5.4 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8 4.3 5.4 6.7 7.3 8.1 8.1.1 8.1.2 8.1.3 8.1.4 8.1.5 8.1.6 8.1.7			OIS-01 SA-01 SA-02	164.308(a)(1)(i) 164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.308(a)(6)(i) 164.308(a)(7)(i) 164.310(a)(1) 164.310(a)(2)(i) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.312(a)(1) 164.312(c)(1) 164.316(b)(2)(ii) 164.316(b)(2)(iii)
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	CC5.3						OIS-01 SA-01 SA-02 SA-03	
Security Governance	Policy Governance	Document Control	[The organization]'s document management criteria is periodically reviewed, approved by management, and communicated to authorized personnel; management determines the treatment and retention of documentation according to legal and regulatory requirements.										164.316(b)(1)(i) 164.316(b)(1)(ii) 164.316(b)(2)(i) 164.316(b)(2)(iii)
Security Governance	Security Documentation	Information Security Program Content	[The organization-defined security leader] conducts a periodic staff meeting to communicate and align on relevant security threats, program performance, and resource prioritization.		A.5.1.1 A.6.1.1 A.6.1.5 A.6.2.1 A.6.2.2 A.9.1.1 A.10.1.1 A.11.2.9 A.13.2.1	CC1.3 CC4.1 CC5.2 CC5.3 CC7.1 CC7.2 CC7.4		AC-1 AT-1 AU-1 CA-1 CA-6 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1	11.5 10.8 10.9 11.6 12.1 12.3 12.3.1 12.3.10 12.3.2 12.3.3 12.3.4 12.3.5 12.3.6 12.3.7 12.3.8 12.3.9 12.4 2.5 3.7 4.3 5.4 6.7 7.3 8.1	314.3(a)			164.306(a) 164.308(a)(1)(i) 164.308(a)(3)(i) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.308(a)(6)(i) 164.308(a)(7)(i) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iv) 164.310(d)(1) 164.312(a)(1) 164.312(c)(1) 164.316(a) 164.316(b)(1)(i)
Security Governance	Security Documentation	Procedures	[The organization's] key control capabilities are supported by documented procedures that are communicated to authorized personnel					AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1					

Security Governance	Privacy Program	Privacy Readiness Review	[The organization] performs privacy readiness reviews to identify high-risk processing activities that impact personal data; identified non- compliance with [the organization] privacy practices is tracked through remediation.		A.18.1.4	CC2.3							
Security Governance	Privacy Documentation	Document Management Standard: HIPAA	Documentation that impacts personal health information, including policies, procedures, and the documentation of actions, activities, or assessments, are retained for 6 years from the date of its creation, or the date when it last was in effect, whichever is later.										164.316(b)(1)(i) 164.316(b)(1)(ii) 164.316(b)(2)(i) 164.316(b)(2)(iii)
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	CC2.3		PS-6				KOS-08	164.306(a) 164.310(b)
Security Governance	Workforce Agreements	Review of Confidentiality Agreements	[The organization's] proprietary rights agreement and network access agreement are reviewed [in accordance with the organization-defined frequency].		A.13.2.4 A.18.1.2	CC2.3		PS-6				KOS-08	164.306(a) 164.306(e) 164.310(b) 164.316(b)(2)(iii)
Security Governance	Workforce Agreements	Key Custodians Agreement	Cryptographic Key Custodians and Cryptographic Materials Custodians (CMC) acknowledge in writing or electronically that they understand and accept their cryptographic-key-custodian responsibilities.						3.6 3.6.8				
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.	4.2 5.1 7.4 9.3		CC1.3 CC7.4		PL-2		314.4(a)		OIS-01	164.308(a)(2)(i) 164.314(b)(1) 164.314(b)(2) 164.316(b)(1)(i) 164.316(b)(2)(ii)
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.	4.2 4.3 4.4 5.2 6.2 7.4 7.5.1 8.1 9.1 9.3	A.6.1.1 A.6.1.5 A.18.2.1	CC1.3 CC5.3 CC7.4		CA-6 PL-2		314.4(b)(3)(e)			
Security Governance	Information Security Management System	Security Roles and Responsibilities	Roles and responsibilities for the governance of Information Security within [the organization] are formally documented within the Information Security Management Standard and communicated on the [the organization] intranet.	5.3 6.2(h) 7.2	A.6.1.1	CC1.3 CC1.4 CC5.3 CC9.2		PL-4	1.1.5 12.10.1 12.4 12.5 12.5.1 12.5.2 12.5.3 12.5.4 12.5.5			AM-02 AM-03 DLL-01 HR-02 HR-03 KOS-08 OIS-01 OIS-02 OIS-03 RB-02 SA-01	

Security Governance	Information Security Management System	Security Roles and Responsibilities: PCI Compliance	Roles and responsibilities and a program charter for the governance of PCI DSS compliance within [the organization] are formally documented and communicated by management.						12.4.1				
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.	5.1(c) 6.2(g) 7.1	A.6.1.5	CC7.4		SA-2					
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 on an annual basis.	9.3		CC4.1 CC4.2 CC5.2						SPN-01	
Service Lifecycle	Release Management	Service Lifecycle Workflow	Major software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.		A.14.1.1 A.14.2.5	CC6.8 CC8.1		SA-1 SA-3 SA-4	6.3			BEI-01 BEI-07 KOS-07	
Service Lifecycle	Source Code Management	Source Code Management	Source code is managed with [the organization]-approved version control mechanisms.		A.14.2.6	CC6.8 CC7.1 CC8.1						BEI-01 BEI-07 BEI-11 KOS-07	
Systems Monitoring	Logging	Audit Logging	[The organization] logs critical information system activity.		A.12.4.1	CC6.8 CC7.1 CC7.2	A.12	AU-12 AU-2 MA-4 SC-7		314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)	RB-10 RB-11 RB-14 SIM-05	164.312(b) 164.312(c)(2)
Systems Monitoring	Logging	Secure Audit Logging	[The organization] logs critical information system activity to a secure repository. [the organization] disables administrators ability to delete or modify enterprise audit logs; the number of administrators with access to audit logs is limited.			CC7.2			10.5 10.5.1 10.5.2 10.5.3 10.5.4				
Systems Monitoring	Logging	Audit Logging: Cardholder Data Environment Activity	[The organization] logs the following activity for cardholder data environments: · individual user access to cardholder data · administrative actions · access to logging servers · failed logins · modifications to authentication mechanisms and user privileges · initialization, stopping, or pausing of the audit logs · creation and deletion of system-level objects · security events · logs of all system components that store, process, transmit, or could impact the security of cardholder data (CHD) and/or sensitive authentication data (SAD) · logs of all critical system components · logs of all servers and system components that perform security functions (e.g., firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, ecommerce redirection servers, etc.)						10.1 10.2 10.2.1 10.2.2 10.2.3 10.2.4 10.2.5 10.2.6 10.2.7 10.6.1				

Systems Monitoring	Logging	Audit Logging: Cardholder Data Environment Event Information	[The organization] records the following information for confirmed events in the cardholder data environment: · user identification · type of event · date and time · event success or failure indication · origination of the event · identification of affected data, system component, or resource						10.3 10.3.1 10.3.2 10.3.3 10.3.4 10.3.5 10.3.6				
Systems Monitoring	Logging	Audit Logging: Service Provider Logging Requirements	[The organization] establishes unique logging and audit trails for each entity's cardholder data environment and complies with the following: · logs are enabled for third-party applications · logs are active by default · logs are available for review by and communicated to the owning entity						A.1 A.1.3 A.1.4				
Systems Monitoring	Logging	Log Reconciliation: CMDB	[The organization] reconciles the established device inventory against the enterprise log repository [in accordance with the organization-defined frequency]; devices which do not forward log data are remediated.		A.12.4.1	CC7.1 CC7.2				314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)		164.312(b) 164.312(c)(2)
Systems Monitoring	Logging	Audit Log Capacity and Retention	[The organization] allocates audit record storage capacity in accordance with logging storage and retention requirements; Audit logs are retained [in accordance with the organization-defined duration] with [the organization-defined duration] of data immediately available for analysis.					CA-7	10.7				
Systems Monitoring	Logging	Enterprise Antivirus Logging	If applicable, [the organization's] managed enterprise antivirus deployments generate audit logs which are retained [in accordance with the organization-defined duration] with [the organization-defined duration] of data immediately available for analysis.						10.7 5.2				
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.9.4.4 A.12.4.3			AC-2 AU-2 AU-3 AU-8 AU-12	10.8 10.9 12.10.5 12.5 12.5.2	314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)	IDM-06 IDM-12 RB-10 RB-11 RB-15	
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			AU-6					
Systems Monitoring	Security Monitoring	Security Monitoring Alert Criteria: Failed Logins	[The organization] defines security monitoring alert criteria for failed login attempts on [the organization's] network						10.2 10.2.4 10.6				164.308(a)(5)(ii)(C)

Systems Monitoring	Security Monitoring	Security Monitoring Alert Criteria: Privileged Functions	[The organization] defines security monitoring alert criteria for privileged functions executed by both authorized and unauthorized users.						10.6				
Systems Monitoring	Security Monitoring	Security Monitoring Alert Criteria: Audit Log Integrity	[The organization] defines security monitoring alert criteria for changes to the integrity of audit logs.						10.5.5				
Systems Monitoring	Security Monitoring	Security Monitoring Alert Criteria: Cardholder System Components	[The organization] defines security monitoring alert criteria for system components that store, process, transmit, or could impact the security of cardholder data and/or sensitive authentication data.						10.6.1				
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	CC7.2 CC7.3	A1.2	AU-2 AU-5 AU-9 SC-7 SI-4	10.2 10.2.4 10.5.5 10.6 10.6.1 10.6.2 10.6.3 10.8.1 12.10.5	314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)	IDM-06 RB-10 RB-11 RB-13 RB-15	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(i) 164.308(a)(6)(ii) 164.312(b)
Systems Monitoring	Security Monitoring	Intrusion Detection Systems	[The organization] has an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) deployment(s) and ensures the following: • signature definitions are updated including the removal of false positive signatures • non-signature based attacks are defined • IDS/IPS are configured to capture malicious (both signature and non-signature based) traffic • alerts are reviewed and resolved by authorized personnel when malicious traffic is detected					SI-4 SI-5	11.4 12.10.5				
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.12.1.3 A.17.2.1		A1.1 A1.2	SI-5				AM-05 BCM-04 BCM-05 PS-04 RB-01 RB-02 RB-04 RB-16	
Systems Monitoring	Availability Monitoring	System Availability Monitoring	Critical systems are monitored in accordance to predefined availability criteria and alerts are sent to authorized personnel.		A.12.1.3 A.17.2.1		A1.1 A1.2	SI-5				AM-05 BCM-04 BCM-05 PS-04 RB-01 RB-02 RB-04 RB-16	
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		A1.2	PE-16 PE-3	9.1 9.1.3 9.5		FERPA_99.31(a)	AM-08 BCM-05 PS-01 PS-02 PS-03 PS-04	164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(C)
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		A1.2					BCM-05 PS-04	

Site Operations	Physical Access Account Lifecycle	Provisioning Physical Access	Physical access provisioning to a [the organization] datacenter requires management approval and documented specification of: · 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	A.1.2	MA-5 MP-2 PE-12 PE-3	9.2 9.3 9.4 9.4.1 9.4.2 9.5		FERPA_99.31(a)	BCM-05 PS-02 PS-04	164.308(a)(3)(ii)(A) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(c)
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	A.1.2	PE-14 PS-4	9.2 9.3 9.4.3 9.5		FERPA_99.31(a)	BCM-05 PS-02 PS-04	164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(c)
Site Operations	Physical Access Account Lifecycle	Periodic Review of Physical Access	[The organization] performs physical access account reviews [in accordance with the organization-defined frequency]; corrective action is taken where applicable.		A.11.1.2	CC6.4	A.1.2	PE-14 PS-5	9.5		FERPA_99.31(a)		164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(c)
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		A.1.2				FERPA_99.31(a)	BCM-05 PS-02 PS-04	164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(c)
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		A.1.2	PE-2 PE-3	9.1 9.1.1			PS-04	
Site Operations	Physical Access Account Lifecycle	Surveillance Feed Retention	Surveillance feed data is retained for [the organization- defined duration].						9.1.1				
Site Operations	Physical Access Account Lifecycle	Visitor Access	Physical access for visitors is managed through monitoring, maintaining records, escorting, and reviewing access [in accordance with the organization-defined frequency]. Visitor access records to the facilities are kept for [the organization-defined duration].					PE-3	9.4.1 9.4.4				164.310(a)(2)(iii) 164.310(c)
Site Operations	Physical Access Account Lifecycle	Physical Access Devices	Physical access devices (i.e., keys, combinations, access cards, etc.) are maintained through an inventory and restricted to authorized individuals. Appropriate devices are rotated when compromised or upon employee termination or transfer.					PE-3					
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		A.1.2	PE-6 PE-14				BCM-05 PS-03 PS-04 PS-05	
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 the organization-defined frequency].		A.11.1.4 A.11.2.1		A.1.2	PE-6 PE-13				BCM-05 PS-03 PS-04 PS-05	

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 the organization-defined frequency].		A.11.2.2		A.1.2					BCM-05 PS-04	
Site Operations	Environmental Security	Emergency Lighting	[The organization] employs emergency lighting in the event of a power disruption or failure. The design and function of relevant equipment is certified [in accordance with the organization-defined frequency].					PE-3					
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.	5.1(d) 7.2 7.3(b) 7.3(c)	A.7.2.1 A.7.2.2 A.16.1.2 A.16.1.3	CC2.2 CC5.3		AT-2 AT-4 IR-6	12.6 12.6.1 12.6.2	314.4(b)(1)		HR-03 SIM-05 SIM-06	164.308(a)(5)(i) 164.308(a)(5)(ii) 164.308(a)(5)(ii)(a)
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.7.1.2 A.7.2.1 A.8.1.3 A.11.2.8	CC1.1 CC2.2			12.3 12.3.5			AM-03 HR-02 KOS-08	164.306(a) 164.310(b)
Training and Awareness	Role-Based Training	Developer Security Training	[The organization's] software engineers are required to complete training based on secure coding techniques [in accordance with the organization-defined frequency].					AT-3	6.5				
Training and Awareness	Role-Based Training	Payment Card Processing Security Awareness Training	[The organization] personnel that interact with cardholder data systems receive awareness training to be aware of attempted tampering or replacement of devices. Training should include the following: • verify the identity of third- party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • do not install, replace, or return devices without verification • be aware of suspicious behaviour around devices (e.g., attempts by unknown persons to unplug or open devices) • report suspicious behaviour and indications of device tampering or substitution to authorized personnel (e.g., to a manager or security officer)						9.9.3				

Training and Awareness	Role-Based Training	Role-based Security Training	[The organization] personnel with key security responsibilities complete relevant role-based training [in accordance with the organization-defined frequency]: • personnel must complete training prior to obtaining access to privileged security systems • personnel with contingency responsibilities must complete role-based training [in accordance with the organization-defined frequency] • records of training completion are documented and retained for tracking purposes					IR-2					
Training and Awareness	Role-Based Training	Role-based Security Training: HIPAA	[The organization] personnel with access to personal health information (PHI) are required to attend and complete HIPAA privacy training.										164.308(a)(5)(i) 164.308(a)(5)(ii) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)
Third Party Management	Vendor Assessments	Third Party Assurance Review	[In accordance with the organization-defined frequency], management reviews controls within third party assurance reports to ensure that they meet 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	CC1.3 CC1.4 CC3.2 CC3.4 CC9.2		PS-7 SA-1 SA-4 SA-9	12.8.3 12.8.4 9.5 9.5.1	314.4(d)(1) 314.4(d)(2)		DLL-01 DLL-02 KOS-07 KOS-08 SIM-02	164.308(b)(1) 164.308(b)(2) 164.314(a) 164.314(b)(2)(iii)
Third Party Management	Vendor Assessments	Vendor Risk Management	[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	CC1.3 CC1.4 CC3.2 CC6.1 CC9.2		PS-7 SA-1 SA-4 SA-9	12.8 12.8.2 12.8.3 12.8.5 2.6	314.4(d)(1) 314.4(d)(2)		DLL-01 KOS-07 KRY-01 PI-03 SIM-02	164.314(a)
Third Party Management	Vendor Assessments	Forensic Investigations	[The organization] enables procedures to conduct a forensic investigation in the event that a hosted merchant or service provider is compromised.						A.1.4				
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	CC2.3		PS-7				KOS-01 KOS-02 KOS-08 PI-04	164.306(a) 164.310(b)

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	CC9.2		PS-7	12.8.2	314.4(d)(2)		BEI-02 DLL-01 KOS-07 KRY-01 SIM-02	164.308(b)(1) 164.308(b)(2) 164.314(a)(1) 164.314(a)(2)(i) 164.314(a)(2)(ii) 164.314(a)(2)(iii)
Third Party Management	Vendor Agreements	Cardholder Data Security Agreement	[The organization] managed service providers that manage, store, or transmit cardholder data on behalf of the customer must provide written acknowledgement to customers of their responsibility to protect cardholder data and the cardholder data environment.						12.9				
Third Party Management	Vendor Agreements	Network Service Level Agreements (SLA)	Vendors providing networking services to [the organization] are contractually bound to provide secure and available services as documented in SLAs.		A.13.1.2	CC6.6 CC9.2		PS-7					
Third Party Management	Vendor Procurement	Approved Service Provider Listing	[The organization] maintains a list of approved managed service providers and the services they provide to [the organization].						12.8.1				
Third Party Management	Vendor Agreements	HIPAA Business Associate Subcontractor Agreement	[The organization] requires a Business Associate Subcontractor Agreement with Business Associates from which it receives or transmits protected health information (PHI); Business Associates under contract are required to provide assurance that they adhere to [the organization] security standards, which includes the security of PHI and reporting security events that potentially expose PHI.										164.308(b)(1) 164.308(b)(2) 164.308(b)(3) 164.314(a)(1) 164.314(a)(2)(i) 164.314(a)(2)(ii) 164.314(a)(2)(iii)
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	CC6.8 CC7.1 CC7.2		CA-7 RA-5 SI-2	11.2 11.2.1 11.2.2 11.2.3 11.3.3 5.1.2	314.4(b)(2)	FERPA_99.31(a)	RB-17 RB-19 RB-20 RB-21	164.306(a)(1) 164.306(a)(2) 164.306(a)(3) 164.308(a)(1)(ii)(B)
Vulnerability Management	Production Scanning	Vulnerability Assessment: Cardholder Data Environment	Vulnerability scans are conducted against cardholder environments [in accordance with the organization-defined frequency] or after significant change; critical vulnerability resolution is confirmed via a rescan.						11.2 11.2.1				
Vulnerability Management	Production Scanning	Approved Scanning Vendor	[In accordance with the organization-defined frequency], [the organization] engages an Approved Scanning Vendor to conduct external vulnerability scans.						11.2.2				
Vulnerability Management	Penetration Testing	Application Penetration Testing	[The organization] conducts penetration tests according to the service risk rating assignment.		A.12.6.1	CC4.1 CC6.8 CC7.1 CC7.2		CA-2(1) CA-7 IA-6 SI-3	11.3 11.3.1 11.3.2 11.3.4	314.4(b)(2)	FERPA_99.31(a)	RB-17 RB-18 RB-19 RB-20 RB-21	

Vulnerability Management	Penetration Testing	Penetration Testing: Cardholder Data Environment	[The organization] conducts penetration tests against cardholder data environments (CDE) and includes the following requirements: · testing covers the entire CDE perimeter and critical data systems · testing verifies that CDE perimeter segmentation is operational · testing is performed from both inside and outside the CDE network · testing validates segmentation and scope reduction controls (e.g, tokenization processes) · network layer penetration tests include components that support network functions as well as operating systems · at the application level, testing provides coverage, at a minimum, against the security testing requirements defined in "Code Security Check: Cardholder Data Environment" · testing is performed with consideration of threats verified [in accordance with the organization-defined frequency] from external alerts, directives, and advisories defined in "External Alerts and Advisories" · testing is performed with consideration of vulnerabilities reported through [the organization's] PSIRT process [in accordance with the organization-defined frequency] · risk ratings are assigned to discovered vulnerabilities, which are tracked through remediation						11.3 11.3.4 11.3.4.1				
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.					CA-7 SI-2	6.2	314.3(b)(2) 314.4(b)(3)	FERPA_99.31(a)	RB-17 RB-19 RB-20 RB-21	
Vulnerability Management	Malware Protection	Enterprise Antivirus	If applicable, [the organization] has managed enterprise antivirus deployments and ensures the following: · signature definitions are updated · full scans are performed [in accordance with the organization-defined frequency] and real-time scans are enabled · alerts are reviewed and resolved by authorized personnel		A.12.2.1	CC6.8 CC7.2		CA-7	5.1 5.1.1 5.1.2 5.2 6.2		FERPA_99.31(a)	MDM-01 RB-05	164.306(a)(2) 164.308(a)(5)(ii)(B)
Vulnerability Management	Malware Protection	Enterprise Antivirus Tampering	Antivirus mechanisms cannot be disabled or altered by users unless specifically authorized by management.						5.3				
Vulnerability Management	Code Security	Code Security Check	[In accordance with the organization-defined frequency], [the organization] conducts source code checks for vulnerabilities according to the service risk rating assignment.		A.14.2.1 A.14.2.5	CC6.8 CC7.2		CA-7 IA-6 SI-3	6.3.1 6.4.4				
Vulnerability Management	Code Security	Code Security Check: Cardholder Data Environment	Where applicable, security testing performed prior to releasing code into production includes the following: · code injection · buffer overflows · insecure cryptographic storage · insecure communications · improper error handling · high-risk vulnerabilities · cross-site scripting · improper access control · cross-site request forgery · broken authentication session management						6.5 6.5.1 6.5.10 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.6				

Vulnerability Management	External Advisories and Inquiries	External Information Security Inquiries	[The organization] reviews information-security-related inquiries, complaints, and disputes.									MDM-01 RB-05	
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				6.1				
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.6.1.5 A.12.6.1 A.14.2.8	CC7.1		CA-7	6.1	314.4(c)	FERPA_99.31(a)	RB-17 RB-19 RB-21	164.306(a)(1) 164.306(a)(2) 164.306(a)(3) 164.308(a)(1)(ii)(B)