v11.2.0 Summary of Changes

Difference Comparison for CSF v11.1.0 to v11.2.0

HITRUST

Table of Contents

Changes for Library Version - v11.1.0 to v11.2.0

Library Version: v11.2.0

Change Count: 1

Field	Content
Name	v11.12.0

Changes for Control Objective - v11.1.0 to v11.2.0

Control Objective: 09.09 On-line Transactions

Change Count: 2

Field	Content
Name	09.09 Electronic Commerce ServiceOn-line Transactions
Description	Ensure the security of electronic commerce services, and their secure useon-line transactions.

Changes for Question Requirement - v11.1.0 to v11.2.0

Question Requirement: 19.13kPHIPAOrganizational.14 / 2758.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.14 / 2758.0

Question Requirement: 19.13kPHIPAOrganizational.13 / 2757.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.13 / 2757.0

Question Requirement: 19.13kPHIPAOrganizational.12 / 2756.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.12 / 2756.0

Question Requirement: 19.13kPHIPAOrganizational.11 / 2755.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.11 / 2755.0

Question Requirement: 19.13kPHIPAOrganizational.10 / 2754.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.10 / 2754.0

Question Requirement: 19.13kPHIPAOrganizational.9 / 2753.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.9 / 2753.0

Question Requirement: 19.13kPHIPAOrganizational.8 / 2752.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.8 / 2752.0

Question Requirement: 19.13dPHIPAOrganizational.3 / 2751.0

Change Count: 0

Field	Content
New Question Requirement	19.13dPHIPAOrganizational.3 / 2751.0

Question Requirement: 19.13kPHIPAOrganizational.7 / 2750.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.7 / 2750.0

Question Requirement: 19.13kPHIPAOrganizational.6 / 2749.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.6 / 2749.0

Question Requirement: 19.13kPHIPAOrganizational.5 / 2748.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.5 / 2748.0

Question Requirement: 19.13uPHIPAOrganizational.6 / 2747.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.6 / 2747.0

Question Requirement: 19.13pPHIPAOrganizational.1 / 2746.0

Change Count: 0

Field	Content
New Question Requirement	19.13pPHIPAOrganizational.1 / 2746.0

Question Requirement: 19.13kPHIPAOrganizational.4 / 2745.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.4 / 2745.0

Question Requirement: 19.13dPHIPAOrganizational.2 / 2744.0

Change Count: 0

Field	Content
New Question Requirement	19.13dPHIPAOrganizational.2 / 2744.0

Question Requirement: 19.13uPHIPAOrganizational.5 / 2743.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.5 / 2743.0

Question Requirement: 19.13bPHIPAOrganizational.2 / 2742.0

Change Count: 0

Field	Content
New Question Requirement	19.13bPHIPAOrganizational.2 / 2742.0

Question Requirement: 19.13uPHIPAOrganizational.4 / 2741.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.4 / 2741.0

Question Requirement: 19.13uPHIPAOrganizational.3 / 2740.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.3 / 2740.0

Question Requirement: 19.13uPHIPAOrganizational.2 / 2739.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.2 / 2739.0

Question Requirement: 19.13uPHIPAOrganizational.1 / 2738.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.1 / 2738.0

Question Requirement: 19.13fPHIPAOrganizational.4 / 2737.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.4 / 2737.0

Question Requirement: 19.13dPHIPAOrganizational.1 / 2736.0

Change Count: 0

Field	Content
New Question Requirement	19.13dPHIPAOrganizational.1 / 2736.0

Question Requirement: 19.13kPHIPAOrganizational.3 / 2735.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.3 / 2735.0

Question Requirement: 19.13bPHIPAOrganizational.1 / 2733.0

Change Count: 0

Field	Content
New Question Requirement	19.13bPHIPAOrganizational.1 / 2733.0

Question Requirement: 19.13eNYDOHOrganizational.2 / 2720.0

Change Count: 0

Field	Content
New Question Requirement	19.13eNYDOHOrganizational.2 / 2720.0

Question Requirement: 19.13dNYDOHOrganizational.2 / 2719.0

Change Count: 0

Field	Content
New Question Requirement	19.13dNYDOHOrganizational.2 / 2719.0

Question Requirement: 19.13oNYDOHOrganizational.2 / 2718.0

Change Count: 0

Field	Content
New Question Requirement	19.13oNYDOHOrganizational.2 / 2718.0

Question Requirement: 19.13kPHIPAOrganizational.2 / 2708.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.2 / 2708.0

Question Requirement: 19.13iPHIPAOrganizational.1 / 2707.0

Change Count: 0

Field	Content
New Question Requirement	19.13iPHIPAOrganizational.1 / 2707.0

Question Requirement: 19.13ePHIPAOrganizational.1 / 2706.0

Change Count: 0

Field	Content
New Question Requirement	19.13ePHIPAOrganizational.1 / 2706.0

Question Requirement: 19.13fPHIPAOrganizational.3 / 2704.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.3 / 2704.0

Question Requirement: 19425.13jGDPROrganizational.1 / 1848.0

Change Count: 1

Field	Content
RequirementStatement	The organization does not process: PII revealing racial origin; PII revealing ethnic origin; PII revealing political opinions; PII revealing religious or philosophical beliefs; PII revealing trade-union membership; PII revealing genetic or biometric data for the purpose of uniquely identifying an individual; data concerning health; or data concerning an individual”s sex life or sexual orientation.

Question Requirement: 19405.13gGDPROrganizational.5 / 1839.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of incidents of processing and whether it was carried out in a manner , as a percentage of all incidents of processing. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that organizations ensure that they process PII in alignment with the six legal bases for processing.

Question Requirement: 19131.06cNYDOHOrganizational.3 / 2104.0

Change Count: 2

Field	Content
RequirementStatement	The following is documented and retained for at least six [6] years from the date of its creation or the date when it was last in effect, whichever is later: decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question; a user's right of access to a workstation, transaction, program, or process; security incidents and their outcomes; satisfactory assurances that a business associate will appropriately safeguard PHI, this documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements - if satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained; repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); changes to organizational policies and procedures.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the following actions, activities, and assessments relating to the security of systems containing PHI are documented and retained for at least six [6] years from the date of its creation or the date when it was last in effect, whichever is later: (i) decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question; (ii) a user's right of access to a workstation, transaction, program, or process; (iii) security incidents and their outcomes; (iv) satisfactory assurances that a business associate will appropriately safeguard PHI, this documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements - if satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained; (v) repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks); and (vi) changes to organizational policies and procedures.

Question Requirement: 19601.13a2Organizational.2 / 1570.0

Change Count: 2

Field	Content
RequirementStatement	The organization defines requirementsRequirements have been defined for providing real-time and/or layered notice when ithe organization collects PII.

IllustrativeProcedureMeasured	For example, the measure(s) could indicate the number of instances in which a real-time and/or layered notice was not provided when PII was collected, as a percentage of all instances of PII collected. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization provides real-time and/or layered notice when ithe organization collects PII.

Question Requirement: 18.09pFTIOrganizational.12 / 2602.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 18139.09pFTIOrganizational.9 / 1020.0

Change Count: 1

Field	Content
RequirementStatement	FTI must never be disclosed to an organization''s agents or contractors during disposal unless authorized by the Internal Revenue Code.

Question Requirement: 18136.09pFTIOrganizational.12 / 1017.1

Change Count: 1

Field	Content
RequirementStatement	Media sanitization requirements are established as applicable for media used in pre-production or test environments: the technique for clearing, purging, and destroying media are the same, regardless of where the information system media is located; every third piece of media must be tested after sanitization has been completed; and media sanitization is witnessed or verified by the organization''s employee.

Question Requirement: 17.03cISO31000Organizational.1 / 2825.0

Change Count: 0

Field	Content
New Question Requirement	17.03cISO31000Organizational.1 / 2825.0

Question Requirement: 17.03bISO31000Organizational.1 / 2824.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO31000Organizational.1 / 2824.0

Question Requirement: 17.03aISO31000Organizational.12 / 2823.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.12 / 2823.0

Question Requirement: 17.03aISO31000Organizational.5 / 2822.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.5 / 2822.0

Question Requirement: 17.03aISO31000Organizational.11 / 2821.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.11 / 2821.0

Question Requirement: 17.03aISO31000Organizational.8 / 2820.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.8 / 2820.0

Question Requirement: 17.03aISO23894Organizational.15 / 2800.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.15 / 2800.0

Question Requirement: 17.03aISO23894Organizational.17 / 2799.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.17 / 2799.0

Question Requirement: 17.03aISO23894Organizational.19 / 2798.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.19 / 2798.0

Question Requirement: 17.03aISO23894Organizational.16 / 2797.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.16 / 2797.0

Question Requirement: 17.03cISO23894Organizational.3 / 2795.0

Change Count: 0

Field	Content
New Question Requirement	17.03cISO23894Organizational.3 / 2795.0

Question Requirement: 17.03cISO23894Organizational.2 / 2794.0

Change Count: 0

Field	Content
New Question Requirement	17.03cISO23894Organizational.2 / 2794.0

Question Requirement: 17.03bISO23894Organizational.11 / 2793.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.11 / 2793.0

Question Requirement: 17.03bISO23894Organizational.10 / 2792.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.10 / 2792.0

Question Requirement: 17.03bISO23894Organizational.12 / 2791.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.12 / 2791.0

Question Requirement: 17.03aISO23894Organizational.21 / 2789.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.21 / 2789.0

Question Requirement: 17.03aISO23894Organizational.20 / 2788.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.20 / 2788.0

Question Requirement: 17.03aISO23894Organizational.23 / 2787.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.23 / 2787.0

Question Requirement: 17.03aISO31000Organizational.4 / 2786.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.4 / 2786.0

Question Requirement: 17.00aNYDOHOrganizational.3 / 2726.0

Change Count: 0

Field	Content
New Question Requirement	17.00aNYDOHOrganizational.3 / 2726.0

Question Requirement: 17.10aVAD6500Organizational.1 / 2695.0

Change Count: 0

Field	Content
New Question Requirement	17.10aVAD6500Organizational.1 / 2695.0

Question Requirement: 17.03cTXRAMPOrganizational.1 / 2686.0

Change Count: 0

Field	Content
New Question Requirement	17.03cTXRAMPOrganizational.1 / 2686.0

Question Requirement: 17127.10aFedRAMPOrganizational.1 / 1254.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the date of the last review/update of the enterprise architecture and related security architecture, and the date of the last significant change to enterprise architecture impacting security architecture. Measures could include the schedule/status of any planned update of security architecture related documentation where enterprise architecture was significantly changed without a review or update. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has up-to-date enterprise architecture and related security architecture documentation, including the security plan and organizational procurements and acquisitions.

Question Requirement: 17.00aFedRAMPOrganizational.8 / 2395.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the measure(s) could indicate whether the system and information risk assessment policy has been formally defined and the percentage of users that have received communication of their roles and responsibilities. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its risk assessment program (e.g., through policy, standards, guidelines, and procedures).

Question Requirement: 17130.03bFedRAMPOrganizational.1 / 0401.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 17.07dFedRAMPOrganizational.1 / 2419.0

Change Count: 2

Field	Content
RequirementStatement	The organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance, and ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official''s designated representative.
DITA	Sampling

Question Requirement: 17224.10aNYDOHOrganizational.6 / 2196.0

Change Count: 3

Field	Content
RequirementStatement	The information system follows system security and privacy engineering principles consistent with: the information security steps of the CMS system developmenTarget lLife cCycle governance process(TLC) to incorporate information security and privacy control considerations; the information system architecture defined within the Technical Reference Architecture (TRA); and the Technical Review Board (TRB) processes defined by CMS.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the information system follows system security and privacy engineering principles consistent with (i) the information security steps of the CMS system developmenTarget lLife cCycle governance process(TLC) to incorporate information security and privacy control considerations; (ii) the information system architecture defined within the Technical Reference Architecture (TRA); and (iii) the Technical Review Board (TRB) processes defined by CMS.
IllustrativeProcedureMeasured	For example, measures indicate the number of developed or acquired information systems where appropriate security and privacy engineering principles were not applied as a percent of developed or acquired information systems. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the information system follows system security and privacy engineering principles consistent with (i) the information security steps of the CMS system developmenTarget lLife cC ycle governance process(TLC) to incorporate information security and privacy control considerations; (ii) the information system architecture defined within the Technical Reference Architecture (TRA); and (iii) the Technical Review Board (TRB) processes defined by CMS.

Question Requirement: 1755.06i2Organizational.1 / 0620.0

Change Count: 1

Field	Content
RequirementStatement	The organization formally addresses [in audit policies and/or standards]: purpose of audit and accountability requirements/controls; scope of audit and accountability requirements/controls; roles; responsibilities; management commitment of audit and accountability; coordination among organizational entities for audit and accountability; and compliance with audit and accountability requirements. The organization facilitates the implementation of audit and accountability requirements/controls.

Question Requirement: 1764.07d2Organizational.11 / 0662.0

Change Count: 1

Field	Content
RequirementStatement	The organization creates and documents a process and procedure to affix an organization identification tag to: newly purchased IT-related assets (tagging required prior to deployment in the computing environment); existing non-capital assets (tagging required within 1one year); and existing capital assets (tagging required within 1one year).

Question Requirement: 1763.07d2Organizational.910 / 0661.0

Change Count: 1

Field	Content
RequirementStatement	Documentation that a physical inventory has been taken, for all locations, is retained in the organization''s central accounting office. Further discrepancies in property inventories are investigated.

Question Requirement: 17.10aHICPOrganizational.2 / 2324.0

Change Count: 1

Field	Content
RequirementStatement	The organization does not use free or consumer e-mail systems for business purposes.

Question Requirement: 1792.10a2Organizational.7814 / 1238.0

Change Count: 1

Field	Content
RequirementStatement	The organization implements a formal System Development Lifecycle (SDLC), which covers request initiation, requirements definition, analysis, communication, conflict detection and resolution, and evolution of requirements. The organization''s security risk management process is integrated into all SDLC activities. Information security roles and responsibilities are defined and documented throughout the SDLC.

Question Requirement: 1723.03bHIXOrganizational.13 / 0411.0

Change Count: 2

Field	Content
RequirementStatement	Within every 365 days, the organization performs a documented assessment of a subset of the security and privacy controls attributable to a system or application in accordance with the Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchange's–such that all the controls are tested within a three year period.

IllustrativeProcedureMeasured	For example, measures indicate the number of risk assessments performed in accordance with the organization's policies. Further, the metrics indicate the number of security and privacy controls assessed on an annual basis to ensure that all controls are tested within a three year period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that within every 365 days, the organization performs a documented assessment of a subset of the security and privacy controls attributable to a system or application in accordance with the Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchange's - such that all the controls are tested within a three year period – to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements.

Question Requirement: 17.10aFTIOrganizational.8 / 2501.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12154.06iNYDOHOrganizational.13 / 2127.0

Change Count: 1

Field	Content
RequirementStatement	The information system takes the following actions in response to an audit failure or audit storage capacity issue: Shutdown the information system or halt processing immediately; and Systems that do not support automatic shutdown are shut down within 1one hour of the audit processing failure.

Question Requirement: 12153.06iNYDOHOrganizational.7 / 2126.0

Change Count: 2

Field	Content
RequirementStatement	The organization reviews and updates the list of auditable events no less often than every three hundred sixty-five [365] days, and whenever there is a significant system modification.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization reviews and updates the list of auditable events no less often than every three hundred sixty-five [365] days and whenever there is a significant system modification.

Question Requirement: 1250.09aaFTISystem.11 / 1133.1

Change Count: 1

Field	Content
RequirementStatement	The organization''s audit record generation capability audits: logons; logoffs; changes of password; all system administrator commands while logged on as system administrator; switching accounts; running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); creation or modification of super-user groups; a subset of security administrator commands, while logged on in the security administrator role; a subset of system administrator commands, while logged on in the user role; clearing of the audit log file; startup of audit functions; and shutdown of audit functions.

Question Requirement: 1201.06e2Organizational.4 / 0585.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides notice that the employee''s actions may be monitored, and the employee consents to such monitoring.

Question Requirement: 12148.06i1Organizational.1 / 2121.0

Change Count: 1

Field	Content
RequirementStatement	The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; and override of access control mechanisms.

Question Requirement: 1217.09ab3System.3 / 1156.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures automated alerts are generated for technical personnel to review and analyze, and suspicious activity or suspected violations are investigated as an integrated part of the organization''s formal incident response and investigations program.

Question Requirement: 1232.09c3Organizational.12 / 0829.0

Change Count: 1

Field	Content
RequirementStatement	The number of administrators is limited to the minimum necessary based upon each users'' role and responsibilities. Security personnel responsible for administering access controls do not perform audit functions for these controls.

Question Requirement: 12.09abCMSSystem.7 / 2611.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09abCMSSystem.8 / 2612.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1226.09af2System.2 / 1222.0

Change Count: 1

Field	Content
RequirementStatement	The organization synchronizes all system clocks and times where a computer or communications device has the capability to operate a real-time clock. This clock is set to an agreed standard received from industry-accepted time sources, either Coordinated Universal Time (UTC) or International Atomic Time and is accurate to within 30 seconds. The correct interpretation of the date/time format is used to ensure that the timestamp reflects the real date/time (e.g., daylight savings). The information system''s internal information system clocks synchronize daily and at system boot.

Question Requirement: 1259.09ab2System.9 / 1921.0

Change Count: 1

Field	Content
RequirementStatement	The organization responds to physical security incidents and coordinates results of reviews and investigations with the organization''s incident response capability.

Question Requirement: 111015.11aCCPAOrganizational.1 / 1923.0

Change Count: 1

Field	Content
RequirementStatement	Businesses notify consumers if there is unauthorized access to the consumer''s non-encrypted or non-redacted personal information due to the business''s lack of sufficient security controls.

Question Requirement: 11128.01tCMSSystem.2 / 1903.0

Change Count: 1

Field	Content
RequirementStatement	The organization requires that users log out when the time-period of expected inactivity exceeds 90 minutes, and at the end of the user''s normal work period. The information system automatically terminates the network connection at the end of the session; otherwise, the system forcibly deallocates DHCP leases after seven days AND forcibly disconnects VPN connections after 30 minutes or less of inactivity.

Question Requirement: 11.01qCMSSystem.5 / 2540.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01pCMSSystem.3 / 2517.0

Change Count: 3

Field	Content
RequirementStatement	The organization configures the information system to lock out the user account automatically after 3three invalid login attempts through either a local or network connection during a 15-minute time window and requires the lock out to persist for a minimum of 30 minutes or until released by an administrator.
IllustrativeProcedureImplemented	For example, obtain the password configuration settings for the applicable information systems and confirm that they have been configured to lock out the user account automatically after 3three invalid login attempts during a 15-minute time window.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of applicable systems that are in compliance with the organization's secure-logon procedures and meet the implementation requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization configures the information system to lock out the user account automatically after 3three invalid login attempts during a 15-minute time window and requires the lock out to persist for a minimum of 30 minutes or until released by an administrator.

Question Requirement: 11107.01pCMSSystem.3 / 1902.0

Change Count: 3

Field	Content
RequirementStatement	The organization configures the information system to lock out the user account automatically after 3three invalid login attempts during a 120-minute time window and requires the lock out to persist until released by an administrator.
IllustrativeProcedureImplemented	For example, obtain the password configuration settings for the applicable information systems and confirm that they have been configured to lock out the user account automatically after 3three invalid login attempts during a 120-minute time window.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of applicable systems that are in compliance with the organization's secure-logon procedures and meet the implementation requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization configures the information system to lock out the user account automatically after 3three invalid login attempts during a 120-minute time window.

Question Requirement: 11.01bFTISystem.2 / 2656.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01jFTIOrganizational.6 / 2576.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.09abFedRAMPSystem.9 / 2471.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01cFedRAMPSystem.4 / 2459.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01bFedRAMPSystem.10 / 2404.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01bFedRAMPSystem.6 / 2403.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01bFedRAMPSystem.4 / 2398.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01bFedRAMPSystem.3 / 2380.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01qFedRAMPSystem.7 / 2387.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01qFedRAMPSystem.5 / 2386.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.02iFedRAMPOrganizational.1 / 2392.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11970.01eNYDOHSystem.1 / 2043.0

Change Count: 3

Field	Content
RequirementStatement	The organization reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every ninety [90] days to validate the need for such privileges, and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every ninety [90] days to validate the need for such privileges, and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of personnel or roles defined in the applicable security plan that are reviewed, every ninety [90] days, to validate the need for assigned privileges to remain unchanged, reassigned, or removed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization reviews the privileges assigned to defined personnel or roles defined in the applicable security plan every ninety [90] days to validate the need for such privileges, and reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Question Requirement: 11177.09abHIXSystem.4 / 1195.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of systems that receive, process or store information that have / do not have intrusion detection monitoring implemented. Additionally, measures could indicate the duration from alert to resolution. Reviews, tests, or audits are completed by the organization to measure any gaps in intrusion detection as well as the effectiveness of the alert resolution process.

Question Requirement: 1166.01e2System.3 / 0100.0

Change Count: 1

Field	Content
RequirementStatement	User access rights are reviewed after promotions, demotions, and termination of employment or end of other arrangement with a workforce member ends. User access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization (i.e., transfer).

Question Requirement: 1150.01c2System.10 / 0042.0

Change Count: 1

Field	Content
RequirementStatement	The access control system for the system components storing, processing, or transmitting covered information is set with a default ""“deny-all”" setting.

Question Requirement: 1177.01j2Organizational.6 / 0129.0

Change Count: 1

Field	Content
RequirementStatement	User IDs assigned to vendors are reviewed in accordance with the organization''s access review policy, at a minimum annually.

Question Requirement: 11.02iFTIOrganizational.1 / 2579.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11967.01cNYDOHSystem.6 / 2040.0

Change Count: 3

Field	Content
RequirementStatement	The organization requires limits on the number of concurrent sessions for each system account to one [1] session for both normal and privileged users. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one [1] concurrent application/process session is documented in the security plan.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the information system limits the number of concurrent sessions for each system account to one [1] session for both normal and privileged users, and the number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one [1] concurrent application/process session is documented in the security plan.

IllustrativeProcedureMeasured	For example, measures indicate the percentage of information systems that require limits on the number of concurrent sessions for each system account as prescribed in the control requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the information system limits the number of concurrent sessions for each system account to one [1] session for both normal and privileged users, and the number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one [1] concurrent application/process session is documented in the security plan.

Question Requirement: 11962.01bNYDOHSystem.3 / 2035.0

Change Count: 3

Field	Content
RequirementStatement	The organization disables accounts of users posing a significant risk within sixty [60] minutes of discovery of the risk.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization implements procedures to disable accounts of users posing a significant risk within sixty [60] minutes of discovery of the risk.
IllustrativeProcedureMeasured	For example, measures indicate the number of accounts posing a significant risk that were disabled within sixty [60] minutes of discovery of the risk. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization disables accounts of users posing a significant risk within sixty [60] minutes of discovery of the risk.

Question Requirement: 11960.01bNYDOHSystem.1 / 2033.0

Change Count: 3

Field	Content
RequirementStatement	The information system automatically disables inactive accounts within sixty [60] days.
IllustrativeProcedureImplemented	For example, examine evidence (audit logs) that confirm the system automatically disables inactive accounts within sixty [60] days.
IllustrativeProcedureMeasured	For example, measures indicate the number of information systems that automatically disable inactive accounts within sixty [60] days. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the information system automatically disables inactive accounts within sixty [60] days.

Question Requirement: 10.01dCMSSystem.7 / 2608.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 10.01dCMSSystem.6 / 2607.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1011.01f1Organizational.1 / 0108.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures users are made aware of the organization''s password policies and requirements, are made aware to keep passwords confidential, avoid keeping a record (e.g., paper, software file, or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved, change passwords whenever there is any indication of possible system or password compromise, do not share individual user accounts or passwords, do not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks), do not use the same password for business and non-business purposes, and select quality passwords.

Question Requirement: 10.01dFTISystem.5 / 2589.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 10.01dFTISystem.4 / 2588.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 09215.09sNYDOHOrganizational.10 / 2187.0

Change Count: 3

Field	Content
RequirementStatement	Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections are acceptable and encouraged. HSTS headers specify a max-age of at least one [1] year.

IllustrativeProcedureImplemented	For example, examine evidence to confirm that allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections are acceptable and encouraged; and HSTS headers specify a max-age of at least one [1] year.
IllustrativeProcedureMeasured	For example, measures indicate the number of HTTP connections that have been redirected to HTTPS connections. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and confirm that HTTP connections for the sole purpose of redirecting clients to HTTPS connections are allowed; and HSTS headers specify a max-age of at least one [1] year.

Question Requirement: 0901.09s2Organizational.5 / 1051.0

Change Count: 1

Field	Content
RequirementStatement	An organization using electronic communication applications or systems for information exchange addresses the following: requirements (e.g., policies, standards) or guidelines are defined outlining acceptable use of electronic communication applications or systems; the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications; procedures are implemented for the use of wireless communications including an appropriate level of encryption; employee, contractor, and any other user''s responsibilities are defined to not compromise the organization (e.g., through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.); the required use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of covered information; the retention and disposal guidelines are defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and controls and restrictions are implemented associated with the forwarding of communications (e.g. automatic forwarding of electronic mail to external mail addresses).

Question Requirement: 09.09mHICPOrganizational.4 / 2331.0

Change Count: 1

Field	Content
RequirementStatement	The organization restricts the ""“send all”" function of email distribution lists to authorized individuals.

Question Requirement: 08.09nFedRAMPOrganizational.3 / 2418.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 08.09mFedRAMPOrganizational.5 / 2451.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 08.09nCMSOrganizational.5 / 2591.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0889.09nCMSOrganizational.1 / 0992.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the metric could indicate the number of connections from an information system to an external information system where the documentation of each connection is not policy compliant . Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements regardless of type if non-compliance with the requirements for interconnection security agreements can be ascertained. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that formal agreements with external information system providers include specific obligations for security and privacy.

Question Requirement: 0897.01mCISOrganizational.10 / 1901.0

Change Count: 1

Field	Content
RequirementStatement	The organization creates separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices (e.g., devices outside of the organization''s control). Enterprise access from this network is treated as untrusted and filtered and audited accordingly.

Question Requirement: 08102.09mCISOrganizational.22 / 0964.0

Change Count: 1

Field	Content
RequirementStatement	The organization deploys network level authentication via 802.1x to limit and control which devices can be connected to the network and integrates the 802.1x data with the organization''s automated inventory management system(s) to help identify authorized and unauthorized devices/systems on the network.

Question Requirement: 07.07aISO23894Organizational.2 / 2796.0

Change Count: 0

Field	Content
New Question Requirement	07.07aISO23894Organizational.2 / 2796.0

Question Requirement: 07.10mNIST80053Organizational.1 / 2782.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNIST80053Organizational.1 / 2782.0

Question Requirement: 07.07aNYDOHOrganizational.6 / 2722.0

Change Count: 0

Field	Content
New Question Requirement	07.07aNYDOHOrganizational.6 / 2722.0

Question Requirement: 07.10mNYDOHOrganizational.9 / 2713.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNYDOHOrganizational.9 / 2713.0

Question Requirement: 07.10mFTIOrganizational.8 / 2504.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07.10mFedRAMPOrganizational.16 / 2482.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07.10mFedRAMPOrganizational.15 / 2444.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07.10mFedRAMPOrganizational.13 / 2438.0

Change Count: 2

Field	Content
RequirementStatement	The organization remediates legitimate vulnerabilities in accordance with an organizational assessment of risk such that high-risk vulnerabilities are mitigated within thirty (30) days from date of discovery, moderate-risk vulnerabilities are mitigated within ninety (90) days from date of discovery, and low risk vulnerabilities are mitigated within one hundred and eighty (180) days from date of discovery.
DITA	Sampling

Question Requirement: 07.07aFedRAMPOrganizational.1 / 2465.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07239.10mNYDOHOrganizational.6 / 2211.0

Change Count: 2

Field	Content
RequirementStatement	The organization scans for vulnerabilities in the information system and hosted applications no less often than once every seventy-two [72] hours and when new vulnerabilities potentially affecting the system/applications are identified and reported.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization scans for vulnerabilities in the information system and hosted applications no less often than once every seventy-two [72] hours and when new vulnerabilities potentially affecting the system/applications are identified and reported.

Question Requirement: 0705.07a3Organizational.3 / 0634.0

Change Count: 1

Field	Content
RequirementStatement	The IT asset lifecycle program is monitored to ensure it effectively addresses all six stages of the lifecycle: planning - defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts; procurement - requisitioning, approving requisitions, ordering, receiving, and validating orders; deployment - tagging assets, entering asset information in a repository, configuring and installing assets including: disabling unnecessary or insecure services or protocols, limiting servers to one primary function, and defining system security parameters to prevent misuse; management - inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration; support - adding and changing configurations, repairing devices, and relocating equipment and software; and disposition - removing assets from service, deleting storage contents, disassembling components for reuse, surplussing equipment, terminating contracts, disposing of equipment, and removing assets from active inventory.

Question Requirement: 0756.10mPCIOrganizational.123 / 1424.0

Change Count: 1

Field	Content
RequirementStatement	The organization performs quarterly internal vulnerability scans and rescans, which may be automated, manual, or a combination thereof, as needed, until all ""high-risk"" vulnerabilities are resolved in accordance with the organizations vulnerability rankings. Scans are performed by qualified personnel. The organization performs quarterly external vulnerability scans, external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC), rescans as needed, until passing scans are achieved, internal scans, and external scans. The organization rescans as needed, after any significant change. Scans are performed by qualified personnel.

Question Requirement: 07.10mCMSOrganizational.8 / 2593.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0731.09r2Organizational.2 / 1035.0

Change Count: 1

Field	Content
RequirementStatement	The organization protects system documentation in accordance with the organization''s risk management strategy and distributes documentation to organization-defined personnel with the need for such documentation.

Question Requirement: 0730.09r2Organizational.3 / 1034.1

Change Count: 4

Field	Content
BaselineUniqueId	0730.09r2Organizational.13
CrossVersionId	1034.01
RequirementStatement	The organization obtains administrator documentation for the information system, system component, or information system service that describes: secure configuration, installation, and operation of the system, component, or service; effective use and maintenance of security and privacy functions/mechanisms; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. The organization obtains user documentation for the information system, system component, or information system service that describes: user-accessible security and privacy functions/mechanisms and how to effectively use those security functions/mechanisms; methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and user responsibilities in maintaining the security and privacy of the system, component, or service. Organizations document attempts to obtain information system documentation when such documentation is either unavailable or non-existent.
IllustrativeProcedureImplemented	For example, select a sample of systems and confirm that the organization has obtained administrator and user documentation for the information system, system component, or information system service. For administrator documentation, confirm that the following has been defined: (i) secure configuration, installation, and operation of the system, component, or service; (ii) effective use and maintenance of security and privacy functions/mechanisms; and, (iii) known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. For user documentation, confirm that the following has been defined: (i) user-accessible security and privacy functions/mechanisms and how to effectively use those security functions/mechanisms; (ii) methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and, (iii) user responsibilities in maintaining the security and privacy of the system, component, or service. Further confirm the organization documents attempts to obtain information system documentation when such documentation is either unavailable or non-existent.

Question Requirement: 0760.07aCISOrganizational.10 / 0640.0

Change Count: 1

Field	Content
RequirementStatement	The organization uses dynamic host configuration protocol (DHCP) logging on all DHCP or IP address management tools to improve the organization''s asset inventory.

Question Requirement: 06.06gNYDOHOrganizational.2 / 2728.0

Change Count: 0

Field	Content
New Question Requirement	06.06gNYDOHOrganizational.2 / 2728.0

Question Requirement: 06.06gNYDOHOrganizational.3 / 2721.0

Change Count: 0

Field	Content
New Question Requirement	06.06gNYDOHOrganizational.3 / 2721.0

Question Requirement: 06.01nNYDOHOrganizational.4 / 2714.0

Change Count: 0

Field	Content
New Question Requirement	06.01nNYDOHOrganizational.4 / 2714.0

Question Requirement: 06.06hTXRAMPOrganizational.2 / 2371.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0630.10h2System.6 / 1309.0

Change Count: 1

Field	Content
RequirementStatement	Physical or logical access is only given to suppliers for support purposes when necessary and with management approval. The supplier''s activities are monitored.

Question Requirement: 06.10kFTIOrganizational.6 / 2662.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.10kFTIOrganizational.5 / 2505.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.00aFTIOrganizational.4 / 2660.0

Change Count: 3

Field	Content
RequirementStatement	The organization develops, documents, and implements a configuration management plan for the system that is reviewed and approved by designated agencyorganizational personnel.
IllustrativeProcedureImplemented	For example, examine relevant evidence of the configuration management plan for the information system and confirm the plan is developed, documented, and implemented and that it has been reviewed and approved by designated agency organizational personnel.
IllustrativeProcedureMeasured	For example, the measure(s) could indicate whether the configuration management plan has been formally reviewed and approved by agencyorganizational personnel. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization develops, documents, and implements a configuration management plan for the system that is reviewed and approved by designated agencyorganizational personnel.

Question Requirement: 068.06g2Organizational.34 / 0603.0

Change Count: 1

Field	Content
RequirementStatement	The organization employs assessors or assessment teams to monitor the security controls in the information system on an ongoing basis as part of a continuous monitoring program. These teams will have a level of independence appropriate to the organization''s continuous monitoring strategy.

Question Requirement: 0604.06g2Organizational.2 / 0602.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s continuous monitoring program includes establishment of defined metrics to be monitored annually at a minimum, annual compliance assessments across the entire organization, third-party independent compliance assessments performed bi-annually, ongoing status monitoring in accordance with its continuous monitoring strategy, correlation and analysis of security-related information generated by assessments and monitoring, response actions to address results of these analyses, and reporting the security state of the information system to appropriate organizational officials monthly and, if required, to external agencies as required by that agency.

Question Requirement: 0672.10k3Organizational.6 / 1342.0

Change Count: 1

Field	Content
RequirementStatement	Any changes made to virtual machine images is logged. An alert is raised for any changes made to virtual machine images. Results of a change or move of an image and the subsequent validation of the image''s integrity is immediately available to the business owner(s) and/or customer(s) through electronic methods (e.g., portals or alerts).

Question Requirement: 06.10kFedRAMPOrganizational.11 / 2455.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.10kFedRAMPOrganizational.10 / 2454.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.10kFedRAMPOrganizational.8 / 2441.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.10kCMSOrganizational.9 / 2605.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 06.10kCMSOrganizational.8 / 2604.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0645.10kCMSOrganizational.12 / 1344.0

Change Count: 1

Field	Content
RequirementStatement	HHS-specific minimum security configurations are used for the following Operating System (OS) and Applications: HHS approved Windows Standards; Blackberry Server; Websense. For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is: USGCB; NIST National Checklist Program (NCP) The organization uses the following CMS hierarchy for implementing security configuration guidelines when an HHS-specific minimum security configuration does not exist, and to resolve configuration conflicts among multiple security guidelines: USGCB; NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order; Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); National Security Agency (NSA) STIGs; Iif formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as T, i.e., the Center for Internet Security [(CIS]), checklists;. In situations where no guidance exists, coordinate with CMS for guidance. CMS collaborates within CMS and the HHS Cybersecurity Program, and other OPDIVorganizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to: (a) establish baseline configurations and communicate industry and vendor best practices; and (b) ensure deployed configurations are supported for security updates. All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented.

Question Requirement: 04.01xCMSOrganizational.2 / 2548.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0415.01y1Organizational.10 / 0284.0

Change Count: 1

Field	Content
RequirementStatement	Suitable protection of the teleworking site is in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization''s internal systems, or misuse of facilities.

Question Requirement: 0429.01x1Organizational.5 / 0273.0

Change Count: 2

Field	Content
RequirementStatement	The organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).
IllustrativeProcedureMeasured	For example, measures indicate the number of mobile devices that have been appropriately configured to prevent users from circumventing built-in security controls, as a percentage of all mobile devices. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).

Question Requirement: 0404.01x1Organizational.5 / 0270.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, determine whether specific mobile devices given to personnel traveling to high -risk locations are specially configured. Examine evidence that the mobile devices are checked for tampering and malware upon return. Confirm that personnel physically observe the mobile devices for tampering and anti-malware scans are performed.

Question Requirement: 0413.01xFTIOrganizational.2 / 0279.0

Change Count: 1

Field	Content
RequirementStatement	When FTI is used in a mobile device environment, mobile device management controls are in place that include security policies, security procedures, inventories of all mobile devices accessing FTI, and standardized security configurations for all mobile devices. An annual risk assessment is conducted on the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI. Protection mechanisms are in place in case a mobile device is lost or stolen. All data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards. All data communication with the organization''s internal network is encrypted using a cryptographic module that is FIPS 140-2 compliant. The organization must control end-user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications. All mobile device management servers that receive, process, store, or transmit FTI are hardened. A centralized mobile device management solution is used to authenticate organization-issued and personally owned mobile devices prior to allowing access to the internal network. Security events are logged for all mobile devices and the mobile device management server. The organization disables wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, is disabled to the extent possible. Disposal of all mobile device component hardware follows the same media sanitization and disposal procedures as other media.

Question Requirement: 03.07eNYDOHOrganizational.2 / 2725.0

Change Count: 0

Field	Content
New Question Requirement	03.07eNYDOHOrganizational.2 / 2725.0

Question Requirement: 03.09qFedRAMPOrganizational.1 / 2399.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0301.09o2Organizational.2 / 0999.0

Change Count: 1

Field	Content
RequirementStatement	The organization formally establishes and enforces controls (e.g., policies and procedures) for the management of removable media and laptops including: restrictions on the type(s) of media, and usages thereof to maintain security; and registration of certain type(s) of media and laptops. Media containing covered and/or confidential information is physically stored and its data encrypted in accordance with the organization''s data protection and privacy policy on the use of cryptographic controls until the media are destroyed or sanitized and commensurate with the confidentiality and integrity requirements for its data classification level.

Question Requirement: 02.01gFedRAMPOrganizational.2 / 2414.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0201.09j1Organizational.124 / 0873.0

Change Count: 1

Field	Content
RequirementStatement	Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization''s business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.

Question Requirement: 0207.09j1Organizational.6 / 0880.0

Change Count: 1

Field	Content
RequirementStatement	Centrally managed spam protection mechanisms are employed at information system entry and exit points, workstations, servers, and mobile computing devices on the network. Spam protection mechanisms detect and take action on unsolicited messages transported by electronic mail, transported by electronic mail attachments, transported by Web accesses, transported by other common means, and inserted through the exploitation of information system vulnerabilities. Malicious code and spam protection mechanisms are centrally managed and updated when new releases are made available in accordance with the organization''s configuration management policy and procedures.

Question Requirement: 01.02bNYDOHOrganizational.1 / 2717.0

Change Count: 0

Field	Content
New Question Requirement	01.02bNYDOHOrganizational.1 / 2717.0

Question Requirement: 01.09qNYDOHOrganizational.4 / 2712.0

Change Count: 0

Field	Content
New Question Requirement	01.09qNYDOHOrganizational.4 / 2712.0

Question Requirement: 01.00aISO27001Organizational.1 / 2697.0

Change Count: 0

Field	Content
New Question Requirement	01.00aISO27001Organizational.1 / 2697.0

Question Requirement: 01.07bVAD6500Organizational.1 / 2694.0

Change Count: 0

Field	Content
New Question Requirement	01.07bVAD6500Organizational.1 / 2694.0

Question Requirement: 01.00aTXRAMPOrganizational.1 / 2687.0

Change Count: 0

Field	Content
New Question Requirement	01.00aTXRAMPOrganizational.1 / 2687.0

Question Requirement: 01100.05aPCIOrganizational.1 / 0452.0

Change Count: 1

Field	Content
RequirementStatement	When being assessed as a service provider, the organization''s executive management establishes: responsibility for the protection of cardholder data; a PCI DSS compliance program which includes overall accountability for maintaining PCI DSS compliance; a PCI DSS compliance program which includes defining a charter for a PCI DSS compliance program; and a PCI DSS compliance program which includes communication to executive management.

Question Requirement: 01.00aCMSOrganizational.1 / 2513.0

Change Count: 1

Field	Content
RequirementStatement	The organization develops and disseminates an organization-wide information security program plan that: provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. The organization: reviews the organization-wide information security program plan within every three hundred sixty-five (365) days; updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and protects the information security program plan from unauthorized disclosure and modification.

Question Requirement: 01.02bCMSOrganizational.2 / 2512.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0166.05b2Organizational.6 / 0455.0

Change Count: 1

Field	Content
RequirementStatement	Information security coordination: involves active cooperation and collaboration across the entire organization; ensures that security activities across the entire organization are executed in compliance with the information security policy; ensures that security policy deviations are identified and reviewed; identifies how to handle non-compliance (such as sanctions or disciplinary action); assesses the adequacy of the implementation of information security controls; coordinates the implementation of information security controls; effectively promotes information security education, training, and awareness throughout the organization; ensures that threat information has been communicated to identified to internal stakeholders; and ensures that threat information has been communicated to identified external stakeholders.

Question Requirement: 0128.05b2Organizational.126 / 0456.0

Change Count: 1

Field	Content
RequirementStatement	Information security coordination: involves the active cooperation and collaboration across the entire organization to include managers, users, administrators, application designers, auditors, and security personnel; also includes specialist skills in areas such as insurance, legal issues, human resources, privacy, IT, or risk management; addresses deviations via a risk acceptance process; approves methodologies and processes for information security management activities (e.g., risk acceptance, information classification, security incidents); identifies and promptly reports to senior management significant threat changes and exposure of information and information processing resources to threats; evaluates information received from the monitoring and reviewing of information security activities to identify ""lessons learned"", and recommends to senior management appropriate actions in response to identified information security incidents; creates an internal security information sharing mechanism, such as an email group, periodic conference call, or standing meeting; and establishes an internal reporting mechanism, such as a telephone hotline or dedicated email address, to allow security contacts to report information security incidents or obtain security policy clarifications on a timely basis. An internal information security sharing mechanism has been created to ensure security-related activities affecting the information system are planned and coordinated with appropriate stakeholders before conducting such activities in order to reduce the impact on other organizational entities. The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on other organizational entities.

Question Requirement: 0167.05b2Organizational.4 / 0458.0

Change Count: 1

Field	Content
RequirementStatement	The organization distributes copies of the information system''s security plan to appropriate individuals and offices (e.g., CCO, CIO, business units), communicates changes to the security plans to appropriate individuals and offices, and protects the plan from unauthorized disclosure and modification.

Question Requirement: 0118.05a2Organizational.6 / 0441.0

Change Count: 1

Field	Content
RequirementStatement	Senior management: formally appoints a senior-level information security official for the development, implementation, and administration of security matters; formally establishes and communicates the organization''s priorities for organizational mission, objectives, and activities; ensures that the organization''s information security processes are in place; ensures that the organization''s information security processes are communicated to all stakeholders; formally ensures that the organization''s information security processes consider and address organizational requirements; formally assigns an organization single point of contact or group to provide program oversight (governance), review and update the organizations security plan (strategy, policies, etc.), ensure compliance with the security plan by the workforce, and evaluate and accept information security risk on behalf of the organization (e.g., CEO, COO, Security Steering Committee, etc.); formulates, reviews, and approves information security policies and a policy exception process; periodically, at a minimum, annually, reviews and assesses the effectiveness of the implementation of the information security policy; provides clear direction and visible management support for security initiatives; provides the resources needed for information security; initiates plans and programs to maintain information security awareness; ensures that all appropriate measures are taken to avoid cases of identity theft targeted at clients/customers, employees, and third parties; ensures that the implementation of information security controls is coordinated across the organization; and determines and coordinates, as needed, internal or external information security specialists, and review and coordinate results of the specialists'' advice throughout the organization.

Question Requirement: 0123.05a2Organizational.4 / 0447.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine the organization's organizational chart and confirm that security contacts have been appointed in each major organizational area or business unit and that the appointments have been formally documented in writing. Select a sample of business units and identify and confirm whether a security contact has been appointed by name. Confirm their roles and responsibilities as part of the information protection program.

Question Requirement: 0121.05a2Organizational.12 / 0445.0

Change Count: 1

Field	Content
RequirementStatement	The organization: ensures that organization''s information security strategy and goals are identified and considered; ensures that organization''s information security strategy and goals address organizational and business-specific requirements; and verifies that appropriate processes are in place to meet the organization''s strategy and goals. Risk management programs, including the risk acceptance process, are formally approved, and reviewed in writing.

Question Requirement: 01111.05a2Organizational.5 / 0448.0

Change Count: 1

Field	Content
RequirementStatement	The CISO reports in writing on the cybersecurity program and material cybersecurity risks at least annually to the board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, reporting is made to the individual or committee responsible for the organization''s cybersecurity program. The report includes, to the extent applicable: the confidentiality of nonpublic information and the integrity and security of the organization''s information systems; the organization''s cybersecurity policies and procedures; material cybersecurity risks to the organization; the overall effectiveness of the organization’s cybersecurity program; and material cybersecurity events involving the organization during the time period addressed by the report.

Question Requirement: 0119.05a2Organizational.7 / 0442.0

Change Count: 1

Field	Content
RequirementStatement	Senior management formally appoints security specialists and reviews and coordinates results of the security specialists'' advice throughout the organization.

Question Requirement: 0182.06a2Organizational.12 / 0544.0

Change Count: 1

Field	Content
RequirementStatement	The organization joins industry trade associations, subscribes to thought leadership and market/security research organizations, or establishes some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal, and regulatory environment trends that may impact the organization''s security policies. Consequences of business sector, industry, technology, infrastructure, legal and regulatory environment trends impacting the organizations security policies are incorporated into the development or update of IT policies and procedures.

Question Requirement: 01.02fFedRAMPOrganizational.1 / 2405.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 01106.05bFedRAMPOrganizational.1 / 0463.0

Change Count: 1

Field	Content
RequirementStatement	Security plans are reviewed at least annually, when changes are made to the information system or information protection requirements, or when incidents occur that impact the plans'' validity.

Question Requirement: 01.07bFedRAMPOrganizational.1 / 2370.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0102.00a2Organizational.123 / 0002.0

Change Count: 1

Field	Content
RequirementStatement	The information security management program (ISMP) has been established, implemented, operational, monitored, reviewed, and maintained. The ISMP is formally documented, protected, controlled, and retained according to federal, state and organizational requirements. The ISMP also incorporates a Plan, Do, Check, ACTct (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the ISMP, or indicates any shortcomings of the ISMP.

Question Requirement: 0135.02f1Organizational.56 / 0362.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal sanctions process: includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action; identifies the individual sanctioned; and identifies the reason for the sanction. The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. The organization notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated.

Question Requirement: 0117.05a1Organizational.1 / 0440.0

Change Count: 1

Field	Content
RequirementStatement	A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization''s information security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.

Question Requirement: 0114.04b1Organizational.1 / 0435.0

Change Count: 1

Field	Content
RequirementStatement	The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies'' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.

Question Requirement: 0113.04a1Organizational.2 / 0431.1

Change Count: 1

Field	Content
RequirementStatement	The organization''s information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management''s commitment; describe management and workforce members'' roles and responsibilities; and establish the organization''s approach to managing information security.

Question Requirement: 01.02fFTIOrganizational.2 / 2644.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 01.02fFTIOrganizational.1 / 2532.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 01.02bFTIOrganizational.4 / 2659.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0149.02bFTIOrganizational.2 / 0314.1

Change Count: 1

Field	Content
RequirementStatement	OThe organizations must initiates a background investigation for all newly hired employees, contractors, and sub-contractors who will require access to FTI to perform assigned duties. Background investigations for any individual granted access to FTI must include, at a minimum, FBI fingerprinting (FD-258),; check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the lastprior five (5) years, and if applicable, of the appropriate agency for any identified arrests,; and citizenship/residency. Agencies must The organization establishes a written background investigation policy that conforms to the standards of Publication 1075.

Question Requirement: 01.02aFTIOrganizational.2 / 2625.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 01.02aFTIOrganizational.1 / 2624.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 01.05bFTIOrganizational.5 / 2622.0

Change Count: 1

Field	Content
RequirementStatement	The organization develops security and privacy plans for the system that: are consistent with the organization's enterprise architecture; explicitly define the constituent system components; describe the operational context of the system in terms of mission and business processes; identify the individuals that fulfill system roles and responsibilities; identify the information types processed, stored, and transmitted by the system; provide the security categorization of the system, including supporting rationale; describe any specific threats to the system that are of concern to the organization; provide the results of a privacy risk assessment for systems processing personally identifiable information; describe the operational environment for the system and any dependencies on or connections to other systems or system components; provide an overview of the security and privacy requirements for the system; identify any relevant control baselines or overlays, if applicable; describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; include risk determinations for security and privacy architecture and design decisions; include security- and privacy-related activities affecting the system that require planning and coordination with authorized agency personnel; and are reviewed and approved by the authorizing official or designated representative prior to plan implementation. The organization: distributes copies of the security and privacy plans and communicates subsequent changes to the plans to designated agency officials; distributes copies of the plans and communicates subsequent changes to the plans to authorized agency personnel; reviews the plans at a minimum annually (or as a result of a significant change); updates the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and protects the plans from unauthorized disclosure and modification.

Question Requirement: 19.13jNIST80053Organizational.4 / 2785.0

Change Count: 0

Field	Content
New Question Requirement	19.13jNIST80053Organizational.4 / 2785.0

Question Requirement: 19.13gNIST80053Organizational.1 / 2780.0

Change Count: 0

Field	Content
New Question Requirement	19.13gNIST80053Organizational.1 / 2780.0

Question Requirement: 19.13kNIST80053Organizational.1 / 2779.0

Change Count: 0

Field	Content
New Question Requirement	19.13kNIST80053Organizational.1 / 2779.0

Question Requirement: 19.13mNIST80053Organizational.1 / 2778.0

Change Count: 0

Field	Content
New Question Requirement	19.13mNIST80053Organizational.1 / 2778.0

Question Requirement: 19.13kPHIPAOrganizational.25 / 2777.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.25 / 2777.0

Question Requirement: 19198.10cPRVSystem.1 / 1284.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s systems processing personal health information: ensures that each subject of care can be uniquely identified within the system; and are capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Question Requirement: 19981.06dGroupPlansOrganizational.1 / 2012.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, but not limited to, obtain and examine the data protection and privacy policy and procedures, and examine evidence to confirm that the Group Health Plan documents incorporate provisions to require the plan sponsor to: i) implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information (ePHI) created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan, except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to 45 CFR § 164.504(f)(1)(ii) or (iii), or as authorized under 45 CFR § 164.508; ii) ensure that adequate separation is supported by reasonable and appropriate security measures; iii) ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and iv) report to the group health plan any security incident of which it becomes aware.
IllustrativeProcedureMeasured	For example, measures indicate whether all plan documents have incorporated the required provisions and that plan sponsors have implemented the appropriate safeguards to protect electronic protected health information. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the Group Health Plan documents incorporate provisions to require the plan sponsor to: i) implement administrative, physical, and technical safeguards to reasonably and appropriately protect electronic protected health information (ePHI) created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan, except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to 45 CFR § 164.504(f)(1)(ii) or (iii), or as authorized under 45 CFR § 164.508; ii) ensure that adequate separation is supported by reasonable and appropriate security measures; iii) ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and iv) report to the group health plan any security incident of which it becomes aware.

Question Requirement: 19495.13lGroupPlansOrganizational.1 / 1679.0

Change Count: 1

Field	Content
RequirementStatement	Requirements have been defined for subjecting amended plan documents to the organization''s retention policy.

Question Requirement: 19.13tCMSOrganizational.2 / 2670.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19.13tCMSOrganizational.1 / 2669.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19315.13b1Organizational.2 / 1790.0

Change Count: 1

Field	Content
RequirementStatement	Organizations provide effective notice to data subjects regarding: its activities that impact privacy including, but not limited to, the collection, use, sharing, safeguarding, maintenance, and disposal of PII; authority for collecting PII; the PII collected, the purpose(s) for which it is collected and how it will be protected; the choice, if any, data subject may have regarding how the PII controller uses PII and the consequence of exercising or not exercising those choices; the ability to object to the processing; if the PII controller intends to levy any fees for access, as may be permitted by law in some jurisdictions; how long the PII will be retained; how data subjects may obtain access to their PII for the purpose of amendment or correction, where appropriate; whether the PII controller shares PII with external entities and the purposes for such sharing; whether the organization on-sells or forwards the data for processing by data analytics organizations and the details applicable to PII risks; and how data subjects are able to communicate with the organization''s privacy officials to provide feedback, including but not limited to complaints and/or direct questions regarding privacy practices.

Question Requirement: 19293.13a1Organizational.1 / 1566.0

Change Count: 1

Field	Content
RequirementStatement	PII controllers provide a plain-language notice to data subjects: which outline the controller’s practices and policies regarding PII; in a manner and time frame required by applicable law and/or regulation; and in a manner that can be understood by individuals not familiar with information technologies, legal jargon and the Internet.

Question Requirement: 19410.13h1Organizational.2 / 1843.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, obtain and review the organization privacy compliance documentation and/or forms used to collect PII and to determine if the organization has identified the specific purpose(s) of collecting PII and it is clearly described. Review complaints from a victim, ethics and/or compliance hotline to determine if complaints about an unclear PII collection has been made. Examine related legal and HR documentation, if available.

Question Requirement: 19403.13g1Organizational.3 / 1837.0

Change Count: 1

Field	Content
RequirementStatement	Organizations will develop and implement guidelines that ensures the processing of PII complies with all applicable laws and regulations and its interpretation by competent authorities. The overall context of the PII processing will be considered when determining purpose legitimacy. This includes the relationship between the organization and the data subjects, scientific and technological developments, and social and cultural changes.

Question Requirement: 19375.13f1Organizational.8 / 1824.0

Change Count: 1

Field	Content
RequirementStatement	PII processors support the PII controller’s facilitation of the exercise of data subject’’s rights to access, correct or delete their PII.

Question Requirement: 19497.13m1Organizational.2 / 1857.0

Change Count: 1

Field	Content
RequirementStatement	Upon collection or creation of PII, organizations, where practicable, will confirm the accuracy of the PII, relevance of the PII, and completeness of the PII. Organizations will check applicable programs or systems for inaccurate or outdated PII and correct inaccurate or outdated PII, as necessary.

Question Requirement: 19605.13m2Organizational.1 / 1671.0

Change Count: 1

Field	Content
RequirementStatement	The organization requests that the individual or individual’’s authorized representative validate PII during the collection process, and periodically revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually.

Question Requirement: 19.06cFTIOrganizational.4 / 2587.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19139.06bFTIOrganizational.1 / 0550.0

Change Count: 1

Field	Content
RequirementStatement	The organization establishes restrictions on the use of open source software. Any open source software used by the organization is legally licensed, approved by the organization''s IT department, and adheres to a secure configuration baseline checklist from the U.S. Government or industry.

Question Requirement: 19.06fFTIOrganizational.1 / 2562.0

Change Count: 1

Field	Content
RequirementStatement	The organization determines the cryptographic uses and implements the cryptography required for each specified cryptographic use (e.g., Latest FIPS-140 validated encryption mechanism, NIST 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, encryption in transit).

Question Requirement: 19440.13kHIPAAOrganizational.12 / 1852.0

Change Count: 2

Field	Content
RequirementStatement	A business associate, or equivalent, only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the covered entity, or equivalent, except if such uses or disclosures are permitted by its contract or other arrangement.
IllustrativeProcedureImplemented	For example, select a sample of uses or disclosures of PHI/PII and confirm that the business associate, or equivalent (such as an agent), did not use or disclose the PHI in a manner that would violate requirements for the protection of such information except as permitted by its contract or other arrangement.

Question Requirement: 19439.13kHIPAAOrganizational.11 / 1851.0

Change Count: 1

Field	Content
RequirementStatement	The business associate discloses PHI to an individual when requested or required under federal or state law and required by the Secretary of Health and Human Services to investigate or determine the business associate''s compliance with the HIPAA Privacy Rule, and as necessary to satisfy a covered entity''s obligations with respect to an individual''s request for an electronic copy of PHI.

Question Requirement: 19438.13kHIPAAOrganizational.10 / 1681.0

Change Count: 1

Field	Content
RequirementStatement	The organization, acting as a covered entity, discloses PHI to an individual when requested or required under federal or state law and when required by the Secretary of Health and Human Services to investigate or determine the covered entity or business associate''s compliance with the HIPAA Privacy Rule, and the covered entity, individual, or individual''s designee, as necessary to satisfy a covered entity''s obligations with respect to an individual''s request for an electronic copy of PHI.

Question Requirement: 19437.13kHIPAAOrganizational.9 / 1643.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the use or disclosure of PHI. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that organization's disclosures of PHI are consistent with applicable law and standards of ethical conduct, to the extent allowed if the organization, in good faith, believes the use or disclosure is reasonable or necessary for safety or law enforcement.

Question Requirement: 19614.13kHIPAAOrganizational.27 / 1630.0

Change Count: 1

Field	Content
RequirementStatement	PHI related to victims of a crime is only disclosed to law enforcement subject to specifically defined criteria as required by HIPAA § 164.512(f)(3). Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosures are made by the individual who agrees to the disclosure or by the covered entity when unable to obtain the individual''s agreement because of incapacity or other emergency circumstances subject to an exercise of professional judgment.

Question Requirement: 19449.13kHIPAAOrganizational.21 / 1775.0

Change Count: 3

Field	Content
RequirementStatement	The organization, acting as a covered entity, or equivalent, will ensure that if an individual is not present or if the opportunity to agree or object to the use or disclosure cannot practicably be provided, it only allows uses or provides disclosures of PHI to a person that is directly relevant to that person's involvement with the individual's health care, as specified in HIPAA § 164.510(b)(3).
IllustrativeProcedureImplemented	For example, interview a representative sample of personnel responsible for the disclosure of PHI and determine if they ensure, when an individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided, they only allow uses or provide disclosure of PHI to a person that is directly relevant to that person's involvement with the individual's health care, in accordance with HIPAA § 164.510(b)(3). Ask for relevant documentation to substantiate the process and their compliance with the policy requirements. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for disclosing PHI contrary to the requirements specified in HIPAA § 164.510(b)(3) when an individual is not present or does not have the capacity to agree or object to disclosure. Review complaints from an ethics and/or compliance hotline to determine if complaints about inappropriate disclosures as specified in HIPAA § 164.510(b)(3) have been made. Interview human resources personnel to determine if workforce members have been disciplined for inappropriate disclosure of PHI contrary to the requirements outlined in HIPAA § 164.510(b)(3). Examine related legal and HR documentation, if available.
IllustrativeProcedureMeasured	For example, the measure(s) could indicate the number of inappropriate disclosures of PHI to a person when the individual is not present as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of the reason, if disclosures contrary to the requirements outlined in HIPAA § 164.510(b)(3) can be discerned. Note a measure could include regular or ad hoc reports or audits of disclosures if they considered the policy requirements. If a metric or measure adequately evaluates the requirements for disclosures when an individual is not present as described in HIPAA § 164.510(b)(3), determine if the measure is tracked over time and if performance goals have been established. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity, or equivalent, ensures that, when an individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided, it only allows uses or provides disclosures of PHI to a person that is directly relevant to that person's involvement with the individual's health care.

Question Requirement: 19448.13kHIPAAOrganizational.20 / 1616.0

Change Count: 1

Field	Content
RequirementStatement	If the organization discloses PHI to a family member, or other relative, or a close personal friend of the individual, or any other person identified by the individual, or to assist and locate such a person, the disclosure is limited to that PHI directly relevant to the person''s involvement with the individual''s care or payment related to such care, or otherwise limited to the requirements for limited uses and disclosures when the individual is not present, for disaster relief purposes, or for a deceased individual, as specified in HIPAA § 164.510(b)(1).

Question Requirement: 19430.13kHIPAAOrganizational.2 / 1624.0

Change Count: 3

Field	Content
RequirementStatement	The organization complies with the regulatory criteria for permitted uses and disclosures of PHI for public health activities (e.g., for purposes including preventing or controlling disease; reporting incidents of child abuse or neglect; relating to the jurisdiction of the Food and Drug Administration; intervention or investigation of communicable diseases; work-related illness or injury; or to disclose proof of immunization) prior to the use or disclosure for said activities, as required by HIPAA § 164.512(b).
IllustrativeProcedureImplemented	For example, inquire of management as to whether the entity discloses PHI for public health activities (e.g., for purposes including preventing or controlling disease; reporting incidents of child abuse or neglect; relating to the jurisdiction of the Food and Drug Administration; intervention or investigation of communicable diseases; work-related illness or injury; or to disclose proof of immunization) as required by HIPAA § 164.512(b). Obtain and review a sample of such uses/disclosures and determine whether all the performance criteria were met. Examine security and privacy incident reports to determine if PHI has been disclosed inappropriately. Interview a representative sample of personnel responsible for handling patient/client information to determine if written or ad hoc procedures are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the regulatory criteria for permitted uses and disclosures of PHI for public health activities prior to the use or disclosure for said activities. Review complaints from an ethics and/or compliance hotline to determine if complaints of inappropriate or unauthorized disclosure as a result of the entity's failure to comply. Interview human resources personnel to determine if workforce members have been disciplined for unauthorized disclosure as the result of a failure to comply with the regulatory criteria for permitted uses and disclosures of PHI for public health activities prior to the use or disclosure for said activities. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI as a result of the entity's failure to comply with the regulatory criteria for permitted uses and disclosures of PHI for public health activities prior to the use or disclosure of said activities as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of type, if the unauthorized public health activity disclosures can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity (or equivalent) complies with the regulatory criteria for permitted uses and disclosures of PHI for public health activities prior to the use or disclosure for said activities.

Question Requirement: 19429.13kHIPAAOrganizational.1 / 1771.0

Change Count: 3

Field	Content
RequirementStatement	The organization, acting as a covered entity, or equivalent, limits permitted use and/or disclosure of PHI to the individual for treatment, payment, or healthcare operations appropriately and not in a manner inconsistent with uses or disclosures that require authorization or are otherwise prohibited, as required by HIPAA.
IllustrativeProcedureImplemented	For example, inquire of management if PHI is used appropriately for treatment, payment. or healthcare operations. Obtain and review a sample of programs/material used to train personnel involved in treatment, payment, or operations and evaluate the content relative to the specified criteria to determine if the use or disclosure of PHI for treatment, payment, or healthcare operations described is consistent with the requirements specified by law, such as in HIPAA. Interview personnel involved in treatment, payment, or operations to determine if written or ad hoc procedures regarding the use and disclosure of PHI in treatment, payment, or operations are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation as the result of an inappropriate use or disclosure for treatment, payment, or operations. Review complaints from a victim, ethics and/or compliance hotline to determine if there were complaints about inappropriate or unauthorized use or disclosure of PHI for treatment, payment, or operations. Interview human resources personnel to determine if workforce members have been disciplined for an inappropriate use or disclosure of PHI for treatment, payment, or operations. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, the measures(s) could indicate the number of inappropriate disclosures of PHI for treatment, payment, or operations contrary to the requirements specified by law, such as in HIPAA during a specific time period. Non-compliance with the policy requirements could be part of a broader metric that considers all inappropriate or unauthorized disclosures, regardless of type, if the inappropriate or unauthorized disclosures of PHI for treatment, payment ,or operations, as required by law, such as HIPAA, can be discerned. If a metric or measure adequately evaluates the requirement for the use and disclosure of PHI for treatment, payment, or operations, determine if the measure is tracked over time and if performance goals have been established. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity, or equivalent, uses and discloses PHI for treatment, payment, or healthcare operations appropriately and not in a manner inconsistent with uses or disclosures that require authorization or are otherwise prohibited.

Question Requirement: 19612.13kHIPAAOrganizational.25 / 1680.0

Change Count: 3

Field	Content
RequirementStatement	In certain instances, an organization uses or discloses protected health informationPHI without the written authorization of the individual or the opportunity for the individual to agree or object and to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law.
IllustrativeProcedureImplemented	For example, select a sample of uses or disclosures of PHI/PII and confirm that the covered entity (or equivalent) used or disclosed the PHI/PII (i) without the written authorization of the individual or the opportunity for the individual to agree or object and (ii) to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law in accordance with the policy requirements and documented procedures.
IllustrativeProcedureMeasured	For example, the measure(s) could indicate the number of incidents of use or disclosure of PHI and whether it met the following: (i) used/disclosed without the written authorization of the individual or the opportunity for the individual to agree or object and (ii) used/disclosed to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, in certain instances, a covered entity (or equivalent) may use or disclose protected health information PHI (i) without the written authorization of the individual or the opportunity for the individual to agree or object and (ii) to the extent that such use or disclosure is required by law and the use or disclosure complies with, and is limited to, the relevant requirements of such law.

Question Requirement: 19433.13kHIPAAOrganizational.5 / 1627.0

Change Count: 3

Field	Content
RequirementStatement	The organization will ensure satisfactory assurances are obtained before providing the appropriate disclosures of PHI pursuant to court orders, subpoenas, or discovery requests for judicial and administrative proceedings, as stipulated in HIPAA § 164.512(e).
IllustrativeProcedureImplemented	For example, inquire of management as to whether satisfactory assurances are obtained prior to the disclosure of PHI in the course or any judicial or administrative proceeding as required by HIPAA § 164.512(e). Obtain and review a sample of disclosures and the corresponding court orders, subpoenas, or discovery requests for judicial and administrative proceedings and determine if disclosures are appropriate. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the disclosure of PHI is in response to an order of a court or administrative tribunal, or a subpoena, discovery request, or other lawful process. Verify disclosure of PHI in the course of any judicial or administrative proceeding is appropriate. Examine security and privacy incident reports to determine if PHI has been disclosed inappropriately. Interview a representative sample of personnel responsible for handling patient/client information to determine if written or ad hoc procedures are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the regulatory criteria for obtaining satisfactory assurances as required by HIPAA § 164.512(e). Review complaints from an ethics and/or compliance hotline to determine if there were complaints about inappropriate or unauthorized disclosure as the result of a failure to obtain the required satisfactory assurances. Interview human resources personnel to determine if workforce members have been disciplined for unauthorized disclosure as the result of such a failure. Examine related legal and HR documentation, if available.
IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI as the result of a failure to obtain satisfactory assurances before providing appropriate disclosures of PHI pursuant to court orders, subpoenas, or discovery requests for judicial and administrative proceedings as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of type, if failures to obtain satisfactory assurances as required under HIPAA § 164.512(e) can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity (or equivalent) ensures that satisfactory assurances are obtained before providing the appropriate disclosures of PHI pursuant to court orders, subpoenas, or discovery requests for judicial and administrative proceedings.

Question Requirement: 19432.13kHIPAAOrganizational.4 / 1626.0

Change Count: 3

Field	Content
RequirementStatement	The organization discloses PHI to a health oversight agency only for those oversight activities authorized by law, as stipulated in HIPAA § 164.512(d).
IllustrativeProcedureImplemented	For example, inquire of management as to whether PHI is disclosed to appropriate health oversight agencies only for those oversight activities authorized by law, as stipulated in HIPAA § 164.512(d). Obtain a sample of disclosures made for this purpose and verify that criteria specified by law, such as in HIPAA § 164.512(d), have been applied appropriately. Examine security and privacy incident reports to determine if PHI has been disclosed inappropriately. Interview a representative sample of personnel responsible for handling patient/client information to determine if written or ad hoc procedures are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the regulatory criteria for permitted uses and disclosures of PHI to a health oversight agency for lawfully authorized oversight activities. Review complaints from an ethics and/or compliance hotline to determine if there were complaints about inappropriate or unauthorized disclosure to a health oversight agency. Interview human resources personnel to determine if workforce members have been disciplined for unauthorized disclosure to a health oversight agency. Examine related legal and HR documentation, if available.
IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI to a health oversight agency as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of type, if the unauthorized health oversight agency disclosures can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity (or equivalent) discloses PHI to a health oversight agency only for those oversight activities authorized by law.

Question Requirement: 19622.13kHIPAAOrganizational.35 / 1642.0

Change Count: 1

Field	Content
RequirementStatement	PHI is only disclosed for purposes of workers'' compensation or similar programs to the extent necessary to comply with related laws and regulations per the requirements outlined in HIPAA § 164.512(l). Based on the complexity of the entity, policy elements to consider include, but are not limited to, whether a disclosure is authorized by and to the extent necessary to comply with laws relating to workers'' compensation and whether it is related to the provision of benefits for work-related injuries, or illness, without regard to fault.

Question Requirement: 19419.13jHIPAAOrganizational.1 / 1718.0

Change Count: 3

Field	Content
RequirementStatement	The covered entity, or equivalent, makes reasonable efforts to limit requests for PHI to, or from, another covered entity or, business associate, or equivalent, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Exceptions include, but are not limited to, treatment, requests by the individual, or uses or disclosures pursuant to a valid authorization, required by law, or required for compliance with other requirements, such as (for example, disclosures made to the Secretary of Health and Human Services).
IllustrativeProcedureImplemented	For example, inquire of management as to whether access to PHI is restricted based on a workforce member's job requirements (duties). Interview a representative sample of key staff involved in the exchange of PHI with another covered entity or, business associate, or equivalent, to determine if the minimum necessary criteria are understood and the exchanges are compliant with HIPAAapplicable laws. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation as the result of an inappropriate or unauthorized disclosure of PHI due to a failure to limit the PHI disclosed to or received from another covered entity or, business associate, or equivalent, to the minimum necessary as required by HIPAAlaw. Review complaints from a victim, ethics and/or compliance hotline to determine if there were complaints about an inappropriate or unauthorized disclosure of PHI due to a failure to limit the disclosure to the minimum necessary, either to, or from, another covered entity or, business associate, or equivalent. Interview human resources personnel to determine if workforce members have been disciplined for an inappropriate or unauthorized disclosure of PHI due to a failure to limit the amount disclosed to the minimum necessary. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, the metric could indicate the number of excessive disclosures contrary to the requirements specified in HIPAAapplicable law, as a percentage of all disclosures. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity, or equivalent, makes reasonable efforts to limit requests for PHI to, or from, another covered entity or, business associate, or equivalent, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Question Requirement: 19423.13jHIPAAOrganizational.5 / 1720.0

Change Count: 3

Field	Content
RequirementStatement	A data use agreement with a limited data set recipient is made before allowing the use or disclosure of a limited data set, which meets the requirements for a limited data set, as specified by HIPAA § 164.514(e).
IllustrativeProcedureImplemented	For example, inquire of management as to whether data use agreements are in place between the covered entity (or equivalent) and its limited data set recipients. Obtain and review an example data use agreement to determine if the agreements comply with HIPAA § 164.514(e)applicable law. Obtain a list of limited data set recipients and verify that a representative sample of recipients have a data use agreement in place. If possible, verify the data use agreement was signed prior to the first disclosure of the limited data set to the recipient. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation as the result of an inappropriate or unauthorized use or disclosure of PHI as the result of releasing a limited data set without a data use agreement in place. Review complaints from a victim, ethics and/or compliance hotline to determine if there were complaints about an inappropriate or unauthorized use or disclosure of PHI as the result of releasing a limited data set without a data use agreement in place. Interview human resources personnel to determine if workforce members have been disciplined for an inappropriate or unauthorized use or disclosure of PHI as the result of releasing a limited data set without a data use agreement in place. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, the measure(s) could indicate the number of limited data set recipients without a valid data use agreement, as specified in HIPAA § 164.514(e), as a percentage of all limited data set recipients for a specific time period. A companion metric could be the number of limited data sets released in a specified time period that did not meet the requirements for a limited data set as specified by HIPAA § 164.514(e). Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity (or equivalent) enters into a data use agreement with a recipient before allowing the use or disclosure of a limited data set and ensures the data provided meets the requirements for a limited data set.

Question Requirement: 19422.13jHIPAAOrganizational.4 / 1716.0

Change Count: 1

Field	Content
RequirementStatement	When de-identifying PHI, the organization, acting as a covered entity, requires the removal of all eighteen (18) data elements as required by the HIPAA Administrative Simplification''s Privacy Rule, and has no knowledge the resulting data set could be re-identified, or an appropriate person applies generally accepting scientific principles and methods for rendering information not individually identifiable and determines the risk of re-identification is appropriately small.

Question Requirement: 19382.13fHIPAAOrganizational.7 / 1653.0

Change Count: 1

Field	Content
RequirementStatement	If access is denied, the covered entity provides timely (30 days plus no more than a 30 day extension), written denial to an individual''s request for access in plain language, the basis for denial, a statement of the individual''s rights for review of the denial, a description of procedures for complaints to the entity and the Secretary of Health and Human Services, as specified in HIPAA § 164.524(d)(2).

Question Requirement: 19392.13fHIPAAOrganizational.17 / 1765.0

Change Count: 1

Field	Content
RequirementStatement	The covered entity only conditions requests for confidential communications on how payment, if any, will be handled and the specification of an alternative address or other method of contact; however, in no case may the organization require an explanation as to the basis of the individual''s request.

Question Requirement: 19376.13fHIPAAOrganizational.1 / 1762.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides individuals the right of access to review and obtain a copy of their PII or records about an individual for as long as the records are maintained, and provides such access in a timely manner (30 days with no more than one 30 day extension) for no more than a reasonable, cost-based fee, or, if the organization does not maintain the PII but knows where it' is located, the organization informs the individual where to direct the request, as required by law, regulation, policy, contract, or similar obligation.

Question Requirement: 19388.13fHIPAAOrganizational.13 / 1833.0

Change Count: 1

Field	Content
RequirementStatement	The covered entity corrects an individual''s PHI if informed by another covered entity of an amendment.

Question Requirement: 19387.13fHIPAAOrganizational.12 / 1669.0

Change Count: 3

Field	Content
RequirementStatement	If a requested amendment is denied, in whole or in part, the organization, acting as a covered entity (or equivalent), provides the individual with a written denial, permits the individual to submit a statement of disagreement, prepares a rebuttal if the individual submits a statement of disagreement and maintains denials, disagreements, and rebuttals as organizational records, and provides relevant information regarding any disagreements in future disclosures of the individual''s PHI, as required in HIPAA § 164.526(d).
IllustrativeProcedureImplemented	For example, inquire of management if the entity has documented requirements for denying an individual's request for an amendment. Obtain and inspect a list of requirements to determine if the entity is in compliance with HIPAA § 164.526(d)applicable laws. Interview key personnel responsible for managing organization records to determine if written or ad hoc procedures for processing the denial of an individual's request for an amendment of the individual's PHI or a record about the individual in a designated record set are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the requirements for denying an amendment as required by HIPAA § 164.526(d)applicable laws. Review complaints from an ethics and/or compliance hotline to determine if there are complaints about a failure to process a denial for a requested amendment as required. Interview human resources personnel to determine if workforce members have been disciplined for a failure to process a denial for an individual's request for an amendment as required. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, measures indicate the number of incidents in which the requirements for processing a denial to a requested amendment were not met as a percentage of all denied amendments. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, if a requested amendment is denied in whole or in part, the covered entity (or equivalent) must provide the individual with timely (within 30 days plus 30 days extension) written denial; permit the individual to submit a statement of disagreement; prepare a written rebuttal if the individual submits a statement of disagreement; maintains denials, disagreements and rebuttals as organizational records; and provides relevant information regarding any disagreements in future disclosures of the individual's PHI.

Question Requirement: 19385.13fHIPAAOrganizational.10 / 1832.0

Change Count: 1

Field	Content
RequirementStatement	The covered entity acts on an individual''s request for amendment within 60 days of the request, with no more than one 30 day extension.

Question Requirement: 19384.13fHIPAAOrganizational.9 / 1667.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures an individual''s request for amendment is denied only if the covered entity determines the PHI or record was not created by the covered entity (unless the originator no longer exists), is not part of the designated record set, is not available for inspection, or is otherwise accurate and complete, as stipulated in HIPAA § 164.526(a)(2).

Question Requirement: 19380.13fHIPAAOrganizational.5 / 1763.0

Change Count: 2

Field	Content
RequirementStatement	The covered entity, or equivalent, denies an individual access to their PHI without providing an opportunity to review if it is denied for an allowable reason.

IllustrativeProcedureImplemented	For example, interview a representative sample of personnel responsible for denying access and determine if access is denied in alignment with HIPAAapplicable laws. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation as the result of denying accessing without appropriate cause. Review complaints from a victim, ethics and/or compliance hotline to determine if there were complaints about access denial. Interview human resources personnel to determine if workforce members have been disciplined for denying access contrary to policies and procedures. Examine related legal and HR documentation, if available.

Question Requirement: 19377.13fHIPAAOrganizational.2 / 1830.0

Change Count: 2

Field	Content
RequirementStatement	The covered entity, or equivalent, provides the individual access to the PHI in the designated record set in a written or electronic form and the format requested by the individual or otherwise agreed to by the covered entity, or equivalent, and the individual. Summaries of the PHI requested are only provided in lieu of the designated record set if the individual agrees in advance to the summary and any fees imposed for providing such summary.
IllustrativeProcedureImplemented	For example, obtain and review the notice of privacy practices to determine if the entity provides an individual a right to access his/her PHI in the designated record set in written or electronic form and format requested by the individual or otherwise agreed to by the covered entity, or equivalent, and the individual. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the requirements. Review complaints from an ethics and/or compliance hotline to determine if there are complaints about providing an individual access to their PHI in the form/format agreed upon. Interview human resources personnel to determine if workforce members have been disciplined for a failure comply with the requirements. Examine related legal and HR documentation, if available.

Question Requirement: 19359.13eHIPAAOrganizational.9 / 1617.0

Change Count: 1

Field	Content
RequirementStatement	If an individual is present or has the authority, the covered entity: obtains the individual''s consent or authorization; provides the individual an opportunity to object; reasonably infers from the circumstances that the individual does not object to disclosure of PHI, as specified in HIPAA § 164.510(b)(2).

Question Requirement: 19358.13eHIPAAOrganizational.8 / 1614.0

Change Count: 3

Field	Content
RequirementStatement	The organization, acting as covered entity, or equivalent: informs individuals of the PHI it may include in a directory; informs individuals to whom it may disclose such information; and provides the individual an opportunity to restrict or prohibit some or all of the disclosures, as specified in HIPAA § 164.510(a)(2).
IllustrativeProcedureImplemented	For example, inquire of management as to whether the entity maintains a directory of individuals in its facility. Obtain and review its notice of privacy practices and evaluate the content in relation to the specified criteria for evidence of the opportunity to restrict or prohibit some or all of the disclosures. Review documentation provided to an individual, if any, and ensure the covered entity, or equivalent, informs individuals of the PHI it may include in a directory, and to whom it may disclose such information, and provide the individual an opportunity to restrict or prohibit some or all of the disclosures, as required by HIPAA § 164.510(a)(2). Inquire of management as to whether objections by individuals to restrict or prohibit some or all of the uses or disclosures are obtained and maintained. Obtain and compare documented objections to the disclosure of PHI in a facility directory with historical records of the directory, if available. Determine if the facility directory is updated on a periodic basis. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for inappropriately disclosing PHI in a facility directory. Review complaints from an ethics and/or compliance hotline to determine if complaints about inappropriate disclosures in a facility directory have been made. Interview human resources personnel to determine if workforce members have been disciplined for inappropriate disclosure of PHI in a facility directory. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI to a person when the individual is present as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of the reason, if disclosures contrary to the requirements outlined in HIPAA § 164.510(b)(2) can be discerned. Note a measure could include regular or ad hoc reports or audits of disclosures if they considered the policy requirements. If a metric or measure adequately evaluates the requirements for disclosures when an individual is present as described in HIPAA § 164.510(b)(2), determine if the measure is tracked over time and if performance goals have been established. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that if an individual is present or has the authority, the covered entity, or equivalent, obtains the individual's consent or authorization, provides the individual an opportunity to object, or reasonably infers from the circumstances that the individual does not object to disclosure of PHI.

Question Requirement: 19357.13eHIPAAOrganizational.7 / 1613.0

Change Count: 3

Field	Content
RequirementStatement	The covered entity, or equivalent, addresses requirements around an individual''s objections regarding the use of their PHI in the directory. If the individual does not object, the covered entity, or equivalent, limits the PHI contained in a directory of individuals at its facility to the individual's name, location, general condition, and religious affiliation. The covered entity, or equivalent, only uses or discloses such information for directory purposes to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name, as specified in HIPAA § 164.510(a)(1).
IllustrativeProcedureImplemented	For example, inquire of management as to whether the entity maintains a directory of individuals in its facility. Obtain and review a directory of individuals in the entity's facility and evaluate the content in relation to the specified criteria to determine if the disclosure and purpose of such information is appropriate, as required by HIPAA § 164.510(a)(1). Obtain and compare documented objections to the disclosure of PHI in a facility directory with historical records of the directory, if available. Determine if the facility directory is updated on a periodic basis. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for inappropriately disclosing PHI in a facility directory. Review complaints from an ethics and/or compliance hotline to determine if complaints about inappropriate disclosures in a facility directory have been made. Interview human resources personnel to determine if workforce members have been disciplined for inappropriate disclosure of PHI in a facility directory. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI in a facility directory as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of the reason, if unauthorized disclosures due to the inappropriate disclosure in a facility directory can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, if an individual does not object, the covered entity, or equivalent, limits the PHI contained in a directory of individuals at its facility to the individual's name, location, general condition, and religious affiliation and only uses or discloses such information for directory purposes to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name.

Question Requirement: 19355.13eHIPAAOrganizational.5 / 1583.0

Change Count: 3

Field	Content
RequirementStatement	The organization, acting as a covered entity, willor equivalent, ensures individuals who exercise any of their lawful rights, including the filing of a complaint, are not subject to intimidation, threats, discrimination, or any other retaliatory action, as required in HIPAA § 164.530(g).
IllustrativeProcedureImplemented	For example, inquire of management if the organization prevents intimidating or retaliatory actions against any individual for the exercise by the individual of any right established, or for participation in any process provided, for filing complaints against the covered entityorganization. Interview key personnel responsible for patient rights management, e.g., an ombudsman, and key personnel responsible for the entity's complaint process, and verify the entity follows written or ad hoc procedures consistently and prevents intimidating or retaliatory actions as required by HIPAA § 164.530(g). Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for intimidating or retaliatory actions against an individual contrary to HIPAA § 164.530(g)applicable law. Review complaints from an ethics and/or compliance hotline to determine if there are complaints about intimidating or retaliatory actions against an individual. Interview human resources personnel to determine if workforce members have been disciplined for intimidating or retaliatory actions. Examine related legal and HR documentation, if available.

IllustrativeProcedureMeasured	For example, measures indicate the number of incidents in which an individual was the subject of intimidation or a retaliatory action due to filing a complaint as a percentage of all complaints received. Non-compliance with the policy requirements could be part of a broader metric that considers all deviations with respect to individual (e.g., patient) rights regardless of type of failure if failures to meet the requirement for prohibiting intimidating or retaliatory actions against an individual, as specified by HIPAA § 164.530(g), can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entityorganization ensures that individuals who exercise any of their lawful rights, including the filing of a complaint, are not subject to intimidation, threats, discrimination, or any other retaliatory action.

Question Requirement: 19335.13dHIPAAOrganizational.4 / 1602.0

Change Count: 1

Field	Content
RequirementStatement	If an individual''s authorization is given in the context of a written declaration which also concerns other matters, the organization ensures requests for authorization are presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Question Requirement: 19327.13cHIPAAOrganizational.4 / 1755.0

Change Count: 1

Field	Content
RequirementStatement	Requirements have been defined for temporarily suspending an individual''s right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the covered entity with a statement that such an accounting to the individual would be reasonably likely to impede the agency''s activities and specifying the time for which such a suspension is required.

Question Requirement: 19326.13cHIPAAOrganizational.3 / 1663.0

Change Count: 1

Field	Content
RequirementStatement	An individual''s request for an accounting is: acted upon no later than 60 days after receipt of the request (with a one-time 30-day extension with proper notice to the requester); free of charge for the first request within any 12-month period; and if informed in advance, provided for a reasonable cost-based fee for subsequent requests within the period, as specified by HIPAA § 164.528(c)(1).

Question Requirement: 19185.09zCMSOrganizational.12 / 1108.0

Change Count: 1

Field	Content
RequirementStatement	Websites are operated within the restrictions addressed in: OMB directives M-10-22 ""Guidance for Online Use of Web Measurement and Customization Technologies""; M-10-23 ""Guidance for Agency Use of Third-Party websites and Applications""; and applicable CMS and DHHS directives and instruction. The organization monitors the CMS and DHHS security programs to determine if there are any modified directives and instruction.

Question Requirement: 19.13lCMSOrganizational.1 / 2674.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19189.10c2System.8 / 1272.0

Change Count: 1

Field	Content
RequirementStatement	When doing system development (e.g., applications, databases), the organization ensures that the application''s design and implementation minimizes the risks of processing failures leading to a loss of integrity.

Question Requirement: 19153.13k1Organizational.4 / 0377.0

Change Count: 1

Field	Content
RequirementStatement	In cases where an employee, contractor or third-party user purchases the organization''s equipment or uses their own personal equipment, all relevant information is transferred to the organization and securely erased from the equipment; and, when they have knowledge important to ongoing operations, that information is documented and transferred to the organization.

Question Requirement: 19508.13p1Organizational.3 / 1862.0

Change Count: 1

Field	Content
RequirementStatement	The data protection officer''s responsibilities include: the development and implementation of privacy policies and procedures; serving as the point of contact for all privacy-related complaints; and providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that will be followed. The data protection officer: will, in the performance of those tasks, have due regard to the risk associated with processing operations, the nature, scope, context and purposes of processing; and may fulfill other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests.

Question Requirement: 19546.13rHIPAAOrganizational.1 / 1739.0

Change Count: 3

Field	Content
RequirementStatement	The organization, acting as a covered entity, or equivalent, confirms each of its business associates, or equivalents, have a valid agreement that addresses the proper management/oversight of the business associate, or equivalent, specifies applicable requirements (e.g., around use, further disclosure, and the implementation of reasonable and appropriate safeguards), and authorize termination of the contract by the covered entity, if the covered entity organization, if the organization determines that the business associate, or equivalent, has violated a material term of the contract.
IllustrativeProcedureImplemented	For example, select a sample of business associates, or equivalents, and confirm that a valid agreement has been executed and that it addresses proper management/oversight and defines applicable requirements.
IllustrativeProcedureMeasured	For example, the measure(s) could indicate the number of business associates, or equivalents, that do not have a valid agreement that addresses proper management/oversight and specifies applicable requirements, as a percent of all business associates, or equivalents. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity , or equivalent, ensures each of its business associates, or equivalents, have a valid agreement that addresses proper management/oversight and specifies applicable requirements.

Question Requirement: 1913.07eTexasOrganizational.1 / 0681.0

Change Count: 1

Field	Content
RequirementStatement	The freestanding emergency medical facilities: require implementation of the Health and Human Services Executive Commissioner''s minimum standards for the contents of medical records; require implementation of the Health and Human Services Executive Commissioner''s minimum standards for the maintenance of medical records; require implementation of the Health and Human Services Executive Commissioner''s minimum standards for the release of medical records; have designated an individual to be in charge of the creation, maintenance, and disposal of medical records per 25 TAC § 131.53; and have standards including the confidentiality, security, and safe storage of medical records throughout the records lifecycle.

Question Requirement: 19480.13kTexasOrganizational.23 / 1690.0

Change Count: 1

Field	Content
RequirementStatement	Family planning information is confidential and may not be disclosed except as provided by 25 Tex. Admin. Code § 56.11: providers ensure client confidentiality and provide safeguards for clients against the invasion of personal privacy; all personnel (both paid and volunteer) must be informed during orientation of the importance of keeping information about a client confidential; clients'' records must be monitored to ensure access is limited to appropriate staff and to department and/or commission staff or their authorized representatives; the client's' preference of methods of follow-up contact are documented in the client's' record; and each client receives verbal assurance of confidentiality and an explanation of what confidentiality means.

Question Requirement: 19479.13kTexasOrganizational.22 / 1607.0

Change Count: 1

Field	Content
RequirementStatement	Requests for information from the Texas immunization registry are only made upon the written consent of the individual or, if a child, the parent, managing conservator or legal guardian, or except as provided by lawthe Tex. Occupations Code § 159, or the Tex. Ins. Code § 28B.04.

Question Requirement: 19478.13kTexasOrganizational.21 / 1606.0

Change Count: 1

Field	Content
RequirementStatement	Individually identifiable immunization information is confidential and may not be disclosed without the written or electronic consent of the individual or the individual''s legally authorized representative per Tex. Occupations Code § 159.005.

Question Requirement: 19468.13kTexasOrganizational.11 / 1710.0

Change Count: 1

Field	Content
RequirementStatement	Client Medicaid information is confidential and not disclosed without effective consent by the client or on behalf of the client, except for purposes directly connected to the administration of the Medicaid program as described in TX Human Resources Code §§ 21.003 and 21.012 and TX Government Code § 552.101.

Question Requirement: 19467.13kTexasOrganizational.10 / 1709.0

Change Count: 1

Field	Content
RequirementStatement	Records associated with a state investigation of alleged abuse or neglect by a chemical dependency counselor or treatment center are treated as confidential and mayare not be released (disclosed) except that the release may be made on court order, on request and consent of the person under investigation or that person"s authorized attorney. Unless prohibited or limited by federal or other state law, Texas Alcohol and Drug Abuse licensing and investigatory records that identify a client may be made available to a state or federal agency or law enforcement authority on request and for official purposes.

Question Requirement: 19483.13kTexasOrganizational.26 / 1648.0

Change Count: 1

Field	Content
RequirementStatement	Policies and/or standards related to the lawful transfer of reports, records, and information specifically address the Texas Cancer Registry. Ensure that the policy specifically states that cancer data may be provided to the Texas Cancer Registry without patient authorization or consent according to 25 TAC § 91.3(e).

Question Requirement: 19458.13kTexasOrganizational.1 / 1700.0

Change Count: 1

Field	Content
RequirementStatement	The policy specifically identifies the requirement to limit disclosure of such reports, records and information. Medical or epidemiological information may be released, in general: for statistical purposes in a manner that prevents identification of individuals, healthcare facilities, clinical laboratories, or healthcare practitioners; with the consent of each person identified in the information; or, to promote cancer research, including release of information to other cancer registries and appropriate state and federal agencies, under rules adopted by the board to ensure confidentiality as required by state and federal laws. The policy specifically states that cancer data provided to the Texas Cancer Registry may not be subject to subpoena consistent with the Registry''s requirements specified in THSC §82.009.

Question Requirement: 19485.13kTexasOrganizational.28 / 1688.0

Change Count: 1

Field	Content
RequirementStatement	Laboratories maintain the confidentiality and accuracy of patient information during all stages of the testing process that are under the laboratory''s control and test results are released only to authorized persons. If applicable, test results are released to the individual responsible for using the test results and the laboratory that initially requested the test. Laboratories have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific information is accurately and reliably transmitted from the point of data entry (whether interfaced or entered manually) to the final reports destination, in a timely manner, as determined by the laboratory''s stated policy requirements.

Question Requirement: 19484.13kTexasOrganizational.27 / 1687.0

Change Count: 1

Field	Content
RequirementStatement	No part of the medical record received from the Social Security Administration is withheld from the individual or, in the case where the medical record pertains to a minor child, from the parent or guardian pursuant to 42 U.S.C. §1306, 20 CFR Part 401.55(c)(2), as referenced by 20 CFR Part 401.100(d). Specifically, the minor patient''s representative (per 20 CFR Part 401.55(c)(2)(ii)) must review the record, discuss its contents with the parent or legal guardian, then release the entire record to the parent or legal guardian. The representative does not have the discretion to withhold any part of the minor''s record.

Question Requirement: 19345.13dTexasOrganizational.2 / 1610.0

Change Count: 1

Field	Content
RequirementStatement	A resident patient may approve or refuse the release of personal and clinical records to any individual outside the facility except as provided in 40 TAC §19.407(3), which states the resident''s right to refuse release of personal and clinical records does not apply when: the resident is transferred to another healthcare institution; record release is required by law; or during surveys.

Question Requirement: 19309.13aTexasOrganizational.7 / 1597.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal statement of patient rights ensure the rights of the patient, within the limits of federal and state law, to personal privacy and confidentiality of personal information and clinical records, per 25 TAC Chapter 404, Subchapter E, referenced by 25 TAC § 134.21(b)(1)(A).

Question Requirement: 19305.13aTexasOrganizational.3 / 1593.0

Change Count: 1

Field	Content
RequirementStatement	The intermediate care facility''s formal statements of patient rights ensures the rights of the patient, within the limits of federal and state law, to personal privacy and confidentiality of personal information and clinical records.

Question Requirement: 19303.13aTexasOrganizational.1 / 1591.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal statement of patient rights ensures the rights of the patient, within the limits of federal and state law, to personal privacy and confidentiality of personal information and clinical records.

Question Requirement: 19133.05eHIEOrganizational.12 / 0481.0

Change Count: 1

Field	Content
RequirementStatement	As part of the agreement with connecting organizations, the HIE specifies which organization owns the data, and any restrictions as part of that ownership such as retention, integrity, and accuracy of data as part of its agreement with connecting organizations. Further, if the HIE is the owner of the data, all federal and state requirements associated with the patients'' information are met.

Question Requirement: 19246.06dDEIDOrganizational.1 / 0576.0

Change Count: 1

Field	Content
RequirementStatement	Encryption has been implemented for covered information in transit, whether internal or external, to the organization''s network. If encryption is not used for data in transit the organization has documented its rationale.

Question Requirement: 18.08jNYDOHOrganizational.2 / 2711.0

Change Count: 0

Field	Content
New Question Requirement	18.08jNYDOHOrganizational.2 / 2711.0

Question Requirement: 1887.08hNIST80053Organizational.1 / 0763.0

Change Count: 1

Field	Content
RequirementStatement	The organization has a suitable electrical supply that conforms to the equipment manufacturer''s specifications.

Question Requirement: 1898.08hPRVOrganizational.123 / 0774.0

Change Count: 1

Field	Content
RequirementStatement	Backup generators, multiple power sources and/or separate substations are implemented based on the level of the organization: Level 1 Providers: A back-up generator is considered if processing is required to continue in case of a prolonged power failure; Level 1 Providers: An adequate supply of fuel is available to ensure that the generator, if used, can perform for a prolonged period; Level 2 Providers: A back-up generator is implemented; Level 2 Providers: An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period; Level 2 Providers: Generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer''s recommendations; Level 3 Providers: Multiple power sources or a separate power substation be used; Level 3 Providers: Telecommunications equipment are connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services; Level 3 Providers: The organization develops telecommunications service agreements that contain priority of service (Telecommunications Service Priority) provisions.

Question Requirement: 18119.08jCMSOrganizational.7 / 0801.0

Change Count: 2

Field	Content
RequirementStatement	The organization obtains maintenance support and/or spare parts for CMS critical systems and applications, (including major applications [(MA]) and general support systems [(GSS]) and their components), within 24 hours of failure.
IllustrativeProcedureMeasured	For example, measures indicate the number of maintenance support agreements and/or spare parts for CMS critical systems required to sufficiently meet the organization's recovery time of 24 hours. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization obtains maintenance support and/or spare parts for CMS critical systems and applications, (including Major Applications [(MA]) and General Support Systems [(GSS]) and their components), within 24 hours of failure.

Question Requirement: 18108.08j1Organizational.1 / 0784.0

Change Count: 1

Field	Content
RequirementStatement	The organization formally addresses purpose, scope, roles associated with, responsibilities associated with, management'' s commitment to, coordination among organizational entities associated with, and compliance with the organization''s equipment maintenance program. Formal, documented procedures exist to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Question Requirement: 1888.08h1Organizational.456 / 0764.0

Change Count: 1

Field	Content
RequirementStatement	An uninterruptable power supply (UPS) to support orderly close down is required for equipment supporting critical business operations. Power contingency plans cover the action to be taken on failure of the UPS. The organization ensures UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer''s recommendations.

Question Requirement: 18122.08k1Organizational.1 / 0806.0

Change Count: 1

Field	Content
RequirementStatement	Regardless of ownership, the use of any information processing equipment outside the organization''s premises, including equipment used by remote workers, even where such use is permanent (e.g., a core feature of the employee''s role), is authorized by management.

Question Requirement: 18.08jFedRAMPOrganizational.2 / 2376.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 18.08bFTIOrganizational.7 / 2682.0

Change Count: 1

Field	Content
RequirementStatement	The organization instructs all personnel to never maintain written combinatations to locked areas.

Question Requirement: 18.08bFTIOrganizational.6 / 2665.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1815.08d2Organizational.123 / 0735.0

Change Count: 1

Field	Content
RequirementStatement	Fire prevention training is included in the regular training programs provided to the organization personnel. Appropriate fire suppression systems (e.g., sprinklers, gas) are implemented throughout the building, and within secure areas containing information processing devices. For facilities not staffed continuously, these suppression systems are automated. The building''s HVAC system is configured to automatically shut down upon fire detection.

Question Requirement: 1860.08c2Organizational.4567 / 0730.0

Change Count: 1

Field	Content
RequirementStatement	Video cameras or other access control mechanisms are securely implemented to monitor individual physical access to sensitive areas. Devices such as video cameras and other access control mechanisms are protected from tampering or disabling. Output/results from video devices and other access control mechanisms are reviewed regularly and correlated with other entries and access control information (e.g., audit trails, sign in sheets, authorization levels, maintenance logs). The information from cameras or other access control mechanisms are stored for at least six months in accordance with the organization''s retention policy.

Question Requirement: 1804.08b2Organizational.12 / 0703.0

Change Count: 1

Field	Content
RequirementStatement	A visitor log includes: the date of entry; time of entry; date of departure; time of departure; the visitor''s name; the organization represented; and the employee authorizing physical access. The log is reviewed no less than monthly and upon occurrence of organization-defined security events. The log is retained for at least two years in accordance with the organization''s retention policy.

Question Requirement: 1834.08a2Organizational.7 / 0684.0

Change Count: 1

Field	Content
RequirementStatement	Any rRepairs or modifications to the physical components of a facility which are related to security (for examplee.g., hardware, walls, doors, and locks) isare documented, and retained in accordance with the organization''s retention policy.

Question Requirement: 1819.08j2Organizational.4 / 0785.0

Change Count: 1

Field	Content
RequirementStatement	Equipment is maintained in accordance with the supplier''s recommended service intervals and specifications, insurance policies, and the organization''s maintenance program. The organization ensures only authorized maintenance personnel carry out repairs and service the equipment. Appropriate controls are implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization.

Question Requirement: 1825.08l2Organizational.1 / 0811.0

Change Count: 1

Field	Content
RequirementStatement	The organization: ensures disk wiping or degaussing is used to securely remove electronic information; ensures shredding, disintegration, grinding surfaces, incineration, pulverization, or melting are used to destroy electronic and hard copy media; ensures devices containing covered and/or confidential information are physically destroyed or the information is destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function; renders information unusable, unreadable, or indecipherable on digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; renders information unusable, unreadable, or indecipherable on non-digital system media prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; destroys media containing covered and/or confidential information that cannot be sanitized.

Question Requirement: 18123.08k2Organizational.1 / 0807.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that equipment and media taken off the premises are not to be left unattended in public places. Portable computers are carried as hand luggage and disguised where possible when travelling. Manufacturers'' instructions for protecting equipment are observed at all times (e.g., protection against exposure to strong electromagnetic fields).

Question Requirement: 19130.05eNIST80053Organizational.1 / 0478.0

Change Count: 1

Field	Content
RequirementStatement	Confidentiality or non-disclosure agreements: address the requirement to protect confidential information using legally enforceable terms; include a definition of the information to be protected (e.g., confidential information); include expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely; include required actions when an agreement is terminated; include responsibilities and actions of signatories to avoid unauthorized information disclosure (such as ''need to know''); include disclosures required to be limited to the limited data set or the minimum necessary to accomplish the intended purpose of such use, disclosure, or request; include ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; include the permitted use of confidential information, and rights of the signatory to use information; include individuals'' rights to obtain a copy of the individual''s information in an electronic format; include individuals'' rights to have the individual''s information transmitted to another entity or person designated by the individual, provided the request is clear, conspicuous, and specific; include the right to audit and monitor activities that involve confidential information; include the process for notification and reporting of unauthorized disclosure or confidential information breaches; include terms for information to be returned or destroyed at agreement cessation; and include expected actions to be taken (i.e. penalties that are possible) in case of a breach of this agreement. The confidentiality agreements are applicable to all personnel accessing covered information.

Question Requirement: 19.06dNIST80053Organizational.4 / 2305.0

Change Count: 2

Field	Content
RequirementStatement	The organization fragments organization-defined information (i.e., covered information) and distributes the fragmented information across the organization-defined systems or system components.
IllustrativeProcedureImplemented	For example, examine evidence to confirm that the organization fragments defined information (i.e., covered information). Confirm whether the configuration of the distribution of data fulfills applicable security and privacy requirements. Examine the results of the review and confirm that the review assessed the configuration(s) employed, and it satisfied all applicable organization-defined security requirements.

Question Requirement: 19.13cCMSOrganizational.1 / 2516.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that the development of the strategic organizational privacy plan be done in consultation with the organization''s CIO and CISO, and establishes and institutionalizes contact for its privacy professionals with selected groups and associations within the privacy community.

Question Requirement: 19.13oCMSOrganizational.1 / 2672.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19312.13aGroupPlansOrganizational.1 / 1577.0

Change Count: 1

Field	Content
RequirementStatement	The health insurance issuer, or HMO, provides an individual (other than an inmate enrolled in a group health plan), a notice of privacy practices for the portion of the group health plan the individual receives benefits. The health notice is: provided to the named insured and one or more dependents; provided to new enrollees at the time of enrollment; and again within 60 days of any material revision to the notice; provided again within 60 days of any material revision to the notice.

Question Requirement: 19.09zFedRAMPOrganizational.1 / 2373.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 19252.10cFedRAMPSystem.1 / 1283.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of information systems have not been configured to provide notification of failed security verification tests, as a percentage of applicable systems. A further measure could indicate the number of instances where a failed security verification occurs and the systems does not shut down, restart or perform another defined alternative action, as a percentage of such instances. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the information system (i) verifies the correct operation of system security functions upon system startup and restart, upon command by a user with appropriate privilege, and periodically on a monthly basis; (ii) provides notification of failed automated security tests, and notifies system administration when anomalies are discovered; and (iii)) shuts down, restarts or performs some other defined, alternative action (defined in the applicable security plan) when anomalies are discovered.

Question Requirement: 17291.10aNIST80053Organizational.1 / 2264.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, metrics could indicate the date the organization last performed a review of its development process, and indicate whether or not it was at least annually. Examine the results of the reviewReviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the review assessed organization reviews the development process, standards, tools, and tool options/configurations to determine if the process, standards, tools, and tool options/configurations selected and employed, and that it satisfiedy all applicable organization-defined security requirements.

Question Requirement: 1730.03cCMSOrganizational.23 / 0421.0

Change Count: 1

Field	Content
RequirementStatement	The organization: develops and submits a Plan of Action and Milestones (POA&M) in accordance with federal reporting requirements by the OMB for the information system within 30 days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization''s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Question Requirement: 1770.09i2System.4 / 0863.1

Change Count: 5

Field	Content
BaselineUniqueId	1770.09i2System.14
CrossVersionId	0863.01
RequirementStatement	The organization requires the developer of the information system, system component, or information system service to: create and implement a security and privacy assessment plan; perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage; produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation; implement a verifiable flaw remediation process; and correct flaws identified during security testing/evaluation.
IllustrativeProcedureImplemented	For example, select a sample of development changes and examine the development record and confirm that the following was performed by the developer of the information system, system component, or information system service: (i) a security and privacy assessment plan was created and implemented; (ii) unit, integration, system and regression testing/evaluation was performed; (iii) evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation was documented; (iv) a verifiable flaw remediation process was implemented; and (v) any flaws identified during security testing/evaluation was corrected.
IllustrativeProcedureMeasured	For example, measures indicate the number of failed/flawed development changes that were implemented that did not undergo the required security and privacy assessment or testing, as a percentage of all development changes. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization requires the developer of the information system, system component, or information system service to (i) create and implement a security and privacy assessment plan; (ii) perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage; (iii) produce evidence of the execution of the security and privacy assessment plan and the results of the security testing/evaluation; (iv) implement a verifiable flaw remediation process; and (v) correct flaws identified during security testing/evaluation.

Question Requirement: 17112.10aHIXOrganizational.1 / 1261.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate which Statements of Work / contracts contain personally identifiable information (PII), indicate the appropriate system owner, and indicate if signoff was completed by the system owner. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has contracts and Statements of Work that contain language consistent with 45 CFR 155.260(b), require adherence to the security and privacy policies and standards set by the organization, and define security roles and responsibilities.

Question Requirement: 17119.05gHIXOrganizational.1 / 0494.0

Change Count: 2

Field	Content
RequirementStatement	The organization: disseminates security alerts, advisories and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; and implements security directives in accordance with established time frames, or notifies the business owner of the degree of noncompliance.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of security directives not sent to appropriate personnel in the organization. A further measure could indicate the number of security directives not implemented in accordance with established time frames, as a percentage of security directives received. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization disseminates security alerts, advisories and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities, and implements security directives in accordance with established time frames, or notifies the business owner of the degree of noncompliance.

Question Requirement: 1701.03a1Organizational.12345678 / 0383.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s risk management program includes: objectives of the risk management process; management''s clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization''s strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management''s stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.

Question Requirement: 17.03cFTIOrganizational.2 / 2649.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1740.05d3Organizational.12 / 0474.0

Change Count: 1

Field	Content
RequirementStatement	All facilities undergo a site security survey, prior to lease or purchase, by the organization''s security department or a trusted third-party. The organization resolves all security shortcomings before any covered information is processed at that location. All sites that process covered information are reviewed whenever the site undergoes a significant change in mission or makes substantive physical changes in its facilities or workforce and no less than annually.

Question Requirement: 1711.03a3Organizational.4 / 0387.0

Change Count: 1

Field	Content
RequirementStatement	The organization has identified that ‘‘Personal Identifying Information' (PII) [also ’ or ‘Personally Identifiable Information]’ (PII) means information that alone, or in conjunction with other information, identifies an individual. The organization’’s definition of PII includes: name, social security number, date of birth, or government-issued identification number; mother’’s maiden name; unique biometric data, including the individuals fingerprint, voice print, and retina or iris image; electronic identification number, address, or routing code; and telecommunication access device.

Question Requirement: 1712.03a3Organizational.5 / 0388.0

Change Count: 1

Field	Content
RequirementStatement	The organization’’s identity theft program includes protections for financial identity theft and medical identity theft, as applicable to the organization.

Question Requirement: 17103.10aCMSOrganizational.2 / 1250.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could include the number of contracts where third-party organizations perform development activities or require access to CMS information, indicate execution date of the agreement, and indicate the status of any amendment or renewal required of such contracts to become compliant with standard CMS information security and privacy contract language. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has up-to-date contracts that include the standard CMS information security and privacy contract language.

Question Requirement: 17104.10aCMSOrganizational.3 / 1251.0

Change Count: 1

Field	Content
RequirementStatement	The organization requires the developer of the information system, system component, or information system service to follow a documented development process that: Eexplicitly addresses security requirements; Iidentifies the standards and tools used in the development process; Ddocuments the specific tool options and tool configurations used in the development process; Dand documents, manages, and ensures the integrity of changes to the process and/or tools used in development.

Question Requirement: 17115.03aCSPOrganizational.1 / 0389.0

Change Count: 1

Field	Content
RequirementStatement	Cloud service providers review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner''s cloud supply chain.

Question Requirement: 17108.10aFTIOrganizational.2 / 1257.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the number of systems and services acquired and the date of the related acquisition contract. Measures could indicate the status of any contract amendment or renewal required to achieve current requirements, if noncompliant. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has acquisition contracts in place for all systems and services acquired and that those contracts include current requirements as stipulated in organization policy.

Question Requirement: 1733.03d2Organizational.3 / 0426.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence that the organization re-evaluated its risk assessment and that confirm that it was performed atwithin the least annuallyyear. Further, identify if any significant changes that occurred in the environment and confirm that a subsequent risk assessment was performed.

Question Requirement: 1708.03c2Organizational.12 / 0419.0

Change Count: 1

Field	Content
RequirementStatement	The organization develops a formal risk treatment plan that includes: risks and nonconformities; priorities for managing information security risks; performing a cost/benefit analysis for identified countermeasures; documenting a risk treatment plan which provides recommended countermeasures to management; documenting and presenting risk treatment summary reports to management; management approves countermeasures documented in the risk treatment plan; mapping decisions taken against the list of HITRUST CSF controls; documenting planned implementations (current and future) in the organization''s security improvement plan; implementing the management approved risk treatment plan; and continually assessing the capability of technology needed to sustain an appropriate level of information security based on the size, complexity, and risk appetite of the organization.

Question Requirement: 1706.03bHIPAAOrganizational.3 / 0395.0

Change Count: 1

Field	Content
RequirementStatement	Risk assessments (analysis) used to determine whether a breach of unsecured Protected Health Information (PHI) as these terms are defined by the Secretary of Health and Human Services is reportable to the Secretary must demonstrate there is a low probability of compromise (lo pro cLoProCo) rather than a significant risk of harm. The methodology, at a minimum, address the following factors: the nature of the PHI involved, including the types of identifiers involved and the likelihood of re-identification; the unauthorized person who used the PHI or to whom the disclosure was made; whether the PHI was actually acquired or viewed; the extent to which the risk to the PHI has been mitigated; and other factors/guidance promulgated by the Secretary.

Question Requirement: 17122.03bFFIECISOrganizational.1 / 0402.0

Change Count: 1

Field	Content
RequirementStatement	The organization implements a risk identification process that produces manageable groupings of information security threats, which include the following: a threat assessment to help focus the risk identification efforts; a method or taxonomy for categorizing threats, sources, and vulnerabilities; a process to determine the institution''s information security risk profile; a validation of the risk identification process through audits, self-assessments, penetration tests, and vulnerability assessments; and a validation though audits, self-assessments, penetration tests, and vulnerability assessments that risk decisions are informed by appropriate identification and analysis of threats and other potential causes of loss.

Question Requirement: 1799.10a3Organizational.34 / 1245.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the date of the last review/update of the information security architecture and the date of the last change to security architecture. Measures could include due dates and activities required for security architecture that was changed without a review or update. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has up-to-date security architecture in the security plan and organizational procurements and acquisitions.

Question Requirement: 17101.10a3Organizational.6 / 1248.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, examine written development policies and procedures and confirm that the policies require the developer of the information system, system component, or information system service to produce specific control design and implementation information (e.g., an acceptable design specification and security architecture). Select a sample of applicablemeasures indicate the number of applicable development changes where developers did not satisfy the requirements as stipulated in the organization requirement statement. Measures also could indicate how such non-compliant requirements were mitigated and whether or not non-compliance was mitigated prior to deveplopyment changes and confirm that an appropriate acceptable design specification and security architecture was formally documented and includes the follow. Reviews, tests, or audits are completed by the organization to measure the effectiveness of developer compliance with providing: (i) a description of the functional properties of the security controls to be employed; and, (ii) design and implementation information for the security controls to be employed that includes: security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.

Question Requirement: 17100.10a3Organizational.5 / 1246.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the number of systems acquired and the date of the related acquisition contract. Measures could indicate the status of any contract amendment or renewal required to achieve current security functional requirements as stipulated by the organization, if noncompliant. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has acquisition contracts in place for all systems acquired and that those contracts include current security functional requirements as stipulated by the organization.

Question Requirement: 16.12bISO23894Organizational.1 / 2805.0

Change Count: 0

Field	Content
New Question Requirement	16.12bISO23894Organizational.1 / 2805.0

Question Requirement: 16905.09hSRSystem.1 / 1957.0

Change Count: 1

Field	Content
RequirementStatement	The organization protects against or limits the effects of the types of denial-of-service attacks defined by NIST SP-800-61 R2, Computer Security Incident Handling Guide, the SANS Organization, the SANS Organization''s Roadmap to Defeating DDoS, and the NIST CVE List National Vulnerability Database.

Question Requirement: 1684.12eCMSOrganizational.1 / 1560.0

Change Count: 1

Field	Content
RequirementStatement	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources, and to evaluate the site''s capabilities to support contingency operations.

Question Requirement: 1652.12cCMSOrganizational.3 / 1524.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures alternate telecommunications Service Level Agreements (SLAs) are in place to permit resumption of service in accordance with the organization''s Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs).

Question Requirement: 1659.12cCMSOrganizational.12 / 1531.0

Change Count: 1

Field	Content
RequirementStatement	Alternate telecommunications service providers that are sufficiently separated from the organization''s primary service provider are identified. Agreements are established to ensure alternate telecommunications service providers are not susceptible to the same hazards as the organization’s primary service provider.

Question Requirement: 16194.09lNYDOHOrganizational.1 / 2166.0

Change Count: 3

Field	Content
RequirementStatement	The organization tests backup information following each backup, at least every six [6] months for Moderate systems, to verify media reliability and information integrity.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization tests backup information following each backup to verify media reliability and information integrity. Examine evidence to confirm that backup information is tested at least every six [6] months for Moderate systems.
IllustrativeProcedureMeasured	For example, measures indicate the number of backups that were not tested for reliability and integrity following each backup as a percentage of all backups. Reviews, tests, or audits are completed by the organization to confirm that the organization tests backup information following each backup to verify media reliability and information integrity at least every six [6] months.

Question Requirement: 1633.12a2Organizational.1 / 1507.0

Change Count: 1

Field	Content
RequirementStatement	The organization brings together the following key information security elements of business continuity management: identifying critical information system assets supporting organizational missions and functions; understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes; understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information assets; implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible; identifying financial, organizational, technical, and environmental resources to address the identified information security requirements; testing and updating, at a minimum, a section of the plans and processes put in place at least annually; ensuring that the management of business continuity is incorporated in the organization''s processes and structure; and assigning responsibility for the business continuity management process at an appropriate level within the organization.

Question Requirement: 1680.12e2Organizational.2 / 1556.0

Change Count: 1

Field	Content
RequirementStatement	Table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions) are used in order to provide assurance that the business continuity plan(s) will operate in real life. Simulations (particularly for training people in their post-incident/crisis management roles) are used in order to provide assurance that the business continuity plan(s) will operate in real life. Testing of the business continuity plans includes: setting system parameters to secure values; reinstalling security critical patches; resetting security configuration settings; making [sure that] system documentation and operating procedures are readily available; reinstalling application system software and configuring it with secure settings; and loading information from the most recent secure back-up(s). Testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site) is used in order to provide assurance that the business continuity plan(s) will operate in real life. Tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment) are used in order to provide assurance that the business continuity plan(s) will operate in real life. Complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions) are used in order to provide assurance that the business continuity plan(s) will operate in real life.

Question Requirement: 1675.12e2Organizational.8 / 1551.0

Change Count: 1

Field	Content
RequirementStatement	Testing is applied on a ''programmatic'' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan.

Question Requirement: 1668.12d2Organizational.5 / 1544.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures emergency procedures, manual "“ fallback"” procedures, and resumption plans are within the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, are usually the responsibility of the service providers.

Question Requirement: 1603.12c2Organizational.8 / 1515.0

Change Count: 1

Field	Content
RequirementStatement	Copies of the business continuity plans are distributed to the Information System Security Officer (or the organization''s functional equivalent), System Owner (or the organization''s functional equivalent), Contingency Plan Coordinator (or the organization''s functional equivalent), System Administrator (or the organization''s functional equivalent), and Database Administrator (or the organization''s functional equivalent).

Question Requirement: 1601.12c2Organizational.7 / 1513.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine the written business continuity plan document(s) and confirm that it includes details on: recovery and restoration of business operations and establishing the availability of information in a time frame specified by the organization; particular attention is given to the assessment of internal and external business dependencies and the contracts in place; documentation of agreed procedures and processes; and testing and updating of at least a section of the plans. The planning process focuses on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered and/or confidential information during an emergency are defined. The services and resources facilitating this are identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. Following an interruption to business operations, full information system restoration without deterioration of the security measures originally planned and implemented can be achieved.

Question Requirement: 1697.12cFedRAMPOrganizational.2 / 1536.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s Service Level Agreements (SLAs) permit telecommunications service providers to resume information system operations for essential missions and business functions with the Recovery Time Objectives (RTOs) documented in a Business Impact Analysis (BIA) when primary telecommunications capabilities are unavailable.

Question Requirement: 1612.09h2System.1 / 0857.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, confirm that the organization has defined capacity and monitoring procedures which include the following: (i) the identification of capacity requirements for each new and ongoing system/service; (ii) the projection of future capacity requirements, taking into account current use, audit record storage requirements, projected trends, and anticipated changes in business requirements; and (iii) the system monitoring and tuning to ensure and improve the availability and effectiveness of current systems. Select a sample of information system resources and confirm that capacity requirements (e.g., disk, system resources) have been defined, considering the business criticality of the concerned system. Confirm that system tuning, and monitoring has been implemented to ensure and where necessary, improve the availability and efficiency of systems. Confirm that detective controls (e.g., capacity monitoring software, alert notification) are put in place to indicate problems. Confirm that projections of future capacity requirements take account of new business and system requirements and current and projected trends in the organizations information processing capabilities.

Question Requirement: 1666.12d1Organizational.1235 / 1542.0

Change Count: 1

Field	Content
RequirementStatement	The organization creates, at a minimum, one business continuity plan. The organization ensures each plan: has an owner; describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security; specifies the escalation plan; specifies the conditions for the escalation plan''s activation; and specifies the individuals responsible for executing each component of the plan.

Question Requirement: 1615.09hFTISystem.1 / 0861.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, confirm that the organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. For the audit record storage system, examine configuration settings to confirm that the storage capacity has been configured to retain audits records for a period of seven years.

Question Requirement: 16.09hFedRAMPSystem.2 / 2446.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 16.09l1Organizational.4 / 2326.0

Change Count: 1

Field	Content
RequirementStatement	The organization maintains offline backups of data and systems.

Question Requirement: 1688.09lCISOrganizational.5 / 0914.0

Change Count: 1

Field	Content
RequirementStatement	The organization automatically backs up each system on a regular basis and ensures that each of the organization''s key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.

Question Requirement: 15.11cNIST80053Organizational.2 / 2784.0

Change Count: 0

Field	Content
New Question Requirement	15.11cNIST80053Organizational.2 / 2784.0

Question Requirement: 15.11aPHIPAOrganizational.4 / 2734.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPHIPAOrganizational.4 / 2734.0

Question Requirement: 15.11cNYDOHOrganizational.3 / 2710.0

Change Count: 0

Field	Content
New Question Requirement	15.11cNYDOHOrganizational.3 / 2710.0

Question Requirement: 15.11aPHIPAOrganizational.3 / 2705.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPHIPAOrganizational.3 / 2705.0

Question Requirement: 15.11aPHIPAOrganizational.2 / 2693.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPHIPAOrganizational.2 / 2693.0

Question Requirement: 15.11aPHIPAOrganizational.1 / 2692.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPHIPAOrganizational.1 / 2692.0

Question Requirement: 15.11aTXRAMPOrganizational.1 / 2688.0

Change Count: 0

Field	Content
New Question Requirement	15.11aTXRAMPOrganizational.1 / 2688.0

Question Requirement: 1561.11c1Organizational.4 / 1488.0

Change Count: 1

Field	Content
RequirementStatement	The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization''s vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).

Question Requirement: 1574.11e2Organizational.7 / 1502.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of incidents which required the support of the organization's in-house or outsourced forensics capability , as a percentage of all incidents. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has a forensics capability, either in-house, outsourced or a combination of the two, which adequately supports its incident response capability.

Question Requirement: 1510.11a2Organizational.47 / 1434.0

Change Count: 1

Field	Content
RequirementStatement	Reports and communications of a breach are made without unreasonable delay and no later than 60 days after the discovery of the incident, unless otherwise stated by law enforcement in writing or orally. If the statement is made in writingorally, the notification is delayed for no longer than 30 days. Incident reports include a description of the event, the date of the breach, the date of discovery, a description of the types of information involved, recommended steps for individuals or organizations affected by the incident, the steps the organization has or will take to address the incident or breach, and organizational point of contact information.

Question Requirement: 1509.11a2Organizational.236 / 1433.0

Change Count: 1

Field	Content
RequirementStatement	The incident management policy refers to the specific procedures and programs to address incidents and to a forensic program. Incident management procedures are developed to provide the definition and assessment of information security incidents (e.g., an event/incident classification scale to decide whether an event classifies as an incident), provide roles and responsibilities [for the incident management program], for incident handling, to provide reporting [of security incidents], and for communication processes [of security incidents]. The organization formally assigns job titles and duties for handling computer and network security incidents to specific individuals and identifies management personnel who will support the incident handling process by acting in key decision-making roles. The incident management program includes feedback to individuals or organizations reporting an incident, tools to support the incident management activities (e.g., report and investigation forms), references to possible sanctions, plain language communications to stakeholders (e.g., law enforcement and third-party organizations or individuals affected by a breach), and automated work flows for incident management, reporting and resolution.

Question Requirement: 1555.11cFTIOrganizational.57 / 1481.0

Change Count: 1

Field	Content
RequirementStatement	The organization performs tabletop exercises using scenarios that include a breach of FTI and test the organization''s incident response policies and procedures. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

Question Requirement: 15.11cHICPOrganizational.2 / 2325.0

Change Count: 1

Field	Content
RequirementStatement	The organization has documented in its incident management program the steps to be followed in the event of malware downloaded on a computer and upon receipt of a phishing attack.

Question Requirement: 1523.11c3Organizational.24 / 1469.0

Change Count: 3

Field	Content
RequirementStatement	The organization: promptly reports incident information to appropriate authorities; and communicates with outside parties regarding the incident. This includes reporting incidents to organizations such as the Federal Computer Incident ResponseNational Cybersecurity and Communications Integration Center (FedNCCIRC) and the CERT Coordination Center (/United States Computer Emergency Readiness Team (US-CERT/CC), contacting law enforcement, and fielding inquiries from the media. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
IllustrativeProcedureImplemented	For example, select a sample of incidents and if applicable, confirm that the appropriate authorities (e.g., FedCIRC, NCCIC/US-CERT/CC, law enforcement) were promptly notified of the incident in accordance with the organization's policy.
IllustrativeProcedureMeasured	For example, measures indicate the number of applicable incidents where the appropriate authorities were promptly notified in accordance with the organization's policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that incidents are promptly reported to the appropriate authorities and outside parties (e.g., FedCIRC, NCCIC/US-CERT/CC).

Question Requirement: 1522.11c3Organizational.13 / 1468.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides an incident response support resource who is an integral part of the organization''s incident response capability and offers advice and assistance to users of information systems for the handling and reporting of security incidents. Weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents.

Question Requirement: 15.00aFedRAMPOrganizational.18 / 2490.0

Change Count: 1

Field	Content
RequirementStatement	The organization protects the incident response plan from unauthorized disclosure and modification.

Question Requirement: 15262.12cNYDOHOrganizational.10 / 2234.0

Change Count: 3

Field	Content
RequirementStatement	The organization maintains the contact information for individuals with incident handling responsibilities in the system Incident Response Plan and documents changes in the system Incident Response Plan within three [3] days of the change.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization maintains the contact information for individuals with incident handling responsibilities in the system Incident Response Plan. Examine evidence to confirm changes are documented in the system Incident Response Plan within three [3] days of the change.
IllustrativeProcedureMeasured	For example, measures indicate the number of individuals with incident handling responsibilities with contact information in the system Incident Response Plan. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and confirm that the system Incident Response Plan is changed no more than three [3] days after a change in contact information.

Question Requirement: 15970.11cCSR002Organizational.5 / 2006.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, but not limited to, obtain and examine the incident management policy and procedures, and examine evidence to confirm that the organization has employed the capability to actively search all deployed endpoints to readily identify threat indicators (e.g. , from investigations or separate intelligence source).

Question Requirement: 151207.11aSCIDSAOrganizational.2 / 1926.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of data incidents potentially and confirm that the appropriate information is being provided. Further, confirm that the incident was appropriately recorded and that the specifics were included as stipulated within the requirement statement.

Question Requirement: 151206.11aSCIDSAOrganizational.1 / 1925.0

Change Count: 1

Field	Content
RequirementStatement	The licensee is required to notify the director no later than 72 hours after notification of a cybersecurity event if South Carolina is the licensee''s state of domicile, or the licensee''s home state in the case of a producer; or the Licensee has reason to believe the information involved in the event involves no less than 250 consumers residing in the State and there' is reasonable likelihood of harm to consumer residing in the State.

Question Requirement: 1576.11ePCIOrganizational.1 / 1505.0

Change Count: 1

Field	Content
RequirementStatement	Service providers protect each organization''s hosted environment and data by enabling a process to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

Question Requirement: 15273.11aHIPAAOrganizational.1 / 2246.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s notifications to individuals affected by security events are written in plain language.

Question Requirement: 1513.11aHIPAAOrganizational.11 / 1437.0

Change Count: 1

Field	Content
RequirementStatement	In the event of a breach that must be reported to affected individuals, the organization notifies affected individuals through written notification by first-class mail, electronic mail (per a previously established and valid agreement), via next of kin if the organization knows the individual(s) is/are deceased, or a substitute form of notice reasonably calculated to reach the individual(s) as required by law. In any case deemed by the organization to require urgency because of possible imminent misuse of unsecured protected health informationPHI, the covered entity provides information to individuals by telephone or other means, as appropriate, in addition to the initial notice.

Question Requirement: 15.11aHIPAAOrganizational.8 / 2353.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal sanctions process includes failure to comply with established policies and procedures on the handling and reporting of PHI breaches.

Question Requirement: 1578.11aDEIDOrganizational.1 / 1442.0

Change Count: 1

Field	Content
RequirementStatement	Organizations receiving de-identified data notify the providing organization''s data custodian of any breach involving de-identified data in order to determine the appropriate response.

Question Requirement: 14.05iNIST80053Organizational.1 / 2781.0

Change Count: 0

Field	Content
New Question Requirement	14.05iNIST80053Organizational.1 / 2781.0

Question Requirement: 14.05iNYDOHOrganizational.6 / 2731.0

Change Count: 0

Field	Content
New Question Requirement	14.05iNYDOHOrganizational.6 / 2731.0

Question Requirement: 14.05iNYDOHOrganizational.5 / 2730.0

Change Count: 0

Field	Content
New Question Requirement	14.05iNYDOHOrganizational.5 / 2730.0

Question Requirement: 14.05iNYDOHOrganizational.4 / 2729.0

Change Count: 0

Field	Content
New Question Requirement	14.05iNYDOHOrganizational.4 / 2729.0

Question Requirement: 14.05iNYDOHOrganizational.3 / 2727.0

Change Count: 0

Field	Content
New Question Requirement	14.05iNYDOHOrganizational.3 / 2727.0

Question Requirement: 14908.05kSROrganizational.1 / 1948.0

Change Count: 1

Field	Content
RequirementStatement	Supplier complies to requirements under the supplier agreement, including maintaining and adhering to documented processes for: reviewing and scanning software developed or customized for the organization to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, and making scan results and remediation plans available to the organization upon request; cooperating with the organization and taking all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats within 90 days of notification of a threat to the organization or its customers'' nonpublic information resources originating from the supplier''s network; and notifying and cooperating with the organization upon discovery of a supplier''s noncompliance with the organization''s security requirements, or of a known or suspected threat/vulnerability impacting the organization or its customers, and to take all reasonable and necessary steps to isolate, mitigate, and/or remediate such noncompliance or threat/vulnerability within 90 days.

Question Requirement: 14909.09fSRSystem.2 / 1956.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures all supplier entities performing any in-scope work are contractually obligated to comply with the organization''s security requirements, or requirements that are no less stringent. The use of the organization''s information resources and in-scope information by supplier entities will only be for the performance of in-scope work. A documented program is maintained and adhered to by which supplier entity compliance to the organization''s security requirements is evaluated by supplier and all corrective actions are documented and implemented. The supplier will provide documentation and/or evidence to adequately substantiate such compliance, upon the organization’s request.

Question Requirement: 1407.05k2Organizational.1 / 0528.0

Change Count: 1

Field	Content
RequirementStatement	The organization employs formal contracts that, at a minimum, specify: the confidential nature and value of the covered information; the security measures to be implemented and/or complied with, including the organizations information security requirements as well as appropriate controls required by applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance; limitations to access to these services by third-parties; the service levels to be achieved in the services provided; the format and frequency of reporting to the organization''s Information Security Management Forum; the arrangement for representation of the third-party in appropriate organization meetings and working groups; the arrangements for compliance auditing of the third-parties; the penalties exacted in the event of any failure in respect of the above; and the requirement to notify a specified person or office of any personnel transfers or terminations of third-party personnel working at organizational facilities with organizational credentials, badges, or information system privileges within one business day.

Question Requirement: 1406.05k2Organizational.3 / 0522.2

Change Count: 1

Field	Content
RequirementStatement	The standard agreement with third-parties states: that the third party, following the discovery of a breach of unsecured covered information, notifies the organization of such breach, including the identification of each individual whose unsecured PII has been, or is reasonably believed by the third party to have been, accessed, acquired, or disclosed during such breach; that all [security incident and breach-related] notifications are made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a breach if the third party is an agent of the organization, otherwise the timing of the notification is explicitly addressed in the contract if the third party is not an agent of the organization; that evidence is maintained demonstrating that all [security incident and breach-related] notifications were made without unreasonable delay; that any other information that may be needed in the [security incident and breach-related] notification to individuals, either at the time notice of the breach is provided or promptly thereafter as information becomes available. The standard agreement with third-parties includes: a description of the product or service to be provided, and a description of the information to be made available along with its security classification; the target level of service and unacceptable levels of service; the definition of verifiable performance criteria, their monitoring and reporting; the right to monitor, and revoke, any activity related to the organization''s assets; the right to audit responsibilities, defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors; the penalties exacted in the event of any failure in respect of the above; the establishment of an escalation process for problem resolution; service continuity requirements, including measures for availability and reliability, in accordance with an organization''s business priorities; the respective liabilities of the parties to the agreement; responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries; intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work; conditions for renegotiation/termination of agreements, including a contingency plan in place in case either party wishes to terminate the relation before the end of the agreements; conditions for renegotiation/termination of agreements, including renegotiation of agreements if the security requirements of the organization change; conditions for renegotiation/termination of agreements, including current documentation of asset lists, licenses, agreements, or rights relating to them. The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.

Question Requirement: 1421.05j2Organizational.12 / 0513.0

Change Count: 1

Field	Content
RequirementStatement	The following security terms related to asset protection are addressed prior to giving customers access to any of the organization's assets: procedures to protect the organization''s assets, including information and software, and management of known vulnerabilities; procedures to determine whether any compromise of the assets (e.g., loss or modification of data) has occurred; integrity; restrictions on copying and disclosing information; permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; an authorization process for user access and privileges; a statement that all access that is not explicitly authorized is forbidden; and a process for revoking access rights or interrupting the connection between systems. The following security terms related to security incident management are addressed prior to giving customers access to any of the organization''s assets: reporting of information inaccuracies (e.g., of personal details), information security incidents, and security breaches; notification of information inaccuracies (e.g., of personal details), information security incidents, and security breaches; and investigation of information inaccuracies (e.g., of personal details), information security incidents, and security breaches. The following security terms are addressed prior to giving customers access to any of the organization''s assets: a description of each service to be made available; the target level of service and unacceptable levels of service; the different reasons, requirements, and benefits for customer access; responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation), especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries; and intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work. Access by customers to the organization''s information is not provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.

Question Requirement: 1424.05j2Organizational.5 / 0516.0

Change Count: 1

Field	Content
RequirementStatement	The organization has a formal mechanism to authenticate the customer''s identity prior to granting access to covered information.

Question Requirement: 1423.05j2Organizational.4 / 0515.0

Change Count: 1

Field	Content
RequirementStatement	For all system connections that allow customers to access the organization''s computing assets such as websites, kiosks, and public access terminals, the organization provides appropriate text or a link to the organization''s privacy policy for data use and protection as well as the customer''s responsibilities when accessing the data.

Question Requirement: 1401.05i2Organizational.3 / 0499.0

Change Count: 1

Field	Content
RequirementStatement	Access to the organization’s information and systems by external parties is not permitted until due diligence is carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider, the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement, all security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party, and it is ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization''s information and information assets.

Question Requirement: 1418.05i2Organizational.5 / 0502.0

Change Count: 3

Field	Content
RequirementStatement	The identification of risks related to external party access takes into account the following issues: the information asset(s) an external party is required to access; the type of access the external party will have to the information and information asset(s), such as: physical access (e.g., to offices, computer rooms, filing cabinets); logical access (e.g., to an organization''s databases, information systems); network connectivity between the organization''s and the external party''s network(s) (e.g., permanent connection, remote access); whether the access is taking place on-site or off-site; the value and sensitivity of the information involved, and its criticality for business operations; the controls necessary to protect information that is not intended to be accessible by external parties; the external party personnel involved in handling the organization''s information; how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed; the different means and controls employed by the external party when storing, processing, communicating, sharing, and exchanging information; the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information; practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident; legal and regulatory requirements and other contractual obligations relevant to the external party are taken into account; how the interests of any other stakeholders may be affected by the arrangements.
IllustrativeProcedureImplemented	For example, select a sample of third-external parties, and examine evidence to confirm that prior to providing access the organization's information systems the organization took into account the issues as noted in the requirement statement.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of risks related to third-external party access identified based on the review of a minimal set of specifically defined issues as noted in the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the identification of risks related to external party access takes into account a minimal set of specifically defined issues.

Question Requirement: 1467.05kGDPROrganizational.4 / 0538.0

Change Count: 1

Field	Content
RequirementStatement	The organization, when acting as a processor, requires the same data protection obligations in a written contract or other legal act (instrument) under EU or Member State law, which may be in electronic form, where it engages another processor for carrying out specific processing activities on behalf of the controller, and in particular provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the EU GDPR. As with the controller-to-processor, the processor-to-processor contract or legal act (instrument) also sets out the: subject-matter of the processing; duration of the processing; nature of the processing; purpose of the processing; type of personal data; categories of data subjects; and obligations and rights of each processor. The contract or other legal act (instrument) also stipulates that the processor: processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; takes all measures required pursuant by the EU GDPR for the security of processing personal data; respects the conditions for obtaining consent from the controller and stipulating data protection requirements in a contract or other legal act when engaging another processor; takes into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller''s obligation to respond to requests for exercising the data subject''s rights laid down in the EU GDPR; assists the controller in ensuring compliance with the obligations for the security of personal data, including the security of processing and data breach notification to the supervisory authority and data subject, data protection impact assessments and prior consultation with a supervisory authority, taking into account the nature of processing and the information available to the processor; at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the contract or other legal act (instrument) and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if, in the processors opinion, an instruction infringes the EU GDPR or other EU or Member State data protection provision.

Question Requirement: 1466.05kGDPROrganizational.3 / 0537.0

Change Count: 1

Field	Content
RequirementStatement	Processing by the processor is governed by a written contract or other legal act (instrument) under Union or Member State law, which may be one in electronic form, that is binding on the processor with regard to the controller. The written contract or other legal act (instrument) that governs the processor sets out the: subject-matter of the processing; duration of the processing; nature of the processing; purpose of the processing; type of personal data processed; categories of data subjects; obligations of the controller; and rights of the controller. The contract or other legal act (instrument) also stipulates that the processor: processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; takes all measures required pursuant by the EU GDPR for the security of processing personal data; respects the conditions for obtaining consent from the controller and stipulating data protection requirements in a contract or other legal act when engaging another processor; takes into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller''s obligation to respond to requests for exercising the data subject''s rights laid down in the EU GDPR; assists the controller in ensuring compliance with the obligations for the security of personal data, including the security of processing and data breach notification to the supervisory authority and data subject, data protection impact assessments and prior consultation with a supervisory authority, taking into account the nature of processing and the information available to the processor; at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; and makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the contract or other legal act (instrument) and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if, in the processors opinion, an instruction infringes the EU GDPR or other EU or Member State data protection provision.

Question Requirement: 1415.09g2System.12 / 0854.0

Change Count: 1

Field	Content
RequirementStatement	The change management on a third-party service includes an assessment and explicit recording of the potential impacts, including security impacts, of such change. Third-party changes are evaluated prior to implementation. Evaluation of third-party changes includes evaluating and implementing changes made by the organization for enhancements made to the current services offered, newly developed applications and systems, modifications or updates of the organization''s policies and procedures, and new controls to resolve information security incidents and to improve security. Evaluation of third-party changes includes evaluating and implementing changes in third-party services for changes and enhancement to networks, use of new technologies, adoption of new products or newer versions/releases, new development tools and environments, and changes to physical location.

Question Requirement: 1438.09e2System.4 / 0841.0

Change Count: 1

Field	Content
RequirementStatement	The service provider protects the company''s data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.

Question Requirement: 14.05kFTIOrganizational.4 / 2645.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 14.05kFTIOrganizational.3 / 2500.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1439.09eFTISystem.3 / 0844.1

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that information systems that receive, process, store, access, protect and/or transmit FTI must be located, operated, and accessed within the United States. When a contract developer is used, agencies mustthe organization documents, through contract requirements, that all FTI systems (i.e., beyond commercial products used as components) are located within the United States and are developed physically within the United States by United States citizens or those with lawful resident status.

Question Requirement: 1420.05jHIPAAOrganizational.34 / 0511.0

Change Count: 1

Field	Content
RequirementStatement	The organization permits an individual to request to restrict the disclosure of the individual''s covered information to a business associate for purposes of carrying out payment or healthcare operations, and is not for purposes of carrying out treatment. The organization responds to any requests from an individual on the disclosure of the individual''s covered information, providing the individual with records of disclosures of covered information that are made by the organization; and either: records of disclosures of covered information made by a business associate acting on behalf of the organization; or, a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

Question Requirement: 1448.10lCMSOrganizational.1 / 1367.0

Change Count: 3

Field	Content
RequirementStatement	The organization protects against supply chain threats by employing leading practices and methodologies such as, wherever possible, selecting components that have been previously reviewed by other government entities, (e.g., National Information Assurance Partnership [(NIAP]), as part of a comprehensive, defense-in-breadth information security strategy).
IllustrativeProcedureImplemented	For example, select a sample of new supplier contracts and confirm that the security organization is contacted and participates in the due diligence and procurement considerations process. Examine evidence to confirm that the security organization performs a security assessment on the supplier's security controls, which also takes into consideration the selection of components that have been previously reviewed by other government entities, (e.g., National Information Assurance Partnership [(NIAP]), as part of a comprehensive, defense-in-breadth information security strategy.
IllustrativeProcedureMeasured	For example, measures indicate the number of suppliers where the security organization was involved in a due diligence or procurement consideration process, as a percentage of suppliers in the supply chain. A metric could further indicate the number of threats identified by the security organization as part of their supplier assessment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization protects against supply chain threats by employing leading practices and methodologies such as, wherever possible, selecting components that have been previously reviewed by other government entities, (e.g., National Information Assurance Partnership [(NIAP]), as part of a comprehensive, defense-in-breadth information security strategy.

Question Requirement: 1408.09e1System.1 / 0838.0

Change Count: 1

Field	Content
RequirementStatement	Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions (e.g., reliability, availability, and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization''s resilience, and change management).

Question Requirement: 14.10aFTIOrganizational.7 / 2499.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1428.05k1Organizational.2 / 0523.0

Change Count: 1

Field	Content
RequirementStatement	The organization identifies and mandates information security controls to specifically address supplier access to the organization''s information and information assets.

Question Requirement: 1419.05j1Organizational.12 / 1749.0

Change Count: 1

Field	Content
RequirementStatement	The following security term is addressed prior to giving customers access to any of the organization''s assets: description of the product or service to be provided; the right to monitor, and revoke, any activity related to the organization''s assets; the respective liabilities of the organization and the customer. It is ensured that the customer is aware of their obligations. It is ensured that the customer accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization''s information and information assets.

Question Requirement: 1435.05kHIEOrganizational.1 / 0540.0

Change Count: 1

Field	Content
RequirementStatement	As part of the agreement with the connecting organizations, the HIE specifies: the requirements of the connecting organization to define and communicate to the HIE access roles for the connecting organization''s employees; that it is the sole responsibility of the connecting organization to appropriately restrict access in accordance with federal and state requirements (e.g., mental health information); and the requirements of connecting organizations to request and receive detailed access logs related to the connecting organization''s records.

Question Requirement: 1462.05jFFIECISOrganizational.1 / 0517.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides secure customer access to financial services, and develops and maintains policies and procedures to securely offer and ensure the resilience of remote financial services (e.g., using appropriate authentication, layered security controls, and fraud detection monitoring) in accordance with Appendix E of the FFIEC IT Handbook ""“ Retail Payment Systems"”” booklet.

Question Requirement: 1461.05iFFIECISOrganizational.3 / 0509.0

Change Count: 1

Field	Content
RequirementStatement	If the organization outsources management of security services to a third-party service provider, the organization addresses the key elements of outsourced security services implementation and risk management in accordance with appendix D of the FFIEC IS IT Handbook ""“Outsourcing Technology Services"”” booklet.

Question Requirement: 13.02eNYDOHOrganizational.12 / 2724.0

Change Count: 0

Field	Content
New Question Requirement	13.02eNYDOHOrganizational.12 / 2724.0

Question Requirement: 13.02eNYDOHOrganizational.10 / 2716.0

Change Count: 0

Field	Content
New Question Requirement	13.02eNYDOHOrganizational.10 / 2716.0

Question Requirement: 13.02eNYDOHOrganizational.9 / 2715.0

Change Count: 0

Field	Content
New Question Requirement	13.02eNYDOHOrganizational.9 / 2715.0

Question Requirement: 1324.07c2Organizational.1 / 0654.0

Change Count: 1

Field	Content
RequirementStatement	The organization confirms employees, contractors, and third-party users using or having access to the organization''s assets are made aware of the limits existing for their use of the organization''s information and assets associated with information processing facilities, and resources. Users are responsible for their use of any information processing resources, and of any such use carried out under their responsibility.

Question Requirement: 13.02eFedRAMPOrganizational.2 / 2425.0

Change Count: 2

Field	Content
RequirementStatement	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system''s information, when required by information system changes, and on an annual basis.
DITA	Sampling

Question Requirement: 13.07cFedRAMPOrganizational.1 / 2391.0

Change Count: 2

Field	Content
RequirementStatement	The organization reviews and updates the rules of behavior annually, receives signed acknowledgments from users indicating that they have read, understand, and agree to abide by the rules of behavior before access to information and the information system is authorized, and requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.
DITA	Sampling

Question Requirement: 1325.09s2Organizational.4 / 1053.0

Change Count: 1

Field	Content
RequirementStatement	Personnel are periodically reminded of: not discussing or leaving critical information on printing systems (e.g., copiers, printers, and facsimile machines) as these may be accessed by unauthorized personnel; taking the necessary precautions, including not to reveal covered information through being overheard or intercepted when making a phone call by: people in their immediate vicinity, particularly when using mobile phones; wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; or people at the recipient''s end; not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing; addressing the problems with printers, facsimile and copy machines, such as: unauthorized access to built-in message stores to retrieve messages; deliberate or accidental programming of machines to send messages to specific numbers; sending documents and messages to the wrong number either by misdialing or using the wrong stored number; registering demographic data, e.g., email address or other personal information, in any software to avoid collection for unauthorized use; and page caches and store page functionality that modern facsimile machines and photocopiers have in case of a paper or transmission fault, which will be printed once the fault is cleared.

Question Requirement: 13.02e1Organizational.6 / 2316.0

Change Count: 1

Field	Content
RequirementStatement	Dedicated phishing awareness training is developed as part of the organization''s onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.

Question Requirement: 1304.02e1Organizational.7 / 0343.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides role-based security-related training, especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization''s information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter.

Question Requirement: 13.02eFTIOrganizational.10 / 2620.0

Change Count: 2

Field	Content
RequirementStatement	The organization provides role-based security and privacy related training, especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization''s information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter. The organization updates role-based training content and literacy training and awareness content annually and following system changes.
DITA	Sampling

Question Requirement: 13.02eFTIOrganizational.5 / 2582.0

Change Count: 2

Field	Content
RequirementStatement	The organization ensures each employee, contractor, or sub-contractor must certify their understanding of the organization'' s security and privacy policy and procedures for safeguarding FTI through the organization''s disclosure awareness training prior to granting access to FTI, or to systems containing FTI. The initial certification and recertification must be documented and retained for at least five years.
DITA	Sampling

Question Requirement: 13.02eFTIOrganizational.11 / 2621.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1323.02ePCIOrganizational.12 / 0359.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of employees and determine if each was trained on the importance of cardholder data security policy and procedures and to be aware of attempted tampering or replacement of devices. Confirm that the training provided includes the following: (i) Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices; (ii) do not install, replace, or return devices without verification. (iii) be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices); and (iv) report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

Question Requirement: 13101.02eNYDOHOrganizational.5 / 2074.0

Change Count: 2

Field	Content
RequirementStatement	The organization provides privacy awareness training to explain the importance of and responsibility for safeguarding PII and ensuring privacy, as established in federal legislation and OMB guidance, before granting access to CMS systems and networks, and within every [365] days thereafter, to all employees contractors.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of all employees and contractors provided privacy awareness training prior to gaining access to CMS systems and networks, and within every [365] days thereafter. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls.

Question Requirement: 13997.02eNYDOHOrganizational.1 / 2070.0

Change Count: 2

Field	Content
RequirementStatement	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: within one [1] month of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter.

IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization provides incident response training to information system users consistent with assigned roles and responsibilities. Examine evidence to confirm that the training is provided within one [1] month of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter.

Question Requirement: 1315.02e2Organizational.67 / 0340.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s security personnel, including organizational business unit security points of contact, receive specialized security and privacy education and training appropriate to their role/responsibilities. The organization trains developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities, and ensures developers understand how sensitive data is handled in memory.

Question Requirement: 1314.02e2Organizational.5 / 0339.0

Change Count: 1

Field	Content
RequirementStatement	The organization conducts an internal annual review of the effectiveness of its security and privacy education and training program and updates the program to reflect risks identified in the organization''s risk assessment.

Question Requirement: 1302.02e2Organizational.134 / 0337.0

Change Count: 1

Field	Content
RequirementStatement	The organization formally creates dedicated security and privacy awareness training as part of a resource on-boarding process to the organization. The training process is formally documented, and includes the recognition and reporting of potential indicators of an insider threat. The organization''s awareness program: focuses on the methods commonly used in intrusions that can be blocked through individual action; delivers content in short online modules convenient for employees; receives frequent updates (at least annually) to address the latest attack techniques; and includes the senior leadership team''s personal messaging and involvement.

Question Requirement: 1301.02e2Organizational.7 / 0333.0

Change Count: 1

Field	Content
RequirementStatement	Security awareness training commences with a formal induction process designed to introduce the organization''s security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired. Ongoing training includes security requirements, privacy requirements, training in the correct use of information assets and facilities, and discusses how the organization addresses each area of the HITRUST CSF (e.g., audit logging and monitoring), how events or incidents are identified (e.g., monitoring for inappropriate or failed user logins), and the actions the organization takes in response to events or incidents (e.g., notifying the workforce member or the members supervisor), as appropriate to the area of training.

Question Requirement: 1336.02e2Organizational.10 / 0336.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s security awareness and training program: identifies how workforce members are provided security awareness and training; identifies the workforce members (including managers, senior executives, and as appropriate, business partners, vendors, and contractors) who will receive security awareness and training; describes the types of security awareness and training that is reasonable and appropriate for its workforce members; describes how workforce members are provided security and awareness training when there is a change in the organization''s information systems; and describes how frequently security awareness and training is provided to all workforce members.

Question Requirement: 1332.02eEHNACOrganizational.1 / 0352.0

Change Count: 1

Field	Content
RequirementStatement	Awareness training includes training on the organization''s breach reporting policies and procedures.

Question Requirement: 12.09abNYDOHSystem.6 / 2732.0

Change Count: 0

Field	Content
New Question Requirement	12.09abNYDOHSystem.6 / 2732.0

Question Requirement: 12.09aaPHIPASystem.2 / 2690.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaPHIPASystem.2 / 2690.0

Question Requirement: 12.09aaPHIPASystem.1 / 2689.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaPHIPASystem.1 / 2689.0

Question Requirement: 1258.09aaPCISystem.1 / 1146.0

Change Count: 1

Field	Content
RequirementStatement	A service provider protects each organization''s hosted environment and data by ensuring logging and audit trails are enabled, unique to each organization''s (customer''s) cardholder data environment, and consistent with PCI DSS v3.1 Requirement 10.

Question Requirement: 12156.06iNYDOHOrganizational.10 / 2129.0

Change Count: 3

Field	Content
RequirementStatement	The organization uses automated utilities to review audit records no less often than once every seventy-two [72] hours for unusual, unexpected, or suspicious behavior.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization uses automated utilities to review audit records no less often than once every seventy-two [72] hours for unusual, unexpected, or suspicious behavior.
IllustrativeProcedureMeasured	For example, measures indicate the number of automated utilities used to review audit records at no less than once every seventy-two [72] hours for actual, unexpected or suspicious behavior.

Question Requirement: 12155.06iNYDOHOrganizational.9 / 2128.0

Change Count: 3

Field	Content
RequirementStatement	The organization reviews system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four [24] 24-hour period and on demand. The information system generates alert notification for technical personnel review and assessment.

IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization reviews system records for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies no less often than once within a twenty-four [24] 24-hour period and on demand. Generate alert notification for technical personnel review and assessment.
IllustrativeProcedureMeasured	For example, measures indicate the number audit reviews that were completed every 24- hours for initialization sequences, logons (successful and unsuccessful), errors, system processes, security software (e.g., malicious code protection, intrusion detection, firewall), applications, performance, and system resource utilization to determine anomalies. Evaluate alert notifications generated in response to the review and analysis of records to appropriate technical personnel.

Question Requirement: 19.13uPHIPAOrganizational.7 / 2774.0

Change Count: 0

Field	Content
New Question Requirement	19.13uPHIPAOrganizational.7 / 2774.0

Question Requirement: 19.13fPHIPAOrganizational.6 / 2773.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.6 / 2773.0

Question Requirement: 19.13kPHIPAOrganizational.22 / 2772.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.22 / 2772.0

Question Requirement: 19.13kPHIPAOrganizational.21 / 2771.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.21 / 2771.0

Question Requirement: 19.13kPHIPAOrganizational.20 / 2770.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.20 / 2770.0

Question Requirement: 19.13pPHIPAOrganizational.3 / 2769.0

Change Count: 0

Field	Content
New Question Requirement	19.13pPHIPAOrganizational.3 / 2769.0

Question Requirement: 19.13kPHIPAOrganizational.19 / 2768.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.19 / 2768.0

Question Requirement: 19.13kPHIPAOrganizational.18 / 2767.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.18 / 2767.0

Question Requirement: 19.13dPHIPAOrganizational.5 / 2766.0

Change Count: 0

Field	Content
New Question Requirement	19.13dPHIPAOrganizational.5 / 2766.0

Question Requirement: 19.13fPHIPAOrganizational.5 / 2765.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.5 / 2765.0

Question Requirement: 19.13iPHIPAOrganizational.2 / 2764.0

Change Count: 0

Field	Content
New Question Requirement	19.13iPHIPAOrganizational.2 / 2764.0

Question Requirement: 19.13dPHIPAOrganizational.4 / 2763.0

Change Count: 0

Field	Content
New Question Requirement	19.13dPHIPAOrganizational.4 / 2763.0

Question Requirement: 19.13kPHIPAOrganizational.17 / 2762.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.17 / 2762.0

Question Requirement: 19.13kPHIPAOrganizational.16 / 2761.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.16 / 2761.0

Question Requirement: 19.13pPHIPAOrganizational.2 / 2760.0

Change Count: 0

Field	Content
New Question Requirement	19.13pPHIPAOrganizational.2 / 2760.0

Question Requirement: 19.13kPHIPAOrganizational.15 / 2759.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.15 / 2759.0

Question Requirement: 19.13oPHIPAOrganizational.1 / 2703.0

Change Count: 0

Field	Content
New Question Requirement	19.13oPHIPAOrganizational.1 / 2703.0

Question Requirement: 19.13fPHIPAOrganizational.2 / 2702.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.2 / 2702.0

Question Requirement: 19.13fPHIPAOrganizational.1 / 2701.0

Change Count: 0

Field	Content
New Question Requirement	19.13fPHIPAOrganizational.1 / 2701.0

Question Requirement: 19.13kPHIPAOrganizational.1 / 2700.0

Change Count: 0

Field	Content
New Question Requirement	19.13kPHIPAOrganizational.1 / 2700.0

Question Requirement: 19.13aPHIPAOrganizational.1 / 2699.0

Change Count: 0

Field	Content
New Question Requirement	19.13aPHIPAOrganizational.1 / 2699.0

Question Requirement: 19.06dVAD6500Organizational.1 / 2696.0

Change Count: 0

Field	Content
New Question Requirement	19.06dVAD6500Organizational.1 / 2696.0

Question Requirement: 19.13mPHIPAOrganizational.1 / 2691.0

Change Count: 0

Field	Content
New Question Requirement	19.13mPHIPAOrganizational.1 / 2691.0

Question Requirement: 19.06dTXRAMPOrganizational.2 / 2685.0

Change Count: 0

Field	Content
New Question Requirement	19.06dTXRAMPOrganizational.2 / 2685.0

Question Requirement: 19.06dTXRAMPOrganizational.1 / 2684.0

Change Count: 0

Field	Content
New Question Requirement	19.06dTXRAMPOrganizational.1 / 2684.0

Question Requirement: 19314.13iNIST80053Organizational.2 / 2287.0

Change Count: 1

Field	Content
RequirementStatement	The organization requests that the individual or individual''s authorized representative revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually.

Question Requirement: 19313.13hNIST80053Organizational.1 / 2286.0

Change Count: 1

Field	Content
RequirementStatement	The organization requests that the individual or individual''s authorized representative validate PII during the collection process.

Question Requirement: 19317.13aNIST80053Organizational.1 / 2290.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence the organization (a) provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; (b) provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; (c) obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and (d) ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Question Requirement: 19365.13eGDPROrganizational.5 / 1759.0

Change Count: 1

Field	Content
RequirementStatement	The organization allows the data subject mayto object to online entities using data for automated means using technical tools, including as an example a browser’s “do not track” feature. The data subject may object to decisions made based on automated processing that have legal or other significant impacts on the data subject.

Question Requirement: 19364.13eGDPROrganizational.4 / 1813.0

Change Count: 1

Field	Content
RequirementStatement	The organization: allows the data subject to object to the processing of their PII for the purposes of direct marketing at any time; includes profiling to the extent that its related to direct marketing; and no longer processes the data subject''s PII for such purposes upon request unless the processing is necessary for the performance of a task carried out in the public interest.

Question Requirement: 19361.13eGDPROrganizational.1 / 1811.0

Change Count: 1

Field	Content
RequirementStatement	If an individual has the authority, the controller informs the data subject of their rights to object. The controller obtains the data subject''s consent or authorization or provides the data subject an opportunity to object.

Question Requirement: 19339.13dGDPROrganizational.1 / 1802.0

Change Count: 1

Field	Content
RequirementStatement	The organization is able to demonstrate that the data subject has consented appropriately based on consent. The data subject can withdrawal consent at any time and will be notified of this when consenting. Consent is not to be used as a basis for processing if there is a power differential and services are not to be conditional upon consent when PII is not required to deliver the services.

Question Requirement: 19.13cFTIOrganizational.1 / 2679.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1901.06d2Organizational.5 / 0567.0

Change Count: 1

Field	Content
RequirementStatement	There is an appointment of a person responsible, such as a data protection officer or privacy officer, who reports directly to the highest level of management in the organization (e.g., a CEO), and is responsible for the organization''s individual privacy protection program. Such appointment is based on professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks. Responsibilities include the development and implementation of privacy policies and procedures, serving as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints, and providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that are followed. The data protection officer will, in the performance of those tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context, and purposes of processing, and may fulfill other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests. The organization supports the data protection officer in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the data protection officers expert knowledge, and ensures that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer is bound by secrecy or confidentiality concerning the performance of those tasks, in accordance with applicable law or regulation. The officer is not to be dismissed or penalized by the organization for performing those tasks.

Question Requirement: 19140.06c2Organizational.5 / 0551.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal policies, formal procedures, other critical records (e.g., results from a risk assessment), and disclosures of individuals'' protected health information are retained for a minimum of six years. For electronic health records, the organization must retain records of disclosures to carry out treatment, payment and healthcare operations for a minimum of three years.

Question Requirement: 19145.06c2Organizational.2 / 0561.1

Change Count: 1

Field	Content
RequirementStatement	A retention schedule is drawn up identifying essential record types and the period of time for which they must be retained. An inventory of sources of key information is maintained. Any related cryptographic keys are kept securely and made available only when necessary. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures are also stored to enable decryption of the records for the length of time the records are retained. Records are securely destroyed when retention is no longer necessary per the organization‘‘s record retention schedule.

Question Requirement: 19144.06c2Organizational.1 / 0560.0

Change Count: 1

Field	Content
RequirementStatement	The organization’’s established and implemented record retention program addresses: the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of covered and/or confidential information; all storage of covered and/or confidential information; and a programmatic review process (automatic or manual) to identify and remove covered and/or confidential information that exceeds the requirements of the data retention policy on a quarterly basis.

Question Requirement: 17.03aISO31000Organizational.14 / 2819.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.14 / 2819.0

Question Requirement: 17.03aISO31000Organizational.9 / 2818.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.9 / 2818.0

Question Requirement: 17.03aISO31000Organizational.13 / 2817.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.13 / 2817.0

Question Requirement: 17.03aISO31000Organizational.17 / 2816.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.17 / 2816.0

Question Requirement: 17.03aISO31000Organizational.7 / 2815.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.7 / 2815.0

Question Requirement: 17.03aISO31000Organizational.15 / 2814.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.15 / 2814.0

Question Requirement: 17.03aISO31000Organizational.10 / 2813.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.10 / 2813.0

Question Requirement: 17.03aISO31000Organizational.6 / 2812.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.6 / 2812.0

Question Requirement: 17.03aISO31000Organizational.16 / 2811.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO31000Organizational.16 / 2811.0

Question Requirement: 17.03bISO23894Organizational.15 / 2808.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.15 / 2808.0

Question Requirement: 17.03bISO23894Organizational.14 / 2807.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.14 / 2807.0

Question Requirement: 17.03bISO23894Organizational.13 / 2806.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.13 / 2806.0

Question Requirement: 17.03bISO23894Organizational.17 / 2804.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.17 / 2804.0

Question Requirement: 17.03bISO23894Organizational.16 / 2803.0

Change Count: 0

Field	Content
New Question Requirement	17.03bISO23894Organizational.16 / 2803.0

Question Requirement: 17.03aISO23894Organizational.12 / 2802.0

Change Count: 0

Field	Content
New Question Requirement	17.03aISO23894Organizational.12 / 2802.0

Question Requirement: 17.03dISO23894Organizational.1 / 2801.0

Change Count: 0

Field	Content
New Question Requirement	17.03dISO23894Organizational.1 / 2801.0

Question Requirement: 17.03aCMSOrganizational.4 / 2668.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 17.03aCMSOrganizational.3 / 2667.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 17.03aCMSOrganizational.2 / 2536.0

Change Count: 1

Field	Content
RequirementStatement	The organization: establishes, maintains, and updates within every 365 days, an inventory of all programs and systems used for collecting, creating, using, disclosing, maintaining, or sharing Personally Identifiable Information (PII); and provides each update of the PII inventory to the organization's designated privacy official or information security official to support the establishment of information security requirements for all new or modified information systems containing PII.

Question Requirement: 17.10mFTIOrganizational.9 / 2534.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 17.10aFedRAMPOrganizational.4 / 2452.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 17110.03bNYDOHOrganizational.5 / 2083.0

Change Count: 3

Field	Content
RequirementStatement	The organization ensures devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability are documented in the applicable risk assessment and security and privacy plan.
IllustrativeProcedureImplemented	For example, examine evidence to confirm devices and appliances that do not support a host-based intrusion detection system/intrusion prevention system (IDS/IPS) sensor capability are documented in the applicable risk assessment and security and privacy plan.

IllustrativeProcedureMeasured	For example, measures indicate the percentage of devices and applications that do not support host-based IDS/IPS sensor capability as a percentage of all devices and applications. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that devices and applications to do not support host-based IDS/IPS sensor capabilities are identified in the applicable risk assessment and security and privacy plan.

Question Requirement: 17108.03bNYDOHOrganizational.3 / 2081.0

Change Count: 2

Field	Content
RequirementStatement	The organization documents risk assessment results in a HIPAA Risk Analysis. Associated risks to PHI are identified within the overall risk assessment. All risk assessment documentation reflects these findings. All HIPAA Risk Analysis documentation is maintained for six [6] years from the date of creation or date it was last in effect –, whichever is later.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization documents risk assessment results in a HIPAA Risk Analysis, and associated risks to PHI are identified within the overall risk assessment, and all risk assessment documentation reflects these findings; and all HIPAA Risk Analysis documentation is maintained for six [6] years from the date of creation or date it was last in effect –, whichever is later.

Question Requirement: 17107.03bNYDOHOrganizational.2 / 2080.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of privacy impact assessments the organization has performed as a percentage of all systems, etc., upon which a privacy impact assessment is performed. The metric also includes findings resulting from the impact assessments. Reviews, tests, or audits are completed by the organization to confirm whether the organization has documented and implemented the following: i. a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and ii. privacy impact assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Question Requirement: 17106.03bNYDOHOrganizational.1 / 2079.0

Change Count: 2

Field	Content
RequirementStatement	The organization: conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; conducts an E-Authentication Risk Assessment (ERA), as required, on systems and determines e-authentication assurance levels; documents risk assessment results in the applicable security plan; reviews risk assessment results within every 365 days; disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and updates the risk assessment before issuing a new authority to operate (ATO) package or within every three [3] years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization (i) conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; (ii) conducts an E-Authentication Risk Assessment (ERA), as required, on systems and determines e-authentication assurance levels; (iii) documents risk assessment results in the applicable security plan; (iv) reviews risk assessment results within every 365 days; (v) disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and (vi) updates the risk assessment before issuing a new authority to operate (ATO) package or within every three [3] years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Question Requirement: 1780.10a2Organizational.11 / 1226.0

Change Count: 1

Field	Content
RequirementStatement	The organization formally addresses the purpose , scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements of system and information integrity requirements/controls. The organization facilitates the implementation of system and information integrity requirements/controls.

Question Requirement: 1796.10a2Organizational.15 / 1242.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the number of commercial products other than operating system software, used to store and/or process covered information, the percentage that underwent a security assessment and/or security certification by a qualified assessor prior to implementation, and the percentage without a security assessment and/or certification by a qualified assessor that are noncompliant. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization formally conducts security assessments, and/or security certification by a qualified assessor, of commercial products other than operating system software, when used to store and/or process covered information.

Question Requirement: 1795.10a2Organizational.13 / 1241.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, system acceptance testing metrics could include s te listing of information security requirements and adherence to secure system development practices. The testing is also conducted on received components and integrated systems. Select a sample of software development changethe tests performed and indicating whether tests were passed/failed/remediated, a measure of the importance and nature of the associated system, as organizationally defined, and a measure of the level of testing independence, as organizationally defined. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the independent (e.g., user acceptance) testing was conducted prior to implementationperformed by the organization to ensure the system works as expected and only as expected is proportional to the importance and nature of the system (both for in-house and for outsourced developments).

Question Requirement: 1794.10a2Organizational.12 / 1240.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, new and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. Select a sample of software development changes and examine the development records to ensure that testing (e.g., unit testing, static code analysis, data flow analysis, metrics analysis, peer code reviews) was performed during the development process.

Question Requirement: 1250.09aaFTISystem.12 / 1133.3

Change Count: 1

Field	Content
RequirementStatement	The organization''s audit record generation capability audits: all successful authorization attempts; all unsuccessful authorization attempts; all changes to logical access control authorities (e.g., rights, permissions); all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services; the enabling of audit report generation services; the disabling of audit report generation services; command line changes; batch file changes; queries made to the system (e.g., operating system, application, and database).

Question Requirement: 1250.09aaFTISystem.10 / 1133.2

Change Count: 1

Field	Content
RequirementStatement	The organization''s audit record generation capability audits: use of identification and authentication mechanisms (e.g., user ID and password); changes of file or user permissions or privileges (e.g., use of suid/guid, chown, su); remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN); all dial-in access to the system; changes made to applications by batch file; changes made to databases by batch file; application-critical record changes; changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); all system and data interactions concerning FTI; additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards Website.

Question Requirement: 12.09aaFTISystem.16 / 2551.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09aaFTISystem.15 / 2550.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09aaFTISystem.14 / 2523.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12104.09aaFedRAMPSystem.7 / 1129.0

Change Count: 3

Field	Content
RequirementStatement	The listing of auditable events and supporting rationale are reviewed and updated periodically within every 365 days or whenever changes in the threat environment are communicated to the service provider by the Joint Authorization Board (JAB).
IllustrativeProcedureImplemented	For example, examine evidence that the listing of auditable events and supporting rationale are reviewed and updated periodically. Further, confirm that the reviews and updates are periodically within every 365 days or whenever changes in the threat environment are communicated to the service provider by the Joint Authorization Board (JAB).
IllustrativeProcedureMeasured	For example, measures indicate the number of periodic reviews and updates of the listing of auditable events and supporting rationale. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the listing of auditable events and supporting rationale are reviewed and updated periodically within every 365 days or whenever changes in the threat environment are communicated to the service provider by the Joint Authorization Board (JAB).

Question Requirement: 12.09aaFedRAMPSystem.9 / 2472.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09aaFedRAMPSystem.8 / 2421.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09afFedRAMPSystem.3 / 2447.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09afFedRAMPSystem.2 / 2422.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09afCMSSystem.2 / 2575.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 12.09afCMSSystem.1 / 2574.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1207.09aa2System.4 / 1115.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures audit records are retained for 90 days and old records archived for one year to provide support for after-the-fact investigations of security incidents and to meet regulatory and the organization''s retention requirements.

Question Requirement: 1227.09af2System.1 / 1223.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that time data is protected according to the organization''s access controls and logging controls.

Question Requirement: 1288.09abCISSystem.13 / 1162.0

Change Count: 1

Field	Content
RequirementStatement	The organization profiles each user''s typical account usage by determining normal time-of-day access and access duration. The organization generates reports that indicate users who have logged in during unusual hours, that indicate users who have exceeded their normal login duration, and which includes flagging the use of the user''s credentials from a computer other than computers on which the user generally works.

Question Requirement: 1282.09aaCISSystem.11 / 1121.0

Change Count: 1

Field	Content
RequirementStatement	The organization logs all URL requests from each of the organization''s systems, whether onsite or on a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

Question Requirement: 11.01qNYDOHSystem.12 / 2723.0

Change Count: 0

Field	Content
New Question Requirement	11.01qNYDOHSystem.12 / 2723.0

Question Requirement: 11.01bNYDOHSystem.4 / 2709.0

Change Count: 0

Field	Content
New Question Requirement	11.01bNYDOHSystem.4 / 2709.0

Question Requirement: 11.02iPHIPAOrganizational.1 / 2698.0

Change Count: 0

Field	Content
New Question Requirement	11.02iPHIPAOrganizational.1 / 2698.0

Question Requirement: 11.01bCMSSystem.3 / 2538.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01aCMSOrganizational.2 / 2544.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11131.01u1System.2 / 0243.0

Change Count: 1

Field	Content
RequirementStatement	Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization''s security management). Connection time controls include using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration), restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation, and re-authentication at timed intervals.

Question Requirement: 11.01eFTISystem.1 / 2521.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 1154.01c3System.4 / 0046.0

Change Count: 1

Field	Content
RequirementStatement	Contractors are provided with minimal system and physical access, and agree to and support the organization''s security requirements. The contractor selection process assesses the contractor''s ability to adhere to and support the organization''s security policy and procedures.

Question Requirement: 1153.01c3System.35 / 0045.0

Change Count: 1

Field	Content
RequirementStatement	All file system access not explicitly required for system, application, and administrator functionality is disabled. The organization ensures only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of the users'' job duties.

Question Requirement: 1179.01j3Organizational.1 / 0131.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s information system monitors and controls remote access methods.

Question Requirement: 11.09abFedRAMPSystem.13 / 2483.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01nFedRAMPOrganizational.2 / 2375.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11202.01jFedRAMPOrganizational.3 / 0136.0

Change Count: 1

Field	Content
RequirementStatement	The organization provides the capability to expeditiously disconnect or disable remote access to the organization''s system(s) within 15 minutes based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information system(s).

Question Requirement: 11.01tFedRAMPSystem.2 / 2477.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01tFedRAMPSystem.1 / 2476.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01qFedRAMPSystem.4 / 2385.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 11.01qFedRAMPSystem.3 / 2382.0

Change Count: 1

Field	Content
RequirementStatement	The organization manages information system identifiers by: receiving authorization from, at a minimum, the ISSO (or similar role within the organization) to assign an individual, group, role, or device identifier; selecting an identifier that identifies an individual, group, role, or device; assigning the identifier to the intended individual, group, role, or device; preventing reuse of identifiers for 2two years; and disabling the identifier after 35 days.

Question Requirement: 0908.10g2Organizational.4 / 1297.0

Change Count: 3

Field	Content
RequirementStatement	Tohe organization maintain thes availability of information in the event of the loss of cryptographic keys, the organization by users. Mechanisms are employed to: prohibits the use of encryption keys that are not recoverable by authorized personnel; requires senior management approval to authorize recovery of keys by anyone other than the key owner; and compliesy with approved cryptography standards.
IllustrativeProcedureImplemented	For example, in the event where encryption keys are lost, examine evidence to confirm that the organization has implemented mechanisms to recover the key, such as key escrow (e.g., AWS KMS, Vault). This can be confirmed through observation of the key escrow in operation. Further, through review of the key escrow agreement, confirm that encryption keys are only recoverable from authorized personnel and that senior management approval is required.
IllustrativeProcedureMeasured	For example, measures indicate the number of encryption keys that have been lost and the percentage of information that was recovered through recovery of the encryption key. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that specific mechanisms are in place to recover infemployed to prohibit the use of encryption keys that are not recoverable by authorized personnel, require senior mation in the event encryption keys are lostnagement approval to authorize recovery of keys by other than the key owner, and comply with approved cryptography standards.

Question Requirement: 0907.10g2Organizational.2 / 1296.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures keys are limited to a period of time, per the manufacturer''s recommendations, or keys are replaced annually if not specified by the manufacturer.

Question Requirement: 0906.10g2Organizational.13 / 1295.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s key management system is consistent with federal or industry-recognized guidelines and best practices relating to: verifying user identity prior to generating new certificates or keys; generating keys for different cryptographic systems and different applications; generating and obtaining public key certificates; distributing keys to intended users, including how keys are activated when received; storing keys in the fewest possible locations, including how authorized users obtain access to keys; changing or updating keys including rules on when keys are changed and how this will be done as deemed necessary and recommended by the associated application; and at least annually; revoking keys including how keys are withdrawn or deactivated (e.g., when keys have been compromised or suspected to have been compromised or when a user leaves an organization, in which case keys are also archived); recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information); archiving keys (e.g., for information archived or backed up); destroying keys; and logging and auditing of key management related activities. The organization securely manages secret and private keys, including the authenticity of public keys using public key certificates issued by a trusted Certification Authority (CA) that is a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

Question Requirement: 0904.10f2Organizational.1 / 1290.0

Change Count: 1

Field	Content
RequirementStatement	When implementing the organization''s cryptographic policy and procedures, the regulations and national restrictions that apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information are adhered to.

Question Requirement: 09.09yFTIOrganizational.5 / 2559.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0957.09mCISOrganizational.15 / 0961.0

Change Count: 1

Field	Content
RequirementStatement	The organization maintains and enforces network-based URL filters that limit a system''s ability to connect to websites not approved by the organization. The organization specifically blocks access to known file transfer and email exfiltration websites. The organization subscribes to URL categorization services to ensure that they are up to date with the most recent website category definitions available. Uncategorized are blocked by default. This filtering is enforced for each of the organization''s systems, whether they are physically at an organization''s facilities or not.

Question Requirement: 08.09mTXRAMPOrganizational.1 / 2683.0

Change Count: 0

Field	Content
New Question Requirement	08.09mTXRAMPOrganizational.1 / 2683.0

Question Requirement: 08114.01wSRSystem.1 / 1784.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures sensitive applications and information are segregated from other customer''s or supplier''s own application or information by using logical access controls and/or physical access controls.

Question Requirement: 0815.01o1Organizational.1 / 0189.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points. The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The application-layer filtering proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a disallow list, or applying lists of allowed sites that can be accessed through the proxy while blocking all other sites. O The organizations forces outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Internal directory services and internal IP addresses are protected and hidden from any external access. Requirements for network routing control are based on the access control policy.

Question Requirement: 0814.01n1Organizational.12 / 0177.0

Change Count: 1

Field	Content
RequirementStatement	At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of its business applications.

Question Requirement: 08.01wFTISystem.4 / 2676.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 08.01nFedRAMPOrganizational.4 / 2492.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0887.09n2Organizational.5 / 0990.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the metric could indicate the number of connections from an information system to an external information system where the documentation of each connection is not policy-compliant . Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements regardless of type if non-compliance with the requirements for interconnection security agreements can be ascertained. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization requires external/outsourced service providers to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services.

Question Requirement: 0886.09n2Organizational.4 / 0989.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the metric could indicate the number of connections from an information system to an external information system where the documentation of each connection is not policy compliant . Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements, regardless of type, if non-compliance with the requirements for interconnection security agreements can be ascertained. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization employs, and documents in a formal agreement or other document, either i) allow-all, deny-by-exception, or ii) deny-all, permit-by-exception (preferred), policy for allowing specific information systems to connect to external information systems.

Question Requirement: 0836.09n2Organizational.1 / 0986.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the metric could indicate the number of connections from an information system to an external information system where the documentation of each connection is not policy-compliant . Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements regardless of type if non-compliance with the requirements for interconnection security agreements can be ascertained. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that formal agreements with external information system providers include specific obligations for security and privacy.

Question Requirement: 0821.09m2Organizational.2 / 0934.0

Change Count: 1

Field	Content
RequirementStatement	All network connections and changes to the firewall, router, and switch configurations are approved and tested. Any deviations from the standard configuration or updates to the standard configuration are documented and approved in a change control system. All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, are also documented and recorded, with a specific business reason for each change, a specific individual'' s name responsible for that business need, and an expected duration of the need.

Question Requirement: 0806.01m2Organizational.12356 / 0161.0

Change Count: 1

Field	Content
RequirementStatement	Networks are divided into separate logical network domains (e.g., an organization''s internal network domains and external network domains) each protected by a defined security perimeter. Separate domains are implaemented by controlling the network data flows using routing/switching capabilities, including access control lists, according to applicable flow control policies. The domains are defined based on a risk assessment and the different security requirements within each of the domains. A graduated set of controls is applied in different logical network domains to further segregate the network security environments (e.g., publicly accessible systems, internal networks; critical assets; and key information security tools, mechanisms, and support components associated with system and security administration). The organization implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. To ensure proper separation, the organization verifies any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, moves it to an internal VLAN and gives it a private address. The criteria for segregation of networks into domains is based on the access control policy and access requirements, and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. Segregation of networks is based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

Question Requirement: 11200.01b2System.11 / 0028.0

Change Count: 1

Field	Content
RequirementStatement	Identity verification of the individual is required prior to establishing, assigning, or certifying an individual''s electronic signature or any element of such signature.

Question Requirement: 1109.01b2System.6 / 0021.0

Change Count: 2

Field	Content
RequirementStatement	User registration and deregistration, at a minimum: communicates password procedures and policies to all users who have system access; grants access to the information systems based on minimum necessary for assigned official duties, intended system usage and personnel security criteria such that usage/access is granular enough to support an individual''s consent that has been captured by the organization and limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function; checks that the user has authorization from the system owner for the use of the information system or service; separates approval for access rights from management; checks that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy (e.g., it is consistent with sensitivity and risks associated with the information and/or information system, and it does not compromise segregation of duties); gives users a written statement of their access rights; requires users to sign statements indicating that they understand the conditions of access; ensures service providers do not provide access until authorization procedures have been completed; maintains a formal record of all persons registered to use the service; removes or blocks critical access rights of users who have changed roles or jobs or left the organization immediately; removes or blocks non-critical access within twenty-four (24) hours; and automatically removes or disables accounts within ninety (90) days that have been inactive for a period of sixty (60) days or more.
IllustrativeProcedureImplemented	For example, select a sample of users and examine evidence to confirm: that password and access control policies were communicated to users as well as a written statement of their access rights; that access was not provided until authorization procedures were completed; that authorization was checked prior to granting access; that a separate approval was provided by management for access rights; that a check was performed to ensure the level of access granted was the minimum necessary to satisfy a particular purpose or carry out a function, was appropriate to the business purpose, and was consistent with organizational policy; and that the user signed a statement indicating that they understand the conditions of access. Further, select a sample of systems and ensure that a formal record of all persons registered to use the system is maintained; and that accounts that have been inactive for a period of sixty (60) days or more are automatically removing or disabled within ninety (90) days. Further, select a sample of transferring and terminated personnel and ensure that any associated critical access rights were removed or blocked immediately and that any non-critical access rights were removed or blocked within twenty-four (24) hours.

Question Requirement: 1108.01b2System.5 / 0020.0

Change Count: 1

Field	Content
RequirementStatement	Account managers are notified when users are: terminated, transferred, their information system usage or need-to-know/need-to-share changes, or when accounts (including shared/group, emergency, and temporary accounts) are no longer required. Account managers modify the user''s account accordingly.

Question Requirement: 11125.01s2System.2 / 0236.0

Change Count: 1

Field	Content
RequirementStatement	The use of system utilities is controlled by implementing authorization for ad hoc use of systems utilities, limiting the availability of system utilities (e.g., limitation of availability by setting restrictive file system level permissions for the access and execution of system utilities such as cmd.exe, ping, tracert, ipconfig, etc.), disabling of public '"“read"”' access to files, objects, and directories, logging of all use of system utilities, defining and documenting authorization levels for system utilities, the deletion of, or file system file execution permission denial of, all unnecessary software based utilities and system software, and the denial of system utilities availability to users who have access to applications on systems where segregation of duties is required. The information system owner regularly reviews the system utilities available to identify and eliminate unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary Web servers.

Question Requirement: 11110.01q2System.10 / 0205.0

Change Count: 1

Field	Content
RequirementStatement	Non-organizational users, or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization''s information systems, are uniquely identified and authenticated.

Question Requirement: 1135.02i3Organizational.1 / 0378.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of terminated employees/contractors and confirm that access to the organization's systems was restricted or removed within 24 hours of receiving notice. Further, examine evidence to confirm that a review is performed to identify and close accounts older than 90 days.

IllustrativeProcedureMeasured	For example, measures indicate the number of terminated employees/contractors accounts that have been restricted or removed within 24 hours of receiving notice as a percentage of all terminated accounts. Further, a metrics indicate the number old accounts that have been removed as part of the 90-day review. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that upon termination or changes in employment for employees, contractors, third-party users or other workforce arrangement, physical and logical access rights and associated materials (e.g., passwords, keycards, keys, or documentation that identify them as current members of the organization) are removed or modified to restrict access within 24 hours and old accounts are closed after 90 days of opening new accounts.

Question Requirement: 1165.01cPCISystem.1 / 0066.0

Change Count: 2

Field	Content
RequirementStatement	A service provider protects each organization''s hosted environment and data by: ensuring that each organization only runs processes that only have access to that organization''s cardholder data environment, and restricting each organization' 's access and privileges to only its own cardholder data environment.
IllustrativeProcedureMeasured	For example, measures indicate the number of entities the service provider is hosting, of which a percentage of those has appropriately implemented controls to ensure that each organization only runs processes that only have access to that organization's cardholder data environment and restricts each organization's access and privileges to only its own cardholder data environment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that a service provider protects each organizations hosted environment and data by (i) ensuring that each organization only runs processes that only have access to that organization's cardholder data environment , and (ii) restricting each organization's access and privileges to only its own cardholder data environment.

Question Requirement: 11140.01vPCISystem.4 / 0264.0

Change Count: 1

Field	Content
RequirementStatement	If there is an authorized business need to allow the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media for personnel accessing cardholder data via remote-access technologies, then the organization''s usage policies require the data be protected in accordance with all applicable PCI DSS requirements.

Question Requirement: 11988.01tNYDOHSystem.1 / 2061.0

Change Count: 3

Field	Content
RequirementStatement	The organization restricts remote access sessions to last no longer than twenty-four [24] hours.
IllustrativeProcedureImplemented	For example, examine evidence, which could be technical control configurations or settings on remote access devices, tools, or utilities, to confirm the organization restricts remote access sessions to last no longer than twenty-four [24] hours. Ensure that the information system demonstrates enabled automated mechanisms that regulate automated log-out for inactivity and enforcement of work-day access restrictions. Inspect organizational personnel workstations after hours to verify users have logged out and interview organizational personnel with account management responsibilities.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of remote access sessions that are within the twenty-four [24] hour parameter. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify remote access sessions last no longer than twenty-four [24] hours.

Question Requirement: 11982.01qNYDOHSystem.11 / 2055.0

Change Count: 1

Field	Content
RequirementStatement	The organization manages information system authenticators by: verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; establishing initial authenticator content for authenticators defined by the organization; ensuring that authenticators have sufficient strength of mechanism for their intended use; establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; changing default content of authenticators prior to information system installation. The organization manages information system authenticators by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators. Passwords are valid for no longer than sixty (60) days or immediately in the event of known or suspected compromise, and immediately upon system installation (e.g., default or vendor-supplied passwords). PIV compliant access cards are valid for no longer than five [5] years. PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three [3] years. Any PKI authentication request is validated by Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) to ensure that the certificate being used for authentication has not been revoked. The organization manages information system authenticators by: protecting authenticator content from unauthorized disclosure and modification; requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; changing authenticators for group/role accounts when membership to those accounts changes.

Question Requirement: 11980.01qNYDOHSystem.11 / 2053.0

Change Count: 3

Field	Content
RequirementStatement	The organization manages information system identifiers by: receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; selecting an identifier that identifies an individual, group, role, or device; assigning the identifier to the intended individual, group, role, or device; preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three [3] years or more has passed; and disabling the identifier after sixty [60] days of inactivity for Moderate systems.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization manages information system identifiers by: (i) receiving authorization from defined personnel or roles (defined in the applicable security plan) to assign an individual, group, role, or device identifier; (ii) selecting an identifier that identifies an individual, group, role, or device; (iii) assigning the identifier to the intended individual, group, role, or device; (iv) preventing reuse of identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of three [3] years or more has passed; and (v) disabling the identifier after sixty [60] days of inactivity for Moderate systems.
IllustrativeProcedureMeasured	For example, measures indicate the number of duplicate identifiers that exist in the environment as a percentage of all accounts. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization ensures identifiers are disabled after sixty [60] days of inactivity.

Question Requirement: 11972.01jNYDOHOrganizational.2 / 2045.0

Change Count: 3

Field	Content
RequirementStatement	The organization requires callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. For application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a User ID and password and enters the network through the standard authentication process. Access to such systems is authorized and logged. User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.

IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization requires callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. Examine evidence (e.g., documents or system configurations) to confirm, for application systems and turnkey systems that require the vendor to log-on, the vendor is assigned a User ID and password and enters the network through the standard authentication process. Examine evidence (e.g., system configurations) to confirm that access to such systems will be authorized and logged and User IDs assigned to vendors will be recertified within every three hundred sixty-five (365) days.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used that are verified with callback capability with re-authentication and include all the vendor authentication parameters prescribed by the control requirement statement, including User ID recertification within every three hundred sixty-five [365] days. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls.

Question Requirement: 11148.02g2Organizational.3 / 0371.0

Change Count: 3

Field	Content
RequirementStatement	The communication of termination responsibilities include ongoing security requirements, legal responsibilities, and where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment or other workforce arrangement continuing for a defined period after the end of the employee''s, contractor's's, or third-party user''s employment or other workforce arrangement.
IllustrativeProcedureImplemented	For example, select a sample of employees/workforce members and examine their employment contract and confirm that the organization has defined and documented termination responsibilities, including ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment or other workforce arrangement continuing for a defined period after the end of the employee's, contractor's, or third-party user's employment or other workforce arrangement.

IllustrativeProcedureMeasured	For example, measures indicate the number of employees/workforce members that did not have an appropriate employment contract that included termination of responsibilities as stipulated in the requirement statement, as a percentage of all employees. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the communication of termination responsibilities include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment or other workforce arrangement continuing for a defined period after the end of the employee's, contractor's, or third-party user's employment or other workforce arrangement.

Question Requirement: 11147.02g2Organizational.2 / 0370.0

Change Count: 1

Field	Content
RequirementStatement	The organization defines any valid duties after termination of employment or when the arrangement of a workforce member ends. Any valid duties after termination of employment or when the arrangement of a workforce member ends are included in the employee''s or workforce members contract or other arrangement.

Question Requirement: 11186.01eCISSystem.3 / 0104.0

Change Count: 1

Field	Content
RequirementStatement	The organization monitors for dormant accounts, and notifies the user or user''s manager of dormant accounts. The organization disables dormant accounts if not needed, or documents and monitors exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). The organization requires that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators are required to disable accounts that are not assigned to valid workforce members.

Question Requirement: 11184.01cCISSystem.10 / 0051.0

Change Count: 1

Field	Content
RequirementStatement	Administrators use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine is isolated from the organization''s primary network and is not allowed Internet access. This machine is not used for reading email, composing documents, or surfing the Internet.

Question Requirement: 1170.01eHIESystem.1 / 0106.0

Change Count: 1

Field	Content
RequirementStatement	The organization, acting as a Health Information Exchange (HIE), reviews user access every 90 days, for all employees and for all employees of connecting organizations, and reviews the appropriateness of each user''s role every 90 days for all employees and for all employees of connecting organizations. Any discrepancies are remediated immediately following the review.

Question Requirement: 1164.01cHIESystem.1 / 0063.0

Change Count: 1

Field	Content
RequirementStatement	The organization, acting as a HIE, defines and assigns roles to all employees and to all employees of connecting organizations with access to the HIE. The roles are based on the individuals'' job function and responsibilities. The roles specify the type of access and level of access.

Question Requirement: 10.01dTXRAMPSystem.1 / 2372.0

Change Count: 1

Field	Content
RequirementStatement	The information system, for password-based authentication: enforces minimum password complexity of a minimum of twelve12 characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters; enforces at least one changed character when new passwords are created; stores and transmits only encrypted representations of passwords; enforces lifetime restrictions of one day minimum and 60 day maximum; prohibits password reuse for 24 generations; and allows the use of a temporary password for system logons with an immediate change to a permanent password.

Question Requirement: 1035.01dFTISystem.3 / 0091.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures passwords are prohibited from being reused for at least six generations and at least four characters are changed when new passwords are created.

Question Requirement: 10.01dFedRAMPSystem.4 / 2384.0

Change Count: 1

Field	Content
RequirementStatement	The organization employs automated tools to determine if password authenticators are configured to satisfy complexity requirements as stipulated in the organization''s information security policy.

Question Requirement: 1026.01dFedRAMPSystem.1 / 0087.0

Change Count: 1

Field	Content
RequirementStatement	The organization enforces the following minimum password requirements: minimum password age = 1/1; maximum password age = 60/60; minimum password length = 12 characters; password complexity = at least one of each of upper-case letters, lower-case letters, numbers, and special characters; password history size = 6; at least one character be changed; and prohibit password reuse for 24 hours.

Question Requirement: 1025.01dHIXSystem.2 / 0093.0

Change Count: 1

Field	Content
RequirementStatement	The organization enforces the following minimum password requirements (user/ / privileged/ / process [acting on behalf of a Uuser]): minimum password age = 1/1/1; maximum password age = 60/60/180; minimum password length = 8/8/15; password complexity = 1/1/3 (minimum one character, [three for a process]) from the four character categories (A-Z, a-z, 0-9, special characters); and password history size = 24/24/24. The information system uses password-protected initialization (boot) settings.

Question Requirement: 1033.01dHIXSystem.4 / 0095.0

Change Count: 1

Field	Content
RequirementStatement	If the system allows, at least four characters are changed when new passwords are created.

Question Requirement: 1027.01d2System.6 / 0080.0

Change Count: 1

Field	Content
RequirementStatement	Electronic signatures that are not based upon biometrics: employ at least two distinct identification components (e.g., user ID and password)–when an individual executes a series of signings during a single continuous period of controlled system access, the first signing is executed using all electronic signature components, and subsequent signings are executed using at least one electronic signature component (when an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing is executed using all of the electronic signature components); and are administered and executed to ensure that attempted use of an individual''s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals (e.g., system administrator and supervisor).

Question Requirement: 09.10gFTIOrganizational.1 / 2564.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0964.10gFedRAMPOrganizational.1 / 1299.0

Change Count: 1

Field	Content
RequirementStatement	The organization produces, controls, and distributes asymmetric cryptographic keys using NSA-approved key management technology and processes, approved PKI Class 3 certificates or prepositioned keying material, or approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user''s private key.

Question Requirement: 0966.09sGDPROrganizational.2 / 1069.0

Change Count: 1

Field	Content
RequirementStatement	Appropriate safeguards for cross-border flows of personal data include: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority and approved by the Commission; an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects'' rights; or an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects'' rights. If authorized by the relevant supervisory authority, appropriate safeguards may also include contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Question Requirement: 0965.09sGDPROrganizational.1 / 1068.0

Change Count: 1

Field	Content
RequirementStatement	The organization maintains records of the basis used to authorize cross-border flows of personal data to a third country or international organization, which include but are not limited to: an adequacy decision by the EU Commission; the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; binding corporate rules approved by the relevant supervisory authority; A court judgement or administrative decision of a third country if based on an international agreement between the third country and the EU; Or if one of the following conditions are met: the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject''s request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; the transfer is necessary for important reasons of public interest; the transfer is necessary for the establishment, exercise or defense of legal claims; the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case.

Question Requirement: 09218.09vNYDOHOrganizational.1 / 2190.0

Change Count: 1

Field	Content
RequirementStatement	Email and any attachment that contains sensitive information when transmitted inside and outside of HHS premises are encrypted using the user’s personal identity verification (PIV) card when possible. If PIV encryption is not feasible, a FIPS 140-2 validated solution must be employed. Password protection of files is recommended to add an additional layer of data protection but shall not be used in lieu of encryption solutions. Password and/or encryption keys are not be included in the same email that contains sensitive information or in separate email, and password/encryption key is provided to the recipient separately via text message, verbally, or other out-of-band solution.

Question Requirement: 0902.09s2Organizational.13 / 1057.0

Change Count: 1

Field	Content
RequirementStatement	The organization permits authorized individuals to use an external information system to access the information system or to process, store or transmit organization-controlled information only when the organization: verifies the implementation of required security controls on the external system as specified in the organization''s information security policy and security plan; or, retains approved information connection or processing agreements with the organizational entity hosting the external information system .

Question Requirement: 0947.09y2Organizational.2 / 1094.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures the storage of the transaction details are located outside of any publicly accessible environments (e.g., on a storage platform existing on the organization''s intranet), not retained, and not exposed on a storage medium directly accessible from the Internet.

Question Requirement: 0938.09x2Organizational.4 / 1084.0

Change Count: 1

Field	Content
RequirementStatement	The confidentiality and integrity for electronic commerce is maintained by: ensuring the level of confidence each party requires in each other''s claimed identity (e.g., through authentication); ensuring the authorization processes associated with who may set prices, issue or sign key trading documents; ensuring that trading partners are fully informed of their authorizations; determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts (e.g. associated with tendering and contract processes); ensuring the level of trust required in the integrity of advertised price lists; ensuring the confidentiality of any covered data or information; ensuring the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts; ensuring the degree of verification appropriate to check payment information supplied by a customer; selecting the most appropriate settlement form of payment to guard against fraud; ensuring the level of protection required to maintain the confidentiality and integrity of order information; ensuring avoidance of loss or duplication of transaction information; ensuring liability associated with any fraudulent transactions; and ensuring insurance requirements.

Question Requirement: 0934.09w2Organizational.12 / 1047.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, review written policies to verify the existence of procedures stating the internal information system components and security and business implications of interconnected business information systems. Confirm that the following have been defined and documented: (i) authorizes and approves connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; (ii) documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated along with their security and business implications; (iii) known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization; (iv) restricting access to diary information relating to selected individuals (e.g., personnel working on sensitive projects); and (v) vulnerabilities of information in business communication systems (e.g., recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail). This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Question Requirement: 0937.09w2Organizational.5 / 1050.0

Change Count: 1

Field	Content
RequirementStatement	A firewall''s physical and logical configuration is established to restrict connections between untrusted networks and systems storing, processing, or transmitting covered information.

Question Requirement: 0935.09w2Organizational.3 / 1048.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, review written policies to verify the existence of procedures linking interconnected business systems to other requirements and controls. Confirm that the following have been defined and documented: (i) the separation of operational systems from interconnected system; (ii) the retention and backup of information held on the system; and (iii) the fallback requirements and arrangements. This control applies to connections between organizational information systems and (separate) constituent system components (i.e., intra-system connections) including, for example, system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers. Instead of authorizing each individual internal connection, organizations can authorize internal connections for a class of components with common characteristics and/or configurations, for example, all digital printers, scanners, and copiers with a specified processing, storage, and transmission capability or all smart phones with a specific baseline configuration.

Question Requirement: 0835.09n1Organizational.1 / 0985.0

Change Count: 1

Field	Content
RequirementStatement	The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored. The right to audit is agreed by management for each network service provider. The security arrangements necessary for particular network services'' security features, service levels, and management requirements, are identified and documented.

Question Requirement: 08.09m1Organizational.8 / 2362.0

Change Count: 1

Field	Content
RequirementStatement	The organization prevents enterprise assets from accessing known malicious addresses and domains on the Internet (for example by means of browser configurations, DNS sinkholing, and/or use of a subscription service) —, unless there is a clear, documented business need and the organization understands and accepts the associated risk.

Question Requirement: 08.09nFTIOrganizational.1 / 2654.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 08.09mFTIOrganizational.7 / 2502.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0879.09mFTIOrganizational.2 / 0977.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of FTI that is identified and analyzed and how it flows from client to database server in accordance with the organization's policy . Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the security arrangements necessary for particular services including security features, service levels, and management requirements, are identified and documented.

Question Requirement: 0899.01oCISOrganizational.4 / 1885.0

Change Count: 1

Field	Content
RequirementStatement	The organization disables all workstation-to-workstation communication to limit an attacker''s ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.

Question Requirement: 0720.07aNYDOHOrganizational.4 / 0628.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s asset inventory does not duplicate other inventories unnecessarily, but will ensure that the content is aligned.

Question Requirement: 0787.10m2Organizational.14 / 1377.0

Change Count: 1

Field	Content
RequirementStatement	The organization requires patches installed in the production environment to also be installed in the organization''s disaster recovery environment in a timely manner, as defined by the organization.

Question Requirement: 0786.10m2Organizational.13 / 1376.0

Change Count: 1

Field	Content
RequirementStatement	A prioritization process is required to determine which patches must be applied across the organization''s systems.

Question Requirement: 0710.10m2Organizational.1 / 1370.0

Change Count: 2

Field	Content
RequirementStatement	The configuration standard for all system components (workstations, databases, servers, applications, routers, switches, wireless access points) are hardened to address, to the extent practical, all known security vulnerabilities. In particular, laptops, workstations, and servers are configured so they will not auto-run content from removable media (e.g., USB tokens–thumb drives, USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares). The organization''s configuration standards are consistent with industry-accepted system hardening standards (e.g., CIS, ISO, NIST, SANS).
IllustrativeProcedureImplemented	For example, confirm whether a configuration standard has been defined and created (e.g., hardened OS image). Select a sample of system components (e.g., workstations, databases, servers, applications) and determine if the configuration is consistent with the organization's defined hardening standard - and industry standards (e.g., CIS, ISO, SANS, NIST). Further, confirm that system components have been configured to disable the auto-run features for removable media (e.g., USB tokens–thumb drives, USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares).

Question Requirement: 0717.10m3Organizational.2 / 1379.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s vulnerability scanning tools are regularly updated with all relevant information system vulnerabilities or it updates its list of vulnerabilities based on a subscription to one or more vulnerability intelligence services to stay aware of emerging exposures.

Question Requirement: 07.09rFedRAMPOrganizational.1 / 2450.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07.10mFedRAMPOrganizational.17 / 2417.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 07241.10mNYDOHOrganizational.8 / 2213.0

Change Count: 3

Field	Content
RequirementStatement	The organization employs automated mechanisms no less often than once every seventy-two [72] hours to determine the state of information system components regarding flaw remediation.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization employs automated mechanisms no less often than once every seventy-two [72] hours to determine the state of information system components regarding flaw remediation.
IllustrativeProcedureMeasured	For example, measures indicate the number of vulnerabilities that have been remediated to determine the current state of the information system components regarding flaw remediation. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization employs automated mechanisms no less often than once every seventy-two [72] hours to determine the state of information system components regarding flaw remediation.

Question Requirement: 0703.07a2Organizational.1 / 0632.0

Change Count: 1

Field	Content
RequirementStatement	The ownership, custodianship, and information classification is agreed and documented for each of the assets. The ownership, custodianship, and information classification is based on the identified importance of the asset, the business value of the asset, security classification of the asset, levels of protection of the asset, and sustainment commensurate with the importance of the assets. The inventory of assets identifies protection and sustainment requirements commensurate with the asset''s categorization.

Question Requirement: 0770.10mCISOrganizational.12 / 1390.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures, wherever possible, that Red Team''s results are documented using open, machine-readable standards (e.g., SCAP), and devises a scoring method for determining the results of Red Team exercises, so that results can be compared over time.

Question Requirement: 06146.06hNYDOHOrganizational.3 / 2119.0

Change Count: 3

Field	Content
RequirementStatement	The organization performs automated reviews of the information system no less often than once every seventy-two [72] hours to identify changes in functions, ports, protocols, and/or services.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization performs automated reviews of the information system no less often than once every seventy-two [72] hours to identify changes in functions, ports, protocols, and/or services.
IllustrativeProcedureMeasured	For example, measures indicate the organization performs automated reviews of the information system no less than once every seventy-two [72] hours. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that issues identified in automated reviews of the information system no less often than once every seventy-two [72] hours are assigned and addressed consistently with policy/control requirements.

Question Requirement: 0607.10h2System.23 / 1307.0

Change Count: 1

Field	Content
RequirementStatement	A configuration control system is used to keep control of all implemented software as well as the system documentation. Previous versions of application software are retained as a contingency measure. Old versions of software are archived. All required information and parameters, procedures, configuration details, and supporting software associated with the old versions are archived for as long as the data is retained in archive or as dictated by the organization''s data retention policy.

Question Requirement: 0664.10h2System.10 / 1311.0

Change Count: 1

Field	Content
RequirementStatement	The organization: identifies unauthorized (disallow listed) software on servers; identifies unauthorized (disallow listed) software on workstations; identifies unauthorized (disallow listed) software on laptops; employs an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized (disallow listed) software; and reviews and updates the list of unauthorized (disallow listed) software periodically - but no less than annually.

Question Requirement: 0622.09d2System.1 / 0834.0

Change Count: 1

Field	Content
RequirementStatement	Separation between operational, test, and development environments is identified and controls are implemented to prevent operational issues, including: Along with removing accounts, a review of all custom code preceding the release to production or to customers is completed in order to identify any possible coding vulnerability. Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines. Appropriate corrections [to code identified through code reviews] are implemented prior to release. Code-review results are reviewed and approved by management prior to release. Test data and accounts are removed completely before the application is placed into a production state. Organizations remove all custom application accounts, user IDs, and passwords before applications go from development to production or are released to customers. Rules for the transfer of software from development to operational status are defined and documented. Development and operational software run on different systems or computer processors and in different domains or directories. Compilers, editors, and other development tools or system utilities are not accessible from operational systems when not required. The test system environment emulates the operational system environment as closely as possible. Users use different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error. Covered information is not copied into the test system environment.

Question Requirement: 06188.09bNYDOHSystem.10 / 2160.0

Change Count: 1

Field	Content
RequirementStatement	The organization uses the following CMS hierarchy for implementing security configuration guidelines is used when an HHS-specific minimum security configuration does not exist, and to resolve configuration conflicts among multiple security guidelines: USGCB; NIST NCP; Tier IV, then Tier III, Tier II, and Tier I, in descending order; Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG); National Security Agency (NSA) STIGs; Iif formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as T, i.e., the Center for Internet Security [(CIS]), checklists;. In situations where no guidance exists, coordinate with CMS for guidance. CMS collaborates within CMS and the HHS Cybersecurity Program, and other organizations through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to: (a) Eestablish baseline configurations and communicate industry and vendor best practices; and (b) Ee nsure deployed configurations are supported for security updates; and. All deviations from existing USGCB, NCP, DISA and/or NSA configurations are documented.

Question Requirement: 06181.09bNYDOHSystem.10 / 2153.0

Change Count: 3

Field	Content
RequirementStatement	The organization retains records of configuration-controlled changes to the information system for a minimum of three [3] years after the change.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization retains records of configuration-controlled changes to the information system for a minimum of three [3) years after the change.
IllustrativeProcedureMeasured	For example, measures indicate the number of records retained for configuration-controlled changes within the information system. Review applicable dates to determine retention period of no less than three [3) years.

Question Requirement: 0614.06h2Organizational.12 / 0611.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the periodicity of technical compliance checks as well as the amount of non-compliance issues identified per review period. A further measure could indicate the number of unqualified technical specialists performing technical compliance checks, as a percentage of all compliance checks . Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to measure the effectiveness of the implemented controls and to confirm whether technical compliance checks are performed by an experienced specialist with the assistance of industry standard automated tools, which generate a technical report for subsequent interpretation, at least annually, but more frequently where needed, based on risk as part of an official risk assessment process.

Question Requirement: 0673.10kCISOrganizational.2 / 1750.0

Change Count: 1

Field	Content
RequirementStatement	The organization builds secure images for workstations, servers and other system types from their secure configuration baselines and uses these images to build all new systems it deploys. Any existing systems that must be rebuilt (e.g., due to compromise) are rebuilt from the organizations secure images. Master images, including regular updates and exceptions, are formally managed by the organization''s change management processes to ensure that only authorized changes are possible.

Question Requirement: 0659.06hCISOrganizational.4 / 1906.0

Change Count: 1

Field	Content
RequirementStatement	The organization utilizes an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization''s technology systems, including those located onsite or at a remote service provider and update the organization''s sensitive information inventory.

Question Requirement: 0419.01yFTIOrganizational.4 / 0291.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of assets (e.g., software, and end-point equipment) that are owned and managed in accordance with the organization's policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and verify that the organization retains ownership and control of all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate worksites.

Question Requirement: 0418.01yFTIOrganizational.123 / 0290.0

Change Count: 1

Field	Content
RequirementStatement	When FTI is accessed at alternative worksites, such as an employee''s home or other non-traditional worksites, the alternative worksites remain subject to the same safeguard requirements as the organization''s offices and the highest level of attainable security. The organization addresses how it will meet its minimum protection standards for FTI at alternate worksites (e.g., employee''s homes or other non-traditional worksites). The organization conducts and fully documents periodic inspections of alternative worksites during the year to ensure that safeguards are adequate.

Question Requirement: 0408.01y3Organizational.12 / 0286.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, obtain the teleworking policy and confirm that the requirements stipulated in the requirement statement have been documented within the policy. Further, confirm that the policy and its requirements have been reviewed by the teleworker and understood. Further, confirm that controls are implemented which confirm the organization provides a definition of the work permitted, standard operating hours, classification of information that may be held/stored, and the internal systems and services that the teleworker is authorized to access; suitable equipment and storage furniture expressly designated for business use by authorized employees for the teleworking activities ; where the use of privately owned equipment not under the control of the organization is forbidden; suitable communication equipment, including methods for securing remote access; rules and guidance on family and visitor access to equipment and information; hardware and software support and maintenance; procedures for back-up and business continuity; a means for teleworkers to communicate with information security personnel in case of security incidents or problems; and audit and security monitoring.

Question Requirement: 0405.01y2Organizational.2 / 0282.0

Change Count: 1

Field	Content
RequirementStatement	Teleworking activities are formally managed/controlled, and only authorized if suitable security arrangements and security controls that comply with relevant security policies and organizational requirements are in place. Communications security requirements address the: need for remote access to the organization''s internal systems; sensitivity of information that will be accessed and that will be accessed and pass over the communication link; and sensitivity of the internal system. The use of home networks and requirements/restrictions on the configuration of wireless network services including encryption (AES WPA2 at a minimum) are addressed with respect to teleworking arrangements. Antivirus protection with respect to teleworking arrangements is addressed. Operating system patching with respect to teleworking arrangements is addressed. Application patching with respect to teleworking arrangements is addressed. Firewall requirements consistent with corporate policy are addressed with respect to teleworking arrangements. Revocation of authority and access rights with respect to teleworking arrangements is addressed. The return of equipment when the teleworking activities are terminated is addressed. Verifiable unique IDs are required for all teleworkers accessing the organization''s network via a remote connection. The connection between the organization and the teleworker''s location is secured via an encrypted channel. The organization maintains ownership over the assets used by teleworkers in order to achieve the requirements of this control.

Question Requirement: 0428.01x2Organizational.8 / 0276.0

Change Count: 1

Field	Content
RequirementStatement	All mobile devices permitted for use allow for remote wipe by the company''s corporate IT or have all company-provided data wiped by the company''s corporate IT.

Question Requirement: 0426.01x2Organizational.8 / 0274.0

Change Count: 1

Field	Content
RequirementStatement	A centralized, mobile device management solution is deployed to all mobile devices permitted to store, transmit, or process organizational and/or customer data. The mobile device management solution allows the following: Remote wipe by the company''s corporate IT or have all company-provided data wiped by the company''s corporate IT; Prohibition on the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) enforced through detective and preventative controls on the device; Mobile devices connecting to corporate networks, or storing and accessing company information, will allow for remote software version/patch validation. All mobile devices: have the latest available security-related patches installed upon general release by the device manufacturer or carrier; and allow authorized IT personnel to perform these updates remotely.

Question Requirement: 0320.09u2Organizational.3 / 1074.0

Change Count: 1

Field	Content
RequirementStatement	Organizations protect information media being transported between sites through the use of: reliable transport or couriers that can be tracked; a list of authorized couriers agreed upon with management; checking/verification of identification of couriers; and packaging sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers'' specifications (e.g., for software), such as by protecting against any environmental factors that may reduce the media''s restoration effectiveness such as exposure to heat, moisture, or electromagnetic fields.

Question Requirement: 0308.09q3Organizational.1 / 1027.0

Change Count: 1

Field	Content
RequirementStatement	Inventory and disposition records for information system media are maintained to ensure control and accountability of the organization''s information. Inventory and disposition of media-related records contain sufficient information to reconstruct the data in the event of a breach, including, at a minimum: the name of media recipient; the signature of media recipient; the date/time media is received; the media control number and contents; the movement or routing information; and if disposed of, the date, time, and method of destruction.

Question Requirement: 0208.09j2Organizational.7 / 0881.0

Change Count: 3

Field	Content
RequirementStatement	User functionality (including user interface services [(e.g., Web services]) is separated from information system management (e.g., database management systems) functionality.
IllustrativeProcedureImplemented	For example, examine evidence to confirm user functionality is separated from information system management activities. Select a sample of systems and review the users associated access rights to confirm that separation of user, (including user interface services [(e.g., Web services]), and management (e.g., database management systems) functionality is implemented. For example, the separation of user functionality from information system management functionality is either physical or logical. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of systems (desktops, applications, laptops, servers, BYOD etc.) where logical and physical access controls have been implemented to ensure that user functionality is separated from information system management activities, along with the percentage of non-compliant systems compared to compliant systems, where the separation can be bypassed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that user functionality, (including user interface services [(e.g., Web services]), is separated from information system management (e.g., database management systems) functionality.

Question Requirement: 02191.09jNYDOHOrganizational.2 / 2163.0

Change Count: 3

Field	Content
RequirementStatement	Malicious code scanning software on servers (to include databases and applications) is configured to perform critical system file scans no less often than once every twelve [12] hours and full system scans no less often than once every seventy-two [72] hours.

IllustrativeProcedureImplemented	For example, examine evidence to confirm malicious code scanning software on servers (to include databases and applications) is configured to perform critical system file scans no less often than once every twelve [12] hours and full system scans no less often than once every seventy-two [72] hours.
IllustrativeProcedureMeasured	For example, measures indicate the number of servers configured to perform malicious code scanning as a percentage of all application servers. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and confirm that malicious code scanning software is employed on servers (to include databases and applications) to perform critical system file scans no less often than once every twelve [12] hours and full system scans no less often than once every seventy-two [72] hours.

Question Requirement: 02.09jFTIOrganizational.4 / 2597.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0232.09jCISOrganizational.13 / 0887.0

Change Count: 2

Field	Content
RequirementStatement	The organization enables anti-exploitation features, (e.g., Data Execution Prevention [(DEP]), Windows Defender Exploit Guard [(WDEG]), Enhanced Mitigation Experience Toolkit [(EMET],), and Address Space Layout Randomization [(ASLR]), in its operating systems and applies anti-exploitation protections to a broader set of applications and executables by deploying additional capabilities, such as the Enhanced Migration Experience Toolkit. The anti-exploitation protection requirements are fully assessed by the organization prior to implementation due to potential difficulties (compatibility issues, etc.).
IllustrativeProcedureMeasured	For example, measures indicate the number of systems enabled with anti-exploitation features, (e.g., DEP, WDEG, EMET, or ASLR) and number of applications/executables with additional capabilities (e.g.,, such as the Enhanced Migration Experience Toolkit), as a percentage of all systems and applications. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm whether the organization enables anti-exploitation features (e.g., Data Execution Prevention [such as DEP] and Address Space Layout Randomization [ASLR]) in its operating systems, and applies anti-exploitation protections to a broader set of applications and executables by deploying additional capabilities, such as the Enhanced Migration Experience ToolkitEMET. These requirements are assessed by the organization prior to implementation due to potential difficulties (compatibility issues, etc.).

Question Requirement: 01.03aISO31000Organizational.3 / 2828.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO31000Organizational.3 / 2828.0

Question Requirement: 01.03aISO31000Organizational.2 / 2827.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO31000Organizational.2 / 2827.0

Question Requirement: 01.03aISO31000Organizational.1 / 2826.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO31000Organizational.1 / 2826.0

Question Requirement: 01.03aISO23894Organizational.13 / 2810.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO23894Organizational.13 / 2810.0

Question Requirement: 01.03aISO23894Organizational.12 / 2809.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO23894Organizational.12 / 2809.0

Question Requirement: 01.03aISO23894Organizational.25 / 2790.0

Change Count: 0

Field	Content
New Question Requirement	01.03aISO23894Organizational.25 / 2790.0

Question Requirement: 01.00aNIST80053Organizational.45 / 2783.0

Change Count: 0

Field	Content
New Question Requirement	01.00aNIST80053Organizational.45 / 2783.0

Question Requirement: 01.00aNIST80053Organizational.46 / 2776.0

Change Count: 0

Field	Content
New Question Requirement	01.00aNIST80053Organizational.46 / 2776.0

Question Requirement: 01.05bNIST80053Organizational.2 / 2775.0

Change Count: 0

Field	Content
New Question Requirement	01.05bNIST80053Organizational.2 / 2775.0

Question Requirement: 01.00aNIST80053Organizational.39 / 2640.0

Change Count: 1

Field	Content
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles an organization-defined personally identifiable information processing and transparency policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance, and procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls. The organization ensures the personally identifiable information processing and transparency policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The organization designates an organization-defined official to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures. The organization reviews and updates the current personally identifiable information processing and transparency policies at least annually or whenever a significant change occurs, and personally identifiable information processing and transparency procedures at least annually or whenever a significant change occurs.

Question Requirement: 01124.05hNYDOHOrganizational.3 / 2097.0

Change Count: 3

Field	Content
RequirementStatement	The organization provides the results of the security and privacy control assessment within thirty [30] days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, updating system security documentation where necessary to reflect any changes to the system.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization provides the results of the security and privacy control assessment within thirty [30] days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, updating system security documentation where necessary to reflect any changes to the system.
IllustrativeProcedureMeasured	For example, measures indicate the organization provides the results of the security and privacy control assessment within thirty [30] days after its completion, in writing, to the Business Owner responsible for the system and personnel responsible for reviewing the assessment documentation, updating system security documentation where necessary to reflect any changes to the system.

Question Requirement: 01123.05hNYDOHOrganizational.2 / 2096.0

Change Count: 3

Field	Content
RequirementStatement	The organization assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every three hundred sixty-five [365] days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standards to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every three hundred sixty-five [365] days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

IllustrativeProcedureMeasured	For example, measures indicate the organization assesses the security and privacy controls in the information system and its environment of operation, as defined in implementation standards, within every three hundred sixty-five [365] days in accordance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements (CMSR) Standard to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

Question Requirement: 0109.02d1Organizational.4 / 0328.0

Change Count: 1

Field	Content
RequirementStatement	Employees, contractors, and third-party users are: properly briefed on their information security roles and responsibilities prior to being granted access to covered and/or confidential information or information systems; provided with guidelines to state security expectations of their role within the organization; motivated and comply with the security policies of the organization; achieve a level of awareness on security relevant to their roles and responsibilities within the organization; conform to the terms and conditions of employment, which includes the organization''s information security policy and appropriate methods of working; and continue to have the skills and qualifications appropriate to their roles and responsibilities.

Question Requirement: 0151.02c1Organizational.23 / 0316.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization''s assets associated with information systems and services. The organization develops and documents access agreements for organizational systems. Privileges are not granted until the terms and conditions have been satisfied and agreements have been signed.

Question Requirement: 0104.02a1Organizational.12 / 0297.0

Change Count: 1

Field	Content
RequirementStatement	Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization''s information security policies; protecting assets from unauthorized access, disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.

Question Requirement: 01.00aFTIOrganizational.3 / 2655.0

Change Count: 1

Field	Content
DITA	Sampling

Question Requirement: 0174.05c2Organizational.12345 / 0469.0

Change Count: 1

Field	Content
RequirementStatement	The organization identifies, by name or position, non-professional or professional security contacts in each major organizational area or business unit. The organization clearly defines the roles of each security contact including the administration and implementation of the organization''s security programs, responsibilities of each security contact including the administration and implementation of the organization''s security programs, and authority of each security contact including the administration and implementation of the organization''s security programs. Each security contact annually documents compliance related to identified legal requirements, reports to the organization''s single point of contact for security, provides evaluations on the effectiveness of the policies and procedures implemented in addressing risk, provides evaluations of service provider arrangements, provides significant incidents and the response, and provides recommendations for material changes to the security programs for which they are responsible. The organization's single point of contact for security matters provides supplemental security awareness and training. Security contacts are responsible for reviewing reports related to the security organization, network, systems and programs implemented, and formally approving any material changes to these items prior to implementation.

Question Requirement: 0179.05h2Organizational.3 / 0497.0

Change Count: 1

Field	Content
RequirementStatement	If an independent review identifies that the organization''s approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document, management takes corrective actions.

Question Requirement: 0177.05h2Organizational.1 / 0495.0

Change Count: 1

Field	Content
RequirementStatement	An independent review of the organization''s information security management program is initiated by management to ensure the continuing suitability, adequacy, and effectiveness of the organization''s approach to managing information security and privacy. The tests and methods used are sufficient to validate the effectiveness of the security plan. Independent security program reviews: include an assessment of the organizations adherence to its security plan; address the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing); carefully control information security tests to limit the risks to confidentiality, integrity, and system availability; are carried out by individuals independent of the area under review (e.g., the internal audit function, an independent manager or a third-party organization specializing in such reviews); are carried out by individuals who have the appropriate skills and experience; and include notification requirements to confirm whom to inform within the organization about the timing and nature of the assessment.

Question Requirement: 0187.07b2Organizational.5 / 0649.0

Change Count: 1

Field	Content
RequirementStatement	The information owner(s) is responsible for: creating an initial information classification, including assigning classification levels to all data; approving decisions regarding controls, access privileges of users, and ongoing decisions regarding information management; ensuring the information will be regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities, or changes in the environment; performing on an organizationally pre-defined timeframe reclassification based upon business impact analysis, changing business priorities and/or new laws, regulations, and security standards; and following the organization''s archive document retention rules regarding proper disposition of all information assets.

Question Requirement: 0186.07b2Organizational.3 / 0648.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures that appropriate software licensing agreements for software used by the organization''s employees are in place, and that the organization is in compliance with those agreements.

Question Requirement: 0185.07b2Organizational.24 / 0647.0

Change Count: 1

Field	Content
RequirementStatement	The organization allocates asset responsibility based on a business process, a defined set of activities, an application, or a defined set of data. All information and assets associated with information processing systems are assigned responsibility to a designated part of the organization. All information has an information owner or owners (e.g., designated individuals responsible) established within the organization''s lines of business.

Question Requirement: 0138.02b3Organizational.3 / 0301.0

Change Count: 1

Field	Content
RequirementStatement	Verification checks consider all relevant: privacy legislation; protection of covered data legislation; and employment-based legislation. Where permitted and appropriate, verification checks: include availability of satisfactory character references (e.g., one business and one personal); include a completeness and accuracy check of the applicant''s curriculum vitae; include confirmation of claimed academic and professional qualifications; include independent identity check (passport or similar document); and require all applicants to complete an I-9 form to verify that they are eligible to work in the United States. Verification checks are completed prior to granting access to covered and/or confidential information.

Question Requirement: 0130.05b3Organizational.1 / 0460.0

Change Count: 1

Field	Content
RequirementStatement	The organization convenes an internal meeting for the organization''s security single point of contact and the organizational area/business unit security contacts on a monthly or near-to-monthly basis.

Question Requirement: 0124.05a3Organizational.1 / 0449.0

Change Count: 1

Field	Content
RequirementStatement	The organization: formally creates a dedicated security management forum; publishes the dedicated security management forum''s member list; and publishes the dedicated security management forum''s charter.

Question Requirement: 0116.04b3Organizational.1 / 0438.0

Change Count: 1

Field	Content
RequirementStatement	Management''s risk profile review addresses: the changing nature of the organization''s operations and thus risk profile and risk management needs; the changes made to the IT infrastructure of the organization, along with the changes these bring to the organization''s risk profile; the changes identified in the external environment that similarly impact the organization'' s risk profile; the latest controls, compliance and assurance requirements from arrangements of national bodies and of new legislation or regulation; the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; the results of legal cases tested in courts that thereby establish or cancel precedents and established practices; and the challenges and issues regarding the policy, as expressed to the organization by its staff, customers, and their partners and care givers, researchers, and governments, e.g., privacy commissioners.

Question Requirement: 01279.02dDGFOrganizational.2 / 2252.0

Change Count: 1

Field	Content
RequirementStatement	Data Custodians ensure that the strategic vision for Data Governance satisfies short-term, mid-term, and long-term needs of the custodian''s domain/application/business segment, as applicable.

Question Requirement: 01113.00aNYCRR500Organizational.2 / 0009.0

Change Count: 1

Field	Content
RequirementStatement	All documentation and information relevant to the organization'' s cybersecurity program are made available to the financial services superintendent of New York upon request.

Question Requirement: 01112.05bNYDOHOrganizational.2 / 2085.0

Change Count: 2

Field	Content
RequirementStatement	The organization updates the security plan: minimally every three (3) years, to address current conditions; whenever there are significant changes to the information system/environment of operation that affect security; whenever problems are identified during plan implementation or security control assessments; whenever the data sensitivity level increases; after a serious security violation due to changes in the threat environment; and before the previous security authorization expires.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization updates the security plan, (i) minimally every three (3) years, to address current conditions (ii) or whenever there are significant changes to the information system/environment of operation that affect security; (iii) problems are identified during plan implementation or security control assessments; (iv) the data sensitivity level increases; (v) after a serious security violation due to changes in the threat environment; or (vi) before the previous security authorization expires.

Question Requirement: 0111.02d2Organizational.2 / 0330.0

Change Count: 1

Field	Content
RequirementStatement	Non-employees are provided the organization''s data privacy and data security policy prior to accessing system resources and data.

Question Requirement: 0110.02d2Organizational.1 / 0329.0

Change Count: 1

Field	Content
RequirementStatement	The organization assigns an individual or team to manage information security responsibilities of employees, contractors, and third-party users.

Question Requirement: 0150.02c2Organizational.3 / 0315.0

Change Count: 1

Field	Content
RequirementStatement	The terms and conditions of employment reflect the organization''s security policy. Terms and conditions of employment: clarify and state that all employees, contractors, and third-party users who are given access to covered information sign a confidentiality or non-disclosure agreement prior to being given access to information assets; clarify and state the employee''s, contractor''s, and any other user''s legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation); clarify and state responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor, or third-party user; clarify and state responsibilities of the employee, contractor, or third-party user for the handling of information received from other companies or external parties; clarify and state responsibilities of the organization for the handling of covered information, including covered information created as a result of, or in the course of, employment with the organization; clarify and state responsibilities that are extended outside the organization''s premises and outside normal working hours (e.g., in the case of home-working); clarify and state actions to be taken if the employee, contractor, or third-party user disregards the organization''s security requirements; and ensure that conditions relating to security policy survive the completion of the employment in perpetuity.

Question Requirement: 0115.04b2Organizational.123 / 0437.0

Change Count: 1

Field	Content
RequirementStatement	The information security policy documents have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. Policies are reviewed no less than every three hundred sixty five (365) days or if significant changes occur in the operating or business environment, updated/improved based on specific feedback (e.g., prior reviews, incidents and preventative/corrective actions), and approved by an appropriate level of management. The input to the management review includes information on: feedback from interested parties; results of independent reviews; status of preventive and corrective actions; results of previous management reviews; process performance and information security policy compliance; changes that could affect the organization''s approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment; trends related to threats and vulnerabilities; reported information security incidents; and recommendations provided by relevant authorities.

Question Requirement: 0162.04b2Organizational.2 / 0436.0

Change Count: 1

Field	Content
RequirementStatement	A process is defined, and implemented for individuals to make complaints concerning the information security policies and procedures or the organization''s compliance with the policies and procedures. All complaints and requests for changes are documented, along with their disposition, if any.

Question Requirement: 0113.04a2Organizational.1 / 0431.2

Change Count: 1

Field	Content
RequirementStatement	As applicable to the focus of a security policy particular document, security policies contain: the organization''s mission, vision, values, objectives, activities, and purpose, including the organization''s place in critical infrastructure; a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; the need for information security; the goals of information security; the organization’s compliance scope; legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination; a definition of general and specific responsibilities for information security management, including reporting information security incidents; references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with); a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including but not limited to CSF control objectives such as: (a) compliance with legislative, regulatory, and contractual requirements; (b) security education, training, and awareness requirements for the workforce, including researchers and research participants; (c) incident response and business continuity management; (d) consequences of information security policy violations; (e) continuous monitoring; (f) designating and maintaining an appropriately resourced and technically experienced information security team; (g) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (h) coordination among organizational entities. As applicable to the focus of a security policy particular document, security policies also prescribe the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls.

Question Requirement: 0183.07b1Organizational.1 / 0645.0

Change Count: 1

Field	Content
RequirementStatement	All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner''s contact information; and purpose (e.g., through labeling, coding, and/or inventory).

Question Requirement: 01108.02fEHNACOrganizational.1 / 0365.0

Change Count: 1

Field	Content
RequirementStatement	The organization''s formal sanctions process includes failure to comply with established privacy policies and procedures.

Question Requirement: 01101.00aFFIECISOrganizational.1 / 0005.0

Change Count: 3

Field	Content
RequirementStatement	Metrics are implemented by management that demonstrate the extent to which the information security management program is implemented and whether the program is effective. The metrics are timely, comprehensive, and actionable to improve the ISMP''s effectiveness and efficiency.
IllustrativeProcedureImplemented	For example, examine evidence to confirm that metrics have been implemented by management. Further, examine evidence to confirm that metrics are timely, comprehensive, and actionable to improve the ISMP''s effectiveness and efficiency.
IllustrativeProcedureMeasured	For example, measures indicate the number of metrics that have been implemented by management. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that metrics are timely, comprehensive, and actionable to improve the ISMP''s effectiveness and efficiency.

Changes for Authoritative Source Document - v11.1.0 to v11.2.0

Authoritative Source Document: NIST AI RMF 1.0

Change Count: 0

Field	Content
New Authoritative Source Document	NIST AI RMF 1.0

Authoritative Source Document: ISO 31000:2018

Change Count: 0

Field	Content
New Authoritative Source Document	ISO 31000:2018

Authoritative Source Document: ISO/IEC 23894:2023

Change Count: 0

Field	Content
New Authoritative Source Document	ISO/IEC 23894:2023

Authoritative Source Document: FTC Red Flags Rule (16 CFR 681)

Change Count: 0

Field	Content
New Authoritative Source Document	FTC Red Flags Rule (16 CFR 681)

Authoritative Source Document: State of Nevada Security and Privacy of Personal Information (NRS 603A)

Change Count: 0

Field	Content
New Authoritative Source Document	State of Nevada Security and Privacy of Personal Information (NRS 603A)

Authoritative Source Document: 23 NYCRR 500

Change Count: 0

Field	Content
New Authoritative Source Document	23 NYCRR 500

Authoritative Source Document: NY OHIP Moderate-Plus Security Baseline v5.0

Change Count: 0

Field	Content
New Authoritative Source Document	NY OHIP Moderate-Plus Security Baseline v5.0

Authoritative Source Document: ISO/IEC 27002:2022

Change Count: 0

Field	Content
New Authoritative Source Document	ISO/IEC 27002:2022

Authoritative Source Document: Veterans Affairs Cybersecurity Program Directive 6500

Change Count: 0

Field	Content
New Authoritative Source Document	Veterans Affairs Cybersecurity Program Directive 6500

Authoritative Source Document: ISO/IEC 27001:2022

Change Count: 0

Field	Content
New Authoritative Source Document	ISO/IEC 27001:2022

Authoritative Source Document: Ontario Personal Health Information Protection Act

Change Count: 0

Field	Content
New Authoritative Source Document	Ontario Personal Health Information Protection Act

Changes for Factor Type - v11.1.0 to v11.2.0

Factor Type: Compliance - Ontario Personal Health Information Protection Act

Change Count: 0

Field	Content
New Factor Type	Compliance - Ontario Personal Health Information Protection Act

Changes for Factor - v11.1.0 to v11.2.0

Factor: General - US Healthcare Entity Type - Not a US healthcare entity

Change Count: 1

Field	Content
Selection	Non-Ht a US healthcare entity

Factor: General - US Healthcare Entity Type - US Healthcare - Other

Change Count: 1

Field	Content
Selection	US Healthcare - Other

Factor: General - US Healthcare Entity Type - US Healthcare - Covered Entity

Change Count: 1

Field	Content
Selection	US Healthcare - Covered Entity

Factor: General - US Healthcare Entity Type - US Healthcare - Business Associate

Change Count: 1

Field	Content
Selection	US Healthcare - Business Associate

Factor: Compliance - Ontario Personal Health Information Protection Act - Consumer Electronic Service Provider

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Consumer Electronic Service Provider

Factor: Compliance - Ontario Personal Health Information Protection Act - Prescribed Organization

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Prescribed Organization

Factor: Compliance - Ontario Personal Health Information Protection Act - Researcher

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Researcher

Factor: Compliance - Ontario Personal Health Information Protection Act - Agent

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Agent

Factor: Compliance - Ontario Personal Health Information Protection Act - Health Data Institute

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Health Data Institute

Factor: Compliance - Ontario Personal Health Information Protection Act - Health Information Custodian

Change Count: 0

Field	Content
New Factor	Compliance - Ontario Personal Health Information Protection Act - Health Information Custodian

Factor: Compliance - HITRUST Reg: Compliance Factors - ISO 31000:2018

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - ISO 31000:2018

Factor: Compliance - HITRUST Reg: Compliance Factors - Artificial Intelligence Risk Management

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - Artificial Intelligence Risk Management

Factor: Compliance - HITRUST Reg: Compliance Factors - NY OHIP Moderate-plus Security Baselines v5.0

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - NY OHIP Moderate-plus Security Baselines v5.0

Factor: Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27002:2022

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27002:2022

Factor: Compliance - HITRUST Reg: Compliance Factors - VA Directive 6500

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - VA Directive 6500

Factor: Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27001:2022

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27001:2022