v11.3.0 Summary of Changes

Difference Comparison for CSF v11.2.0 to v11.3.0

HITRUST

Table of Contents

Changes for Library Version - v11.2.0 to v11.3.0

Library Version: v11.3.0

Change Count: 1

Field	Content
Name	v11.23.0

Changes for Question Requirement - v11.2.0 to v11.3.0

Question Requirement: 11.01qNIST80053System.4 / 2975.0

Change Count: 0

Field	Content
New Question Requirement	11.01qNIST80053System.4 / 2975.0

Question Requirement: 11.01qNIST80053System.3 / 2974.0

Change Count: 0

Field	Content
New Question Requirement	11.01qNIST80053System.3 / 2974.0

Question Requirement: 09.09x2Organizational.4 / 1084.0

Change Count: 0

Field	Content
New Question Requirement	09.09x2Organizational.4 / 1084.0

Question Requirement: 09.09yOWASPOrganizational.1 / 2973.0

Change Count: 0

Field	Content
New Question Requirement	09.09yOWASPOrganizational.1 / 2973.0

Question Requirement: 06.10mATLASOrganizational.9 / 2972.0

Change Count: 0

Field	Content
New Question Requirement	06.10mATLASOrganizational.9 / 2972.0

Question Requirement: 12.09abOWASPSystem.2 / 2971.0

Change Count: 0

Field	Content
New Question Requirement	12.09abOWASPSystem.2 / 2971.0

Question Requirement: 14.05kOWASPOrganizational.1 / 2970.0

Change Count: 0

Field	Content
New Question Requirement	14.05kOWASPOrganizational.1 / 2970.0

Question Requirement: 11.01vOWASPSystem.1 / 2969.0

Change Count: 0

Field	Content
New Question Requirement	11.01vOWASPSystem.1 / 2969.0

Question Requirement: 19.13jOWASPOrganizational.4 / 2968.0

Change Count: 0

Field	Content
New Question Requirement	19.13jOWASPOrganizational.4 / 2968.0

Question Requirement: 19.13kOWASPOrganizational.2 / 2967.0

Change Count: 0

Field	Content
New Question Requirement	19.13kOWASPOrganizational.2 / 2967.0

Question Requirement: 19.13jOWASPOrganizational.5 / 2966.0

Change Count: 0

Field	Content
New Question Requirement	19.13jOWASPOrganizational.5 / 2966.0

Question Requirement: 07.10mOWASPOrganizational.3 / 2965.0

Change Count: 0

Field	Content
New Question Requirement	07.10mOWASPOrganizational.3 / 2965.0

Question Requirement: 10.01dNIST800172System.1 / 2932.0

Change Count: 0

Field	Content
New Question Requirement	10.01dNIST800172System.1 / 2932.0

Question Requirement: 11.01jNIST800172Organizational.1 / 2931.0

Change Count: 0

Field	Content
New Question Requirement	11.01jNIST800172Organizational.1 / 2931.0

Question Requirement: 07.07aNIST800172Organizational.1 / 2930.0

Change Count: 0

Field	Content
New Question Requirement	07.07aNIST800172Organizational.1 / 2930.0

Question Requirement: 06.10kNIST800172Organizational.1 / 2929.0

Change Count: 0

Field	Content
New Question Requirement	06.10kNIST800172Organizational.1 / 2929.0

Question Requirement: 13.02eNIST800172Organizational.2 / 2928.0

Change Count: 0

Field	Content
New Question Requirement	13.02eNIST800172Organizational.2 / 2928.0

Question Requirement: 13.02eNIST800172Organizational.1 / 2927.0

Change Count: 0

Field	Content
New Question Requirement	13.02eNIST800172Organizational.1 / 2927.0

Question Requirement: 04.01xNIST800172Organizational.1 / 2926.0

Change Count: 0

Field	Content
New Question Requirement	04.01xNIST800172Organizational.1 / 2926.0

Question Requirement: 11.01vNIST800172System.1 / 2925.0

Change Count: 0

Field	Content
New Question Requirement	11.01vNIST800172System.1 / 2925.0

Question Requirement: 10.01dCISSystem.1 / 2924.0

Change Count: 0

Field	Content
New Question Requirement	10.01dCISSystem.1 / 2924.0

Question Requirement: 15.11aNYCRR500Organizational.2 / 2923.0

Change Count: 0

Field	Content
New Question Requirement	15.11aNYCRR500Organizational.2 / 2923.0

Question Requirement: 15.11aPDPAOrganizational.2 / 2922.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPDPAOrganizational.2 / 2922.0

Question Requirement: 19.13mPDPAOrganizational.2 / 2921.0

Change Count: 0

Field	Content
New Question Requirement	19.13mPDPAOrganizational.2 / 2921.0

Question Requirement: 15.11aPDPAOrganizational.3 / 2920.0

Change Count: 0

Field	Content
New Question Requirement	15.11aPDPAOrganizational.3 / 2920.0

Question Requirement: 19.13nPDPAOrganizational.1 / 2919.0

Change Count: 0

Field	Content
New Question Requirement	19.13nPDPAOrganizational.1 / 2919.0

Question Requirement: 11.01lHICPOrganizational.2 / 2918.0

Change Count: 0

Field	Content
New Question Requirement	11.01lHICPOrganizational.2 / 2918.0

Question Requirement: 13.02eCISOrganizational.2 / 2917.0

Change Count: 0

Field	Content
New Question Requirement	13.02eCISOrganizational.2 / 2917.0

Question Requirement: 07.10mFFIECCATOrganizational.7 / 2884.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.7 / 2884.0

Question Requirement: 07.10mFFIECCATOrganizational.6 / 2883.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.6 / 2883.0

Question Requirement: 17.03dFFIECCATOrganizational.3 / 2882.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.3 / 2882.0

Question Requirement: 14.09tFFIECCATOrganizational.2 / 2881.0

Change Count: 0

Field	Content
New Question Requirement	14.09tFFIECCATOrganizational.2 / 2881.0

Question Requirement: 12.09abFFIECCATSystem.9 / 2880.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.9 / 2880.0

Question Requirement: 06.10hCISSystem.4 / 2879.0

Change Count: 0

Field	Content
New Question Requirement	06.10hCISSystem.4 / 2879.0

Question Requirement: 07.10mCISOrganizational.12 / 2878.0

Change Count: 0

Field	Content
New Question Requirement	07.10mCISOrganizational.12 / 2878.0

Question Requirement: 06.10hCISSystem.3 / 2877.0

Change Count: 0

Field	Content
New Question Requirement	06.10hCISSystem.3 / 2877.0

Question Requirement: 19.06dATLASOrganizational.2 / 2876.0

Change Count: 0

Field	Content
New Question Requirement	19.06dATLASOrganizational.2 / 2876.0

Question Requirement: 07.10bATLASSystem.3 / 2875.0

Change Count: 0

Field	Content
New Question Requirement	07.10bATLASSystem.3 / 2875.0

Question Requirement: 07.10mATLASOrganizational.8 / 2874.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.8 / 2874.0

Question Requirement: 07.10mATLASOrganizational.5 / 2873.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.5 / 2873.0

Question Requirement: 07.10bATLASSystem.2 / 2872.0

Change Count: 0

Field	Content
New Question Requirement	07.10bATLASSystem.2 / 2872.0

Question Requirement: 07.10mATLASOrganizational.4 / 2871.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.4 / 2871.0

Question Requirement: 07.10mATLASOrganizational.3 / 2870.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.3 / 2870.0

Question Requirement: 07.10mATLASOrganizational.2 / 2869.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.2 / 2869.0

Question Requirement: 0962.10fPCIOrganizational.1 / 1292.0

Change Count: 2

Field	Content
RequirementStatement	When being assessed as a service provider, the organization maintainsThe organization maintains and updates at least annually a documented description of the cryptographic architecture that includes: details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date; description of the key usage for each key; and inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management; active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use; and a documented strategy to respond to anticipated changes in cryptographic vulnerabilities.
IllustrativeProcedureMeasured	For example, measures indicate the number of components in the organization's cryptographic architecture that have/have not been formally documented as stipulated in the requirement statement, as a percentage of its cryptographic architecture. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, when being assessed as a service provider, the organization maintains the organization maintains and updates at least annually a documented description of the cryptographic architecture that includes: (i) details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date (ii) description of the key usage for each key (iii) inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management.

Question Requirement: 18.09pNIST80053Organizational.3 / 1022.0

Change Count: 1

Field	Content
BaselineUniqueId	18141.09pFTINIST80053Organizational.113

Question Requirement: 18.09pNIST80053Organizational.2 / 1021.0

Change Count: 1

Field	Content
BaselineUniqueId	18140.09pFTINIST80053Organizational.1012

Question Requirement: 17.10aNIST80053Organizational.4 / 1260.0

Change Count: 1

Field	Content
BaselineUniqueId	17111.10aFTINIST80053Organizational.54

Question Requirement: 12.09aeNIST80053System.2 / 1212.0

Change Count: 1

Field	Content
BaselineUniqueId	1267.09aeFTINIST80053System.12

Question Requirement: 01.02cNIST80053Organizational.2 / 0323.0

Change Count: 1

Field	Content
BaselineUniqueId	01104.02cFedRAMPNIST80053Organizational.2

Question Requirement: 11.01tCMSSystem.3 / 2477.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01tFedRAMPCMSSystem.23

Question Requirement: 11.01tFedRAMPSystem.1 / 2476.0

Change Count: 1

Field	Content
RequirementStatement	The information system terminates the network connection associated with a communications session at the end of the session or after no longer than ten (10) minutes of inactivity for privileged sessions and no longer than fifteen (15) minutes of inactivity for user sessions.

Question Requirement: 11.01qFedRAMPSystem.3 / 2382.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of information identifiers configured for use and the number of information identifiers authorized for use in number and as a percentage. 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 configured to meet requirements as stipulated.

Question Requirement: 11.01qNIST80053System.6 / 0222.0

Change Count: 1

Field	Content
BaselineUniqueId	11221.01qFedRAMPNIST80053System.36

Question Requirement: 17129.05gFedRAMPOrganizational.2 / 0493.1

Change Count: 3

Field	Content
BaselineUniqueId	17129.05gFedRAMPOrganizational.12
CrossVersionId	0493.01
RequirementStatement	The organization: receives information system security alerts, advisories, and directives on an ongoing basis (for example, from the U.S. Computer Emergency Readiness Team); generates andsecurity alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; 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: 01.05bNIST80053Organizational.3 / 0463.0

Change Count: 1

Field	Content
BaselineUniqueId	01106.05bFedRAMPNIST80053Organizational.13

Question Requirement: 16.09hNIST80053System.4 / 0860.0

Change Count: 1

Field	Content
BaselineUniqueId	1691.09hFedRAMPNIST80053System.14

Question Requirement: 1455.05kCSPOrganizational.4 / 0532.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of customerthird-party contracts and confirm that a review is performed annually to ensure compliance with information security and confidentiality, access control, service definitions, and service-level agreements included in third-party contracts. Examine the evidence of the review and confirm that it was appropriately reviewed by management.

Question Requirement: 07.10mNIST80053Organizational.4 / 1389.0

Change Count: 1

Field	Content
BaselineUniqueId	0769.10mCNIST80053Organizational.124

Question Requirement: 07.10mFedRAMPOrganizational.19 / 1387.0

Change Count: 1

Field	Content
BaselineUniqueId	0767.10mCISFedRAMPOrganizational.129

Question Requirement: 13.02eISO27001Organizational.2 / 0347.0

Change Count: 1

Field	Content
BaselineUniqueId	1328.02eCISO27001Organizational.92

Question Requirement: 08.01oHICPOrganizational.3 / 1885.0

Change Count: 1

Field	Content
BaselineUniqueId	0899.01oCISHICPOrganizational.43

Question Requirement: 08.01mNIST80053Organizational.3 / 1900.0

Change Count: 1

Field	Content
BaselineUniqueId	0893.01mCNIST80053Organizational.43

Question Requirement: 08.01mNIST80053Organizational.2 / 1901.0

Change Count: 1

Field	Content
BaselineUniqueId	0897.01mCNIST80053Organizational.102

Question Requirement: 08.01mHICPOrganizational.2 / 0166.0

Change Count: 1

Field	Content
BaselineUniqueId	0896.01mCISHICPOrganizational.92

Question Requirement: 12.13l3Organizational.2 / 1119.0

Change Count: 1

Field	Content
BaselineUniqueId	1211.09aa3System.4.13l3Organizational.2

Question Requirement: 12.13k3Organizational.2 / 1118.0

Change Count: 1

Field	Content
BaselineUniqueId	1210.09aa3System.3.13k3Organizational.2

Question Requirement: 13.01p2System.4 / 0195.0

Change Count: 1

Field	Content
BaselineUniqueId	1312.01p32System.34

Question Requirement: 01.02bFFIECISOrganizational.2 / 0310.0

Change Count: 1

Field	Content
BaselineUniqueId	0146.02b3FFIECISOrganizational.12

Question Requirement: 0409.01y3Organizational.3 / 0287.0

Change Count: 3

Field	Content
RequirementStatement	The organization has provided additional cyber security insurance to address the risks of teleworking.
IllustrativeProcedureImplemented	For example, examine the cyber security insurance policy and confirm that additional insurance has been purchased and that it covers risk associated with teleworking.

IllustrativeProcedureMeasured	For example, measures indicate the amount of the cyber security insurance coverage to cover evolving teleworking risks in accordance to the organization's policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and verify that additional cyber security insurance to address the risks of teleworking is provided.

Question Requirement: 18.08bNIST80053Organizational.12 / 0717.0

Change Count: 1

Field	Content
BaselineUniqueId	18146.08bNIST80053Organizational.812

Question Requirement: 18.08bNIST80053Organizational.11 / 0716.0

Change Count: 1

Field	Content
BaselineUniqueId	18145.08bNIST80053Organizational.711

Question Requirement: 19367.13ePDPAOrganizational.2 / 1816.1

Change Count: 4

Field	Content
CrossVersionId	1816.01
RequirementStatement	The organization ensures that people may subscribe to have their numbers on the Do Not Call Register or to have it removed therefrom. Withdraw of consent to specific messages may be done at any time, and must be respecteddoes not, as a condition for supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that Singapore telephone numberer any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user.
IllustrativeProcedureImplemented	For example, review a log of requests or a sample of requests for restriction/withdrawal and verify the controller provided the restriction/withdrawal. Verification is based on a comparable log of when such restrictions/withdrawals were put in place and associated internal documentation initiating the restriction for a representative sample of requestscustomers and verify the organization did not require consent for the sending of messages beyond what is reasonable to provide the goods, services, land, interest or opportunity to that customer.
IllustrativeProcedureMeasured	For example, measures indicate the number of people who have their numbers on the Do Not Call Register as percentage of all numberspercentage of messages sent to customers without consent. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the person's consent is respected.

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: 15.11aHIPAAOrganizational.6 / 2351.0

Change Count: 2

Field	Content
RequirementStatement	The organization trains all members of its workforce on the policies and procedures with respect to handling and reporting of PHI breaches in accordance with HIPAA §1604.530(b)(2).
IllustrativeProcedureImplemented	For example, examine evidence that the organization trains all members of its workforce on the policies and procedures with respect to handling and reporting of PHI breaches in accordance with HIPAA §1604.530(b)(2).

Question Requirement: 15.11aHIPAAOrganizational.10 / 2355.0

Change Count: 1

Field	Content
RequirementStatement	The organization implements policies and procedures, with respect to the handling and reporting of PHI breaches, that are designed to comply with the requirements of HIPAA §1604 .530(i).

Question Requirement: 0758.10mPCIOrganizational.6 / 1426.1

Change Count: 3

Field	Content
BaselineUniqueId	0758.10mPCIOrganizational.56
CrossVersionId	1426.01

RequirementStatement	The organization conducts regular penetration testing, no less than every 365 days per the entity's defined methodology, no less than every 365 days or after any significant infrastructure or application upgrade or change, on defined information systems or system components to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems. Penetration testing occurs from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks. This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation. For organizations assessed as a service provider, penetration testing on segmentation controls are performed at least every six months and after any changes to segmentation controls/methods. The organization also requires use of a qualified and independent penetration agent or penetration team to perform penetration testing on the information system or system components.

Question Requirement: 0757.10mPCIOrganizational.4 / 1425.0

Change Count: 1

Field	Content
RequirementStatement	The organization implements a methodology for penetration testing that: is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115); includes coverage for the entire card data environment (CDE) perimeter and critical systems; includes testing from both inside and outside the network; includes testing to validate any segmentation and scope-reduction controls; defines application-layer penetration tests to include, at a minimum, the vulnerabilities identified in PCI DSS v3.14; defines network-layer penetration tests to include components that support network functions as well as operating systems; includes review and consideration of threats and vulnerabilities experienced in the last 12 months; and specifies retention of penetration testing results and remediation activities results for at least 12 months.

Question Requirement: 0756.10mPCIOrganizational.123 / 1424.0

Change Count: 2

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 and independent 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 and independent personnel.
IllustrativeProcedureMeasured	For example, measures indicate the number of vulnerabilities identified through the performance of quarterly internal and external scans. A further metric can indicate the number of vulnerabilities that have been remediated as part of the vulnerability rescans. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization conducts quarterly internal and external scans, and rescans, as needed, by a qualified and independent entity.

Question Requirement: 10.01dSRSystem.2 / 0097.0

Change Count: 1

Field	Content
BaselineUniqueId	1037.01dPCISRSystem.2

Question Requirement: 19549.13rGDPROrganizational.1 / 1783.0

Change Count: 1

Field	Content
RequirementStatement	Processors maintain adequate records and logs of processing activities in which it engages which include at least the information detailed in GDPR Article 30(2).

Question Requirement: 19512.13pGDPROrganizational.5 / 1741.1

Change Count: 3

Field	Content
BaselineUniqueId	19512.13pGDPROrganizational.15
CrossVersionId	1741.01
RequirementStatement	The controller or their representative maintains adequate records and logs of processing activities. Records or logs of processing are in writing and, are available to supervisory authorities, and include at least the information detailed in GDPR Article 30(1).

Question Requirement: 19258.06dGDPROrganizational.4 / 0580.1

Change Count: 5

Field	Content
BaselineUniqueId	19258.06dGDPROrganizational.24
CrossVersionId	0580.01
RequirementStatement	A data protection officer is designated for a controller, processor, group of undertakings, provided the officer is accessible from each establishment, or group of multiple public authorities or bodies, taking account of their organizational structure and size, in any case where (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; OR (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law, also designates a data protection officer, who may act for such associations and other bodies representing controllers or processors. The controller or the processor requires publication of the contact details and communication of those details to the supervisory authority.
IllustrativeProcedureImplemented	For example, review relevant organizational charts to determine if the data protection officer role exists. Verify the data protection officer is referenced in relevant data privacy notices and the correct contact information is included. Note full credit is not given for this requirement if the data protection officer is replaced frequently (e.g., every 18 to 24 months), as this indicates a lack of support for the position on the part of management. Obtain relevant communications with the supervisory authority and verify the appropriate contact details have been communicated for the current data protection officer.
IllustrativeProcedureMeasured	For example, measures indicate the number of regulatory mandated positions that are not filled during a specific reporting period, e.g., on a monthly basiswhether the organization has communicated the appropriate contact details for the data protection officer. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the entity designates a data protection officer, as required, publishes the officer's contact details as specified in the organization's policies and procedure, and communicates those communicates the appropriate contact details to the supervisory authority.

Question Requirement: 02.09jNIST80053Organizational.5 / 0893.0

Change Count: 1

Field	Content
BaselineUniqueId	0223.09jFTINIST80053Organizational.35

Question Requirement: 09.09yNIST80053Organizational.3 / 1100.0

Change Count: 1

Field	Content
BaselineUniqueId	0953.09yFTINIST80053Organizational.63

Question Requirement: 01.00aCMSOrganizational.4 / 2394.0

Change Count: 1

Field	Content
BaselineUniqueId	01.00aFedRAMPCMSOrganizational.94

Question Requirement: 11.01pCISSystem.3 / 2378.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01pFedRAMPCISSystem.53

Question Requirement: 11.02iCMSOrganizational.2 / 2392.0

Change Count: 1

Field	Content
BaselineUniqueId	11.02iFedRAMPCMSOrganizational.12

Question Requirement: 11.02gCMSOrganizational.4 / 0375.0

Change Count: 1

Field	Content
BaselineUniqueId	11211.02gFedRAMPCMSOrganizational.14

Question Requirement: 14.05iNIST80053Organizational.3 / 0506.0

Change Count: 1

Field	Content
BaselineUniqueId	1465.05iFedRAMPNIST80053Organizational.13

Question Requirement: 13.07cFedRAMPOrganizational.1 / 2391.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of users who have signed acknowledgments indicating that they had read, understand, and agree to abide by the rules of behavior before access to information and the information system was authorized as a percentage of all users. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the rules of behavior were updated annually at a minimum.

Question Requirement: 18.08jFTIOrganizational.3 / 2376.0

Change Count: 1

Field	Content
BaselineUniqueId	18.08jFedRAMPTIOrganizational.23

Question Requirement: 12.09abHICPSystem.6 / 1162.0

Change Count: 1

Field	Content
BaselineUniqueId	1288.09abCISHICPSystem.136

Question Requirement: 12.09abFFIECISSystem.9 / 1166.0

Change Count: 1

Field	Content
BaselineUniqueId	1286.09abFFIECISSystem.119

Question Requirement: 12.09abNIST80053System.5 / 1165.0

Change Count: 1

Field	Content
BaselineUniqueId	1285.09abCNIST80053System.105

Question Requirement: 12.09abPCISystem.5 / 1889.0

Change Count: 1

Field	Content
BaselineUniqueId	1284.09abPCISSystem.25

Question Requirement: 11.01eNIST80053System.3 / 0104.0

Change Count: 1

Field	Content
BaselineUniqueId	11186.01eCNIST80053System.3

Question Requirement: 11.01eNIST80053System.2 / 0103.0

Change Count: 1

Field	Content
BaselineUniqueId	11185.01eCNIST80053System.32

Question Requirement: 07.10mNIST80053Organizational.6 / 1396.0

Change Count: 1

Field	Content
BaselineUniqueId	0776.10mCNIST80053Organizational.126

Question Requirement: 0773.10mCISOrganizational.13 / 1913.1

Change Count: 3

Field	Content
BaselineUniqueId	0773.10mCISOrganizational.123
CrossVersionId	1913.01
RequirementStatement	The organization conducts both authenticated and unauthenticated scans utilizesing an up-to-date Security Content Automation Protocol (SCAP)-compliant vulnerability scanning tool that looks for code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and for configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Question Requirement: 07.10mNIST80053Organizational.5 / 1391.0

Change Count: 1

Field	Content
BaselineUniqueId	0771.10mCNIST80053Organizational.125

Question Requirement: 15.11bNIST80053Organizational.3 / 1458.0

Change Count: 1

Field	Content
BaselineUniqueId	1536.11b2NIST80053Organizational.23

Question Requirement: 15.11aNIST80053Organizational.6 / 1436.0

Change Count: 1

Field	Content
BaselineUniqueId	1512.11a2NIST80053Organizational.86

Question Requirement: 16.12cDEIDOrganizational.4 / 1519.0

Change Count: 1

Field	Content
BaselineUniqueId	1607.12c2DEIDOrganizational.4

Question Requirement: 16.12cNIST80053Organizational.7 / 1515.0

Change Count: 1

Field	Content
BaselineUniqueId	1603.12c2NIST80053Organizational.87

Question Requirement: 11.01eNIST800171System.3 / 0101.0

Change Count: 1

Field	Content
BaselineUniqueId	1167.01e2NIST800171System.13

Question Requirement: 1010.01d2System.5 / 0079.0

Change Count: 1

Field	Content
RequirementStatement	Identification codes used in conjunction with passwords for electronic signatures are protected by: maintaining the uniqueness of each combined identification code and password, such that no two (2) individuals have the same combination of identification code and password; ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging); following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls; using transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report, in an immediate and urgent manner, any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Question Requirement: 11.01tCISSystem.3 / 0239.0

Change Count: 1

Field	Content
BaselineUniqueId	11127.01t2CISSystem.3

Question Requirement: 15.02fHIPAAOrganizational.3 / 0361.0

Change Count: 1

Field	Content
BaselineUniqueId	1502.02f2HIPAAOrganizational.3

Question Requirement: 13.02eNIST80053Organizational.6 / 0342.0

Change Count: 1

Field	Content
BaselineUniqueId	1334.02e2NIST80053Organizational.126

Question Requirement: 13.02eNIST80053Organizational.5 / 0337.0

Change Count: 1

Field	Content
BaselineUniqueId	1302.02e2NIST80053Organizational.1345

Question Requirement: 1748.05f2Organizational.45 / 0487.0

Change Count: 2

Field	Content
RequirementStatement	The organization conducts an exercise at least annually to make contact with a majority (at least eighty (80) percent) of the listed contacts in the plan being exercised. The organization documents that the contact person and information are current during an incident/continuity plan exercise.
IllustrativeProcedureImplemented	For example, the results of the annual exercise and confirm that the organization contacted at least eighty (80) percent of the listed contacts in the incident management/continuity plans being exercised. Confirm that, as a result of the exercise, the contact person and information are updated based on the exercise.

Question Requirement: 17.05fVAD6500Organizational.3 / 0482.0

Change Count: 1

Field	Content
BaselineUniqueId	1743.05f2VAD6500Organizational.43

Question Requirement: 19.13b2Organizational.2 / 0512.0

Change Count: 1

Field	Content
BaselineUniqueId	19.134.05jb2Organizational.52

Question Requirement: 19.13d2Organizational.3 / 0568.0

Change Count: 1

Field	Content
BaselineUniqueId	1902.06.13d2Organizational.43

Question Requirement: 19.06cHIPAAOrganizational.8 / 0555.0

Change Count: 1

Field	Content
BaselineUniqueId	1909.06c2HIPAAOrganizational.68

Question Requirement: 13.07cCMSOrganizational.3 / 0654.0

Change Count: 1

Field	Content
BaselineUniqueId	1324.07c2CMSOrganizational.13

Question Requirement: 18.08bNIST80053Organizational.10 / 0703.0

Change Count: 1

Field	Content
BaselineUniqueId	1804.08b2NIST80053Organizational.120

Question Requirement: 18.08bSROrganizational.2 / 0710.0

Change Count: 1

Field	Content
BaselineUniqueId	1848.08b2SROrganizational.112

Question Requirement: 19.07eMASSOrganizational.4 / 0669.0

Change Count: 1

Field	Content
BaselineUniqueId	19166.07e2MASSOrganizational.74

Question Requirement: 17.07dNIST80053Organizational.4 / 0657.0

Change Count: 1

Field	Content
BaselineUniqueId	1759.07d2NIST80053Organizational.34

Question Requirement: 17.07dNIST80053Organizational.3 / 0663.0

Change Count: 1

Field	Content
BaselineUniqueId	1765.07d2NIST80053Organizational.123

Question Requirement: 11.01qNIST80053System.5 / 2976.0

Change Count: 0

Field	Content
New Question Requirement	11.01qNIST80053System.5 / 2976.0

Question Requirement: 07.10mOWASPOrganizational.2 / 2964.0

Change Count: 0

Field	Content
New Question Requirement	07.10mOWASPOrganizational.2 / 2964.0

Question Requirement: 07.10eOWASPSystem.2 / 2963.0

Change Count: 0

Field	Content
New Question Requirement	07.10eOWASPSystem.2 / 2963.0

Question Requirement: 01.00aOWASPOrganizational.2 / 2962.0

Change Count: 0

Field	Content
New Question Requirement	01.00aOWASPOrganizational.2 / 2962.0

Question Requirement: 07.10mOWASPOrganizational.1 / 2961.0

Change Count: 0

Field	Content
New Question Requirement	07.10mOWASPOrganizational.1 / 2961.0

Question Requirement: 19.13lOWASPOrganizational.2 / 2960.0

Change Count: 0

Field	Content
New Question Requirement	19.13lOWASPOrganizational.2 / 2960.0

Question Requirement: 19.13gOWASPOrganizational.1 / 2959.0

Change Count: 0

Field	Content
New Question Requirement	19.13gOWASPOrganizational.1 / 2959.0

Question Requirement: 19.13jOWASPOrganizational.1 / 2958.0

Change Count: 0

Field	Content
New Question Requirement	19.13jOWASPOrganizational.1 / 2958.0

Question Requirement: 19.06aOWASPOrganizational.2 / 2957.0

Change Count: 0

Field	Content
New Question Requirement	19.06aOWASPOrganizational.2 / 2957.0

Question Requirement: 06.09bOWASPSystem.2 / 2956.0

Change Count: 0

Field	Content
New Question Requirement	06.09bOWASPSystem.2 / 2956.0

Question Requirement: 01.00aOWASPOrganizational.1 / 2955.0

Change Count: 0

Field	Content
New Question Requirement	01.00aOWASPOrganizational.1 / 2955.0

Question Requirement: 06.10cATLASSystem.1 / 2954.0

Change Count: 0

Field	Content
New Question Requirement	06.10cATLASSystem.1 / 2954.0

Question Requirement: 11.01cATLASSystem.1 / 2953.0

Change Count: 0

Field	Content
New Question Requirement	11.01cATLASSystem.1 / 2953.0

Question Requirement: 12.09abATLASSystem.1 / 2952.0

Change Count: 0

Field	Content
New Question Requirement	12.09abATLASSystem.1 / 2952.0

Question Requirement: 11.01jATLASOrganizational.1 / 2951.0

Change Count: 0

Field	Content
New Question Requirement	11.01jATLASOrganizational.1 / 2951.0

Question Requirement: 13.02eATLASOrganizational.1 / 2950.0

Change Count: 0

Field	Content
New Question Requirement	13.02eATLASOrganizational.1 / 2950.0

Question Requirement: 07.10hATLASSystem.2 / 2949.0

Change Count: 0

Field	Content
New Question Requirement	07.10hATLASSystem.2 / 2949.0

Question Requirement: 17.03bStateRAMPOrganizational.1 / 2916.0

Change Count: 0

Field	Content
New Question Requirement	17.03bStateRAMPOrganizational.1 / 2916.0

Question Requirement: 01.05dStateRAMPOrganizational.1 / 2915.0

Change Count: 0

Field	Content
New Question Requirement	01.05dStateRAMPOrganizational.1 / 2915.0

Question Requirement: 08.09nStateRAMPOrganizational.1 / 2914.0

Change Count: 0

Field	Content
New Question Requirement	08.09nStateRAMPOrganizational.1 / 2914.0

Question Requirement: 07.10mOWASPOrganizational.5 / 2913.0

Change Count: 0

Field	Content
New Question Requirement	07.10mOWASPOrganizational.5 / 2913.0

Question Requirement: 06.09bFFIECCATSystem.2 / 2912.0

Change Count: 0

Field	Content
New Question Requirement	06.09bFFIECCATSystem.2 / 2912.0

Question Requirement: 07.10mFFIECCATOrganizational.2 / 2911.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.2 / 2911.0

Question Requirement: 14.09fFFIECCATSystem.2 / 2910.0

Change Count: 0

Field	Content
New Question Requirement	14.09fFFIECCATSystem.2 / 2910.0

Question Requirement: 14.05kFFIECCATOrganizational.2 / 2909.0

Change Count: 0

Field	Content
New Question Requirement	14.05kFFIECCATOrganizational.2 / 2909.0

Question Requirement: 14.09fFFIECCATSystem.3 / 2908.0

Change Count: 0

Field	Content
New Question Requirement	14.09fFFIECCATSystem.3 / 2908.0

Question Requirement: 14.05jFFIECCATOrganizational.2 / 2907.0

Change Count: 0

Field	Content
New Question Requirement	14.05jFFIECCATOrganizational.2 / 2907.0

Question Requirement: 08.01nFFIECCATOrganizational.2 / 2906.0

Change Count: 0

Field	Content
New Question Requirement	08.01nFFIECCATOrganizational.2 / 2906.0

Question Requirement: 08.09mFFIECCATOrganizational.2 / 2905.0

Change Count: 0

Field	Content
New Question Requirement	08.09mFFIECCATOrganizational.2 / 2905.0

Question Requirement: 07.10mFFIECCATOrganizational.3 / 2904.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.3 / 2904.0

Question Requirement: 12.09abFFIECCATSystem.2 / 2903.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.2 / 2903.0

Question Requirement: 12.09abFFIECCATSystem.3 / 2902.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.3 / 2902.0

Question Requirement: 12.09abFFIECCATSystem.4 / 2901.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.4 / 2901.0

Question Requirement: 07.10bATLASSystem.1 / 2868.0

Change Count: 0

Field	Content
New Question Requirement	07.10bATLASSystem.1 / 2868.0

Question Requirement: 07.10mATLASOrganizational.1 / 2867.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.1 / 2867.0

Question Requirement: 19.09zATLASOrganizational.2 / 2866.0

Change Count: 0

Field	Content
New Question Requirement	19.09zATLASOrganizational.2 / 2866.0

Question Requirement: 07.10mATLASOrganizational.7 / 2865.0

Change Count: 0

Field	Content
New Question Requirement	07.10mATLASOrganizational.7 / 2865.0

Question Requirement: 04.01xCISOrganizational.1 / 2864.0

Change Count: 0

Field	Content
New Question Requirement	04.01xCISOrganizational.1 / 2864.0

Question Requirement: 07.07aCISOrganizational.5 / 2863.0

Change Count: 0

Field	Content
New Question Requirement	07.07aCISOrganizational.5 / 2863.0

Question Requirement: 12.09aaCISSystem.3 / 2862.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaCISSystem.3 / 2862.0

Question Requirement: 11.01jCISOrganizational.2 / 2861.0

Change Count: 0

Field	Content
New Question Requirement	11.01jCISOrganizational.2 / 2861.0

Question Requirement: 07.07aCISOrganizational.4 / 2860.0

Change Count: 0

Field	Content
New Question Requirement	07.07aCISOrganizational.4 / 2860.0

Question Requirement: 11.01qCISSystem.3 / 2859.0

Change Count: 0

Field	Content
New Question Requirement	11.01qCISSystem.3 / 2859.0

Question Requirement: 11.01pCISSystem.1 / 2858.0

Change Count: 0

Field	Content
New Question Requirement	11.01pCISSystem.1 / 2858.0

Question Requirement: 19.06dCISOrganizational.2 / 2857.0

Change Count: 0

Field	Content
New Question Requirement	19.06dCISOrganizational.2 / 2857.0

Question Requirement: 11.01lCISOrganizational.1 / 2856.0

Change Count: 0

Field	Content
New Question Requirement	11.01lCISOrganizational.1 / 2856.0

Question Requirement: 01.00aPCIOrganizational.1 / 2855.0

Change Count: 0

Field	Content
New Question Requirement	01.00aPCIOrganizational.1 / 2855.0

Question Requirement: 01.00aPCIOrganizational.4 / 2854.0

Change Count: 0

Field	Content
New Question Requirement	01.00aPCIOrganizational.4 / 2854.0

Question Requirement: 01.00aPCIOrganizational.3 / 2853.0

Change Count: 0

Field	Content
New Question Requirement	01.00aPCIOrganizational.3 / 2853.0

Question Requirement: 07.10mPCIOrganizational.6 / 2852.0

Change Count: 0

Field	Content
New Question Requirement	07.10mPCIOrganizational.6 / 2852.0

Question Requirement: 15.11cPCIOrganizational.1 / 2851.0

Change Count: 0

Field	Content
New Question Requirement	15.11cPCIOrganizational.1 / 2851.0

Question Requirement: 16.09lPCIOrganizational.1 / 2850.0

Change Count: 0

Field	Content
New Question Requirement	16.09lPCIOrganizational.1 / 2850.0

Question Requirement: 11.01qPCISystem.6 / 2849.0

Change Count: 0

Field	Content
New Question Requirement	11.01qPCISystem.6 / 2849.0

Question Requirement: 07.10mPCIOrganizational.4 / 2848.0

Change Count: 0

Field	Content
New Question Requirement	07.10mPCIOrganizational.4 / 2848.0

Question Requirement: 11.01qPCISystem.5 / 2847.0

Change Count: 0

Field	Content
New Question Requirement	11.01qPCISystem.5 / 2847.0

Question Requirement: 19.10iPCISystem.1 / 2846.0

Change Count: 0

Field	Content
New Question Requirement	19.10iPCISystem.1 / 2846.0

Question Requirement: 09.10gPCIOrganizational.3 / 2845.0

Change Count: 0

Field	Content
New Question Requirement	09.10gPCIOrganizational.3 / 2845.0

Question Requirement: 09.10gPCIOrganizational.2 / 2844.0

Change Count: 0

Field	Content
New Question Requirement	09.10gPCIOrganizational.2 / 2844.0

Question Requirement: 01.02fFedRAMPOrganizational.2 / 2843.0

Change Count: 0

Field	Content
New Question Requirement	01.02fFedRAMPOrganizational.2 / 2843.0

Question Requirement: 11.02iFedRAMPOrganizational.2 / 2842.0

Change Count: 0

Field	Content
New Question Requirement	11.02iFedRAMPOrganizational.2 / 2842.0

Question Requirement: 06.10kFedRAMPOrganizational.14 / 2841.0

Change Count: 0

Field	Content
New Question Requirement	06.10kFedRAMPOrganizational.14 / 2841.0

Question Requirement: 01.02aFedRAMPOrganizational.1 / 2840.0

Change Count: 0

Field	Content
New Question Requirement	01.02aFedRAMPOrganizational.1 / 2840.0

Question Requirement: 08.01lFedRAMPOrganizational.4 / 2839.0

Change Count: 0

Field	Content
New Question Requirement	08.01lFedRAMPOrganizational.4 / 2839.0

Question Requirement: 19.13fGDPROrganizational.9 / 2838.0

Change Count: 0

Field	Content
New Question Requirement	19.13fGDPROrganizational.9 / 2838.0

Question Requirement: 19.13pGDPROrganizational.5 / 2837.0

Change Count: 0

Field	Content
New Question Requirement	19.13pGDPROrganizational.5 / 2837.0

Question Requirement: 07.10mFedRAMPOrganizational.18 / 2836.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFedRAMPOrganizational.18 / 2836.0

Question Requirement: 15.11cFedRAMPOrganizational.9 / 2835.0

Change Count: 0

Field	Content
New Question Requirement	15.11cFedRAMPOrganizational.9 / 2835.0

Question Requirement: 18.09pFedRAMPOrganizational.3 / 2834.0

Change Count: 0

Field	Content
New Question Requirement	18.09pFedRAMPOrganizational.3 / 2834.0

Question Requirement: 17.03cFedRAMPOrganizational.2 / 2833.0

Change Count: 0

Field	Content
New Question Requirement	17.03cFedRAMPOrganizational.2 / 2833.0

Question Requirement: 02.09mFedRAMPOrganizational.7 / 2832.0

Change Count: 0

Field	Content
New Question Requirement	02.09mFedRAMPOrganizational.7 / 2832.0

Question Requirement: 12.09hFedRAMPSystem.3 / 2831.0

Change Count: 0

Field	Content
New Question Requirement	12.09hFedRAMPSystem.3 / 2831.0

Question Requirement: 11.01bFedRAMPSystem.8 / 2830.0

Change Count: 0

Field	Content
New Question Requirement	11.01bFedRAMPSystem.8 / 2830.0

Question Requirement: 11.01bFedRAMPSystem.7 / 2829.0

Change Count: 0

Field	Content
New Question Requirement	11.01bFedRAMPSystem.7 / 2829.0

Question Requirement: 17.03bISO23894Organizational.15 / 2808.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the measure(s) indicate the completeness of the organization's AI system assessment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization uses internal and external information on the trustworthiness of the AI system to assess for previously undetected risks or previously assessed risks that are no longer acceptable. If such a risk is identified, the organization assesses the effect on previous risk management activities and feeds the results of this assessment back into the risk management process.

Question Requirement: 17.03aISO23894Organizational.12 / 2802.0

Change Count: 1

Field	Content
RequirementStatement	To support the risk management process, the organization maintains documentation of the following: steps to understand uncertainty in all parts of the AI system, including the utilized data, software, mathematical models, physical extension, and human-in-the-loop aspects of the system; awareness that AI is a fast-moving technology domain. Measurement methods should be consistently evaluated according to their effectiveness and appropriateness for the AI systems in use; a consistent approach to determine the risk level. The approach should reflect the potential impact of AI systems regarding different AI-related objectives; consideration of the organization’s AI capacity, knowledge level, and ability to mitigate realized AI risks when deciding its AI risk appetite.

Question Requirement: 01.03aISO23894Organizational.13 / 2810.0

Change Count: 1

Field	Content
RequirementStatement	In support of the risk management process, tThe organization maintains documentation of the following aspects of the internal context of organization's development and/or use of AI: the effect that an AI system can have on the organization’s culture by shifting and introducing new responsibilities, roles and tasks; any additional international, regional, national and local standards and guidelines that are imposed by the use of AI systems; the additional risks to organizational knowledge related to transparency and explainability of AI systems; the use of AI systems can result in changes to the number of human resources needed to realize a certain capability, or in a variation of the type of resources needed, for instance, deskilling or loss of expertise where human decision-making is increasingly supported by AI systems; the specific knowledge in AI technologies and data science required to develop and use AI systems; the availability of AI tools, platforms and libraries which can enable the development of AI systems without there being a full understanding of the technology, its limitations and potential pitfalls; the potential for AI to raise issues and opportunities related to intellectual property for specific AI systems; how AI systems can be used to automate, optimize and enhance data handling; as consumers of data, additional quality and completeness constraints on data and information can be imposed by AI systems; internal stakeholder perceptions, needs, and expectations; how the use of AI systems can increase the complexity of interdependencies and interconnections; the consideration that the use of AI systems can increase the need for specialized training.

Question Requirement: 01.03aISO23894Organizational.12 / 2809.0

Change Count: 1

Field	Content
RequirementStatement	In support of the risk management process, tThe organization maintains documentation of the following aspects of the external context of organization's development and/or use of AI: relevant legal requirements, including those specifically relating to AI; guidelines on ethical use and design of AI and automated systems issued by government-related groups, regulators, standardization bodies, civil society, academia and industry associations; domain-specific guidelines and frameworks related to AI; technology trends and advancements in the various areas of AI; societal and political implications of the deployment of AI systems, including guidance from social sciences; external stakeholder perceptions, needs, and expectations; how the use of AI, especially AI systems using continuous learning, can affect the ability of the organization to meet contractual obligations and guarantees; contractual relationships during the design and production of AI systems and services; how the use of AI can increase the complexity of networks and dependencies; and how an AI system can replace an existing system and, in such a case, an assessment of the risk benefits and risk transfers of an AI system versus the existing system can be undertaken, considering safety, environmental, social, technical and financial issues associated with the implementation of the AI system.

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 12 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 daypassword minimum and maximum lifetime restrictions of organization-defined numbers for lifetime minimum, lifetime 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: 01.00aNIST80053Organizational.39 / 2640.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the version and most recent date of the relevant personally identifiable information processing and transparency policy and confirm that the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance have been formally defined and documented.

Question Requirement: 01.00aNYDOHOrganizational.5 / 2678.0

Change Count: 1

Field	Content
BaselineUniqueId	01.00aNIST80053YDOHOrganizational.435

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. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the 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 satisfy all applicable organization-defined security requirements.

Question Requirement: 09.09sFTIOrganizational.5 / 2187.0

Change Count: 1

Field	Content
BaselineUniqueId	09215.09sNYDOHFTIOrganizational.105

Question Requirement: 08195.09mNYDOHOrganizational.7 / 2167.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence to confirm firewalls from two [2] or more different vendors are utilized at the various levels within the network to reduce the possibility of compromising the entire network.

Question Requirement: 10969.01dNYDOHSystem.1 / 2042.0

Change Count: 2

Field	Content
RequirementStatement	The information system, for password-based authentication, meets or exceeds the following minimum password requirement: prohibits the use of dictionary names or words; M minimumP passwordA age = one [1] day; MmaximumP p asswordA age = sixty [60] days; MminimumP passwordL l ength = Mminimum length of eight [8] characters for regular user passwords, and minimum length of fifteen [15] characters for administrators or privileged user passwords; PpasswordC c omplexity = minimum (one [1] for Mmoderate) character(s) from the four [4] character categories (A-Z, a-z, 0-9, special characters); PpasswordH historyS size = six [6] passwords for Mmoderate; minimum length (MminimumP passwordL length) for administrators or privileged users of fifteen [15] characters; if the operating environment enforces a minimum of number of changed characters when new passwords are created, set the value at six [6] for Mmoderate systems; store and transmit only encrypted representations of passwords; and allow the use of a temporary password for system logons with an immediate change to a permanent password.
IllustrativeProcedureMeasured	For example, measures indicate the number or percentage of systems/applications where minimum password requirements have been implemented and are consistent with the organization's password policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the information system for password-based authentication (i) enforces password minimum lifetime restriction of one day; (ii) enforces the minimum length for administrators or privileged users is fifteen15 characters.

Question Requirement: 11960.01bNYDOHSystem.1 / 2033.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of information systems that automatically disable inactive accounts within 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: 15967.11cCSR002Organizational.2 / 2003.0

Change Count: 2

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 developed incident response plans that include the roles and responsibilities of both internal resources and third-party service providers, including details on when third-party service providers are required to assist in investigation and response activities.

IllustrativeProcedureMeasured	For example, measures indicate the number of endpoints that can be actively searched as a percentage of all endpoints deployed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and 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)key roles and responsibilities indicated in the incident management policy and procedures and indicate whether or not those roles are current filled by active internal resources or third-party service providers. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization develops incident response plans that include the roles and responsibilities of both internal resources and third-party service providers, including details on when third-party service providers are required to assist in investigation and response activities.

Question Requirement: 191014.13tCCPAOrganizational.1 / 1944.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of individuals responsible for handling consumer inquiries who are/aren' not aware of relevant requirements, as a percentage of all individuals responsible for handling consumer inquiries. Review and/or auditors should be completed by the business to measure the effectiveness of the implemented control(s).

Question Requirement: 16.09hNIST80053System.3 / 0855.0

Change Count: 1

Field	Content
BaselineUniqueId	1610.09h2NIST80053System.43

Question Requirement: 09.09mNIST80053Organizational.7 / 0941.0

Change Count: 1

Field	Content
BaselineUniqueId	099.09m2NIST80053Organizational.117

Question Requirement: 08.09mCMSOrganizational.9 / 0928.0

Change Count: 1

Field	Content
BaselineUniqueId	0858.09m2CMSOrganizational.129

Question Requirement: 0819.09m2Organizational.15 / 0927.1

Change Count: 5

Field	Content
BaselineUniqueId	0819.09m2Organizational.115
CrossVersionId	0927.01
RequirementStatement	A current network diagram exists, documents all high-risk environments, documents all data flows, documents all connections to systems storing, processing, or transmitting covered information, and documents any wireless networks that may have legal compliance impacts. The network diagram is updated based on changes to the network and no less than every six monthsannually.
IllustrativeProcedureImplemented	For example, obtain and examine the network diagram(s) and determine if the network diagram, which includes wireless networks has been reviewed and updated within the past six monthsyear. Ensure that the network diagram identifies all high-risk environments, data flows, and connections to systems storing, processing, or transmitting covered information.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of the organization's high-risk environments, data flows, and connections to systems storing, processing, or transmitting covered information that is appropriately documented in the organization's network diagram, as well as the percentage of systems missing from the network diagram. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that a current network diagram (including wireless networks) exists and is updated whenever there are network changes and no less than every six monthsannually.

Question Requirement: 08.09mNIST80053Organizational.6 / 0940.0

Change Count: 1

Field	Content
BaselineUniqueId	0863.09m2NIST80053Organizational.9106

Question Requirement: 02.09jTXRAMPOrganizational.2 / 0878.0

Change Count: 1

Field	Content
BaselineUniqueId	0205.09j2TXRAMPOrganizational.2

Question Requirement: 02.09jNIST80053Organizational.4 / 0876.0

Change Count: 1

Field	Content
BaselineUniqueId	0214.09j2NIST80053Organizational.94

Question Requirement: 03.09uNIST80053Organizational.4 / 1077.0

Change Count: 1

Field	Content
BaselineUniqueId	0323.09u2NIST80053Organizational.34

Question Requirement: 14.09tDEIDOrganizational.3 / 1073.0

Change Count: 1

Field	Content
BaselineUniqueId	1445.09t2DEIDOrganizational.13

Question Requirement: 09.09sNIST80053Organizational.6 / 1054.0

Change Count: 1

Field	Content
BaselineUniqueId	0912.09s2NIST80053Organizational.76

Question Requirement: 09.09sNIST80053Organizational.7 / 1051.0

Change Count: 1

Field	Content
BaselineUniqueId	0901.09s2NIST80053Organizational.57

Question Requirement: 1204.09aa2System.6 / 1112.0

Change Count: 1

Field	Content
RequirementStatement	The logs of activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, information about the event (e.g., files handled) or failure (e.g., error occurred and corrective action taken), the account or administrator involved, and which processes were involved.

Question Requirement: 17.10k2Organizational.10 / 1241.0

Change Count: 1

Field	Content
BaselineUniqueId	1795.10ak2Organizational.130

Question Requirement: 17.10kNIST80053Organizational.3 / 1240.0

Change Count: 1

Field	Content
BaselineUniqueId	1794.10a2kNIST80053Organizational.123

Question Requirement: 17.10aFFIECISOrganizational.2 / 1237.0

Change Count: 1

Field	Content
BaselineUniqueId	1791.10a2FFIECISOrganizational.62

Question Requirement: 1790.10a2Organizational.45 / 1236.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, confirm thatmeasures indicate the percentage of the organization identified's systems where business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components, or architectures are considered. Where applicable, redundant information systems are tested to ensure the failover from one component to another component works as intended. Examine the organization's disaster recovery and continuity plans and co have not been documented. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization includes business requirements for the availability of infiorm that they takeation systems when specifying security requirements into consideration.

Question Requirement: 19.10eNIST80053System.3 / 1288.0

Change Count: 1

Field	Content
BaselineUniqueId	19200.10e2NIST80053System.13

Question Requirement: 19.10cISO27001System.3 / 1272.0

Change Count: 1

Field	Content
BaselineUniqueId	19189.10c2ISO27001System.83

Question Requirement: 15.10cNIST80053System.5 / 1277.0

Change Count: 1

Field	Content
BaselineUniqueId	1529.10c2NIST80053System.65

Question Requirement: 07.10bATLASSystem.4 / 2948.0

Change Count: 0

Field	Content
New Question Requirement	07.10bATLASSystem.4 / 2948.0

Question Requirement: 19.09zATLASOrganizational.3 / 2947.0

Change Count: 0

Field	Content
New Question Requirement	19.09zATLASOrganizational.3 / 2947.0

Question Requirement: 15.11dNIST800172Organizational.1 / 2946.0

Change Count: 0

Field	Content
New Question Requirement	15.11dNIST800172Organizational.1 / 2946.0

Question Requirement: 06.10kNIST800172Organizational.2 / 2945.0

Change Count: 0

Field	Content
New Question Requirement	06.10kNIST800172Organizational.2 / 2945.0

Question Requirement: 08.01wNIST800172System.2 / 2944.0

Change Count: 0

Field	Content
New Question Requirement	08.01wNIST800172System.2 / 2944.0

Question Requirement: 07.10mNIST800172Organizational.4 / 2943.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNIST800172Organizational.4 / 2943.0

Question Requirement: 08.01wNIST800172System.1 / 2942.0

Change Count: 0

Field	Content
New Question Requirement	08.01wNIST800172System.1 / 2942.0

Question Requirement: 07.10mNIST800172Organizational.3 / 2941.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNIST800172Organizational.3 / 2941.0

Question Requirement: 07.10mNIST800172Organizational.2 / 2940.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNIST800172Organizational.2 / 2940.0

Question Requirement: 17.03bNIST800172Organizational.1 / 2939.0

Change Count: 0

Field	Content
New Question Requirement	17.03bNIST800172Organizational.1 / 2939.0

Question Requirement: 17.03dNIST800172Organizational.1 / 2938.0

Change Count: 0

Field	Content
New Question Requirement	17.03dNIST800172Organizational.1 / 2938.0

Question Requirement: 17.10aNIST800172Organizational.1 / 2937.0

Change Count: 0

Field	Content
New Question Requirement	17.10aNIST800172Organizational.1 / 2937.0

Question Requirement: 07.10mNIST800172Organizational.1 / 2936.0

Change Count: 0

Field	Content
New Question Requirement	07.10mNIST800172Organizational.1 / 2936.0

Question Requirement: 17.03aNIST800172Organizational.1 / 2935.0

Change Count: 0

Field	Content
New Question Requirement	17.03aNIST800172Organizational.1 / 2935.0

Question Requirement: 17.03cNIST800172Organizational.1 / 2934.0

Change Count: 0

Field	Content
New Question Requirement	17.03cNIST800172Organizational.1 / 2934.0

Question Requirement: 10.01qNIST800172System.1 / 2933.0

Change Count: 0

Field	Content
New Question Requirement	10.01qNIST800172System.1 / 2933.0

Question Requirement: 17.03dFFIECCATOrganizational.2 / 2900.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.2 / 2900.0

Question Requirement: 12.09abFFIECCATSystem.5 / 2899.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.5 / 2899.0

Question Requirement: 12.09abFFIECCATSystem.6 / 2898.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.6 / 2898.0

Question Requirement: 12.09abFFIECCATSystem.7 / 2897.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.7 / 2897.0

Question Requirement: 07.10mFFIECCATOrganizational.4 / 2896.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.4 / 2896.0

Question Requirement: 07.10mFFIECCATOrganizational.5 / 2895.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.5 / 2895.0

Question Requirement: 11.01pFFIECCATSystem.2 / 2894.0

Change Count: 0

Field	Content
New Question Requirement	11.01pFFIECCATSystem.2 / 2894.0

Question Requirement: 12.09abFFIECCATSystem.8 / 2893.0

Change Count: 0

Field	Content
New Question Requirement	12.09abFFIECCATSystem.8 / 2893.0

Question Requirement: 14.05dFFIECCATOrganizational.2 / 2892.0

Change Count: 0

Field	Content
New Question Requirement	14.05dFFIECCATOrganizational.2 / 2892.0

Question Requirement: 17.03dFFIECCATOrganizational.7 / 2891.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.7 / 2891.0

Question Requirement: 17.03dFFIECCATOrganizational.6 / 2890.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.6 / 2890.0

Question Requirement: 17.03dFFIECCATOrganizational.5 / 2889.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.5 / 2889.0

Question Requirement: 07.10mFFIECCATOrganizational.9 / 2888.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.9 / 2888.0

Question Requirement: 08.09mFFIECCATOrganizational.3 / 2887.0

Change Count: 0

Field	Content
New Question Requirement	08.09mFFIECCATOrganizational.3 / 2887.0

Question Requirement: 07.10mFFIECCATOrganizational.8 / 2886.0

Change Count: 0

Field	Content
New Question Requirement	07.10mFFIECCATOrganizational.8 / 2886.0

Question Requirement: 17.03dFFIECCATOrganizational.4 / 2885.0

Change Count: 0

Field	Content
New Question Requirement	17.03dFFIECCATOrganizational.4 / 2885.0

Question Requirement: 15.11eNIST80053Organizational.2 / 1505.0

Change Count: 1

Field	Content
BaselineUniqueId	1576.11ePCINIST80053Organizational.12

Question Requirement: 17.03aNYDOHOrganizational.2 / 0393.0

Change Count: 1

Field	Content
BaselineUniqueId	17131.03aGDPRNYDOHOrganizational.12

Question Requirement: 07.10bNIST80053System.2 / 1271.0

Change Count: 1

Field	Content
BaselineUniqueId	0734.10bFTINIST80053System.12

Question Requirement: 08.01iCMSOrganizational.2 / 0120.0

Change Count: 1

Field	Content
BaselineUniqueId	08107.01iFedRAMPCMSOrganizational.2

Question Requirement: 11.01jNIST80053Organizational.3 / 0136.0

Change Count: 1

Field	Content
BaselineUniqueId	11202.01jFedRAMPNIST80053Organizational.3

Question Requirement: 13.02eFTIOrganizational.14 / 2426.0

Change Count: 1

Field	Content
BaselineUniqueId	13.02eFedRAMPTIOrganizational.314

Question Requirement: 18.08gCMSOrganizational.2 / 0759.0

Change Count: 1

Field	Content
BaselineUniqueId	18148.08gFedRAMPCMSOrganizational.12

Question Requirement: 08.09nCMSOrganizational.6 / 0996.0

Change Count: 2

Field	Content
BaselineUniqueId	08114.09nFedRAMPCMSOrganizational.26
IllustrativeProcedureImplemented	For example, examine the organizations system/network diagram and confirm that any system processing, transmitting, or storing Controlled Unclassified Information (CUI) won'ill not be able to connect to an external network without the use of a boundary protection device that meets Trusted Internet Connection (TIC) requirements.

Question Requirement: 08113.09nFedRAMPOrganizational.1 / 0995.0

Change Count: 2

Field	Content
RequirementStatement	The organization requires external/outsourced service providers of all external systems where Federalgovernment information is processed or stored to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services.

IllustrativeProcedureImplemented	For example, examine the list of connections between the information systems in scope for the assessment and information system(s) external to the organization. Select a representative sample of these connections and examine evidence to confirm that the organization required external/outsourced service providers of all external systems where federalgovernment information is processed or stored to identify the specific functions, ports, and protocols used in the provision of the external/outsourced services.

Question Requirement: 16.09lCMSOrganizational.4 / 0919.0

Change Count: 1

Field	Content
BaselineUniqueId	1693.09lFedRAMPCMSOrganizational.24

Question Requirement: 1016.01dCMSSystem.1 / 0082.0

Change Count: 1

Field	Content
RequirementStatement	The organization enforces the following minimum password requirements (Uuser/P / privileged): Mminimum Ppassword Aage = 1/1; Mmaximum Ppassword Aage = 60/60; Mminimum Ppassword Llength = 8/8; Ppassword Ccomplexity = 1/1 (minimum one (1) character from the four (4) character categories (A-Z, a-z, 0-9, special characters); and Ppassword Hhistory Ssize = 6.

Question Requirement: 06.10kPCIOrganizational.3 / 1750.0

Change Count: 1

Field	Content
BaselineUniqueId	0673.10kPCISOrganizational.23

Question Requirement: 07.10bNIST80053System.3 / 1270.0

Change Count: 1

Field	Content
BaselineUniqueId	0764.10bCNIST80053System.63

Question Requirement: 12.09abNIST80053System.8 / 1170.0

Change Count: 1

Field	Content
BaselineUniqueId	1292.09abCNIST80053System.158

Question Requirement: 12.09abNIST80053System.7 / 1169.0

Change Count: 1

Field	Content
BaselineUniqueId	1291.09abCNIST80053System.147

Question Requirement: 12.09abNIST80053System.6 / 1163.0

Change Count: 1

Field	Content
BaselineUniqueId	1289.09abCNIST80053System.146

Question Requirement: 06.06hNIST80053Organizational.3 / 0616.0

Change Count: 1

Field	Content
BaselineUniqueId	0661.06hCNIST80053Organizational.63

Question Requirement: 06.06hNIST80053Organizational.2 / 1887.0

Change Count: 1

Field	Content
BaselineUniqueId	0660.06hCNIST80053Organizational.52

Question Requirement: 09.09mNIST80053Organizational.9 / 1907.0

Change Count: 1

Field	Content
BaselineUniqueId	0958.09mCNIST80053Organizational.169

Question Requirement: 09.09mNIST80053Organizational.8 / 0961.0

Change Count: 1

Field	Content
BaselineUniqueId	0957.09mCNIST80053Organizational.158

Question Requirement: 16.09lHIPAAOrganizational.2 / 0914.0

Change Count: 1

Field	Content
BaselineUniqueId	1688.09lCISHIPAAOrganizational.52

Question Requirement: 1575.11e2Organizational.8 / 1503.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of forensics staff that aren' not trained or qualified to perform forensics activities, as a percentage of all forensics staff. A further metric could indicate the percentage of evidence collected where the proper chain of evidence was not maintained due to inadequate training, staff, and processes. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization has appropriate staff, training and processes to maintain a proper chain of evidence when forensics is conducted.

Question Requirement: 15.11aNIST80053Organizational.7 / 1434.0

Change Count: 1

Field	Content
BaselineUniqueId	1510.11a2NIST80053Organizational.47

Question Requirement: 11.01bFedRAMPSystem.12 / 0027.0

Change Count: 1

Field	Content
BaselineUniqueId	1112.01b2FedRAMPSystem.12

Question Requirement: 10.01dMASSSystem.5 / 0073.0

Change Count: 1

Field	Content
BaselineUniqueId	1014.01d2MASSSystem.95

Question Requirement: 0811.01n2Organizational.6 / 0180.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of authorized remote devices and examine the configuration settings to confirm that the devices cannot establish a connection to communicate with unauthorized remote resourcepolicy exceptions to the traffic flow/access control policy and examine evidence to confirm that the exceptions are appropriately documented with a supporting business need and duration. Further, confirm that the exceptions were reviewed within 365 days.

Question Requirement: 11144.02g2Organizational.5 / 0367.0

Change Count: 1

Field	Content
RequirementStatement	The organization terminates access when the access is no longer needed, assigns of responsibility for removing information system and/or physical access, and timely communicates termination actions to ensure that the termination procedures are appropriately followed.

Question Requirement: 01.13o2Organizational.2 / 0436.0

Change Count: 1

Field	Content
BaselineUniqueId	0162.04b.13o2Organizational.2

Question Requirement: 01.05aNIST80053Organizational.4 / 0441.0

Change Count: 1

Field	Content
BaselineUniqueId	0118.05a2NIST80053Organizational.64

Question Requirement: 01.05aFFIECISOrganizational.2 / 0447.0

Change Count: 1

Field	Content
BaselineUniqueId	0123.05a2FFIECISOrganizational.42

Question Requirement: 12.06jFTIOrganizational.2 / 2015.0

Change Count: 1

Field	Content
BaselineUniqueId	1262.06j2FTIOrganizational.32

Question Requirement: 17.07dCMSOrganizational.4 / 0662.0

Change Count: 1

Field	Content
BaselineUniqueId	1764.07d2CMSOrganizational.114

Question Requirement: 12.09cFISMAOrganizational.7 / 0824.0

Change Count: 1

Field	Content
BaselineUniqueId	1230.09c2FISMAOrganizational.17

Question Requirement: 12.09cFISMAOrganizational.6 / 0827.0

Change Count: 1

Field	Content
BaselineUniqueId	1277.09c2FISMAOrganizational.46

Question Requirement: 06.09bNIST800171System.3 / 0820.0

Change Count: 1

Field	Content
BaselineUniqueId	0618.09b2NIST800171System.3

Question Requirement: 1825.08l2Organizational.1 / 0811.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, observe the organization's process for disposal of assets. Confirm that devices containing covered information are wiped or degaussed to securely remove electronic information. If the information can'not be sanitized confirm that it is shredded, disintegrated, grinded, incinerated, pulverized, or melted to destroy electronic and hard copy media. This can also be confirmed through review of the disposal record for each asset being disposed or reused.

Question Requirement: 06900.09d1System.2 / 1955.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of changes, and examine the change management record to confirm the following: (i) along with removing accounts, a review of all custom code preceding the release to production, or to customers, must be completed in order to identify any possible coding vulnerability, to include at least the following: (a) code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices, (b) code reviews ensure code is developed according to secure coding guidelines, (c) appropriate corrections are implemented prior to release, and (d) code-review results are reviewed and approved by management prior to release; (ii) test data and accounts are removed completely before the application is placed into a production state; (iii) organizations remove all custom application accounts, user IDs, and passwords before applications go from development to production or are released to customers; (iv) rules for the transfer of software from development to operational status are defined and documented; (v) development and operational software runs on different systems or computer processors and in different domains or directories; (vi) compilers, editors, and other development tools or system utilities are not accessible from operational systems when not required; (vii) the test system environment emulates the operational system environment as closely as possible; (viii) users will use different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error; and (ix) covered information will not be copied into the test system environment. Further, review of test data used and configuration of testing and production environments may be performed to ensure that controls are implemented to ensure the separation between operational, test, and development environments.

Question Requirement: 16.09l1Organizational.4 / 2326.0

Change Count: 3

Field	Content
RequirementStatement	The organization maintains offline and/or immutable backups of data.
IllustrativeProcedureImplemented	For example, observe the organization's facility and determine where offline backup media is stored. If an immutable backup solution is in place, examine configurations and whitepapers to support the backup cannot be modified or deleted.
IllustrativeProcedureMeasured	For example, measures indicate the number of offline and/or immutable backup copies that the organization maintains. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that offline and/or immutable backup copies data and systems are maintained.

Question Requirement: 0778.10m1Organizational.5 / 1398.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence that the organization documents and tracks vulnerabilities identified through vulnerability scans. Select a sample of vulnerabilities identified through previous scans and confirm whether the vulnerability has been addressed or accepted by management. Further, select a sample of risks accepted by management and examine formal evidence that acceptance was reviewed on a periodic basis.

Question Requirement: 06.09b1System.2 / 2368.0

Change Count: 2

Field	Content
RequirementStatement	Changes to information systems (including changes to applications, databases, configurations, AI models, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.
IllustrativeProcedureImplemented	For example, select a sample of changes made to information systems (including changes to applications, databases, configurations, AI models, network devices, and operating systems and with the potential exception of automated security patches) and confirm that they were documented, tested, and approved.

Question Requirement: 16.12eNIST80053Organizational.2 / 1562.0

Change Count: 1

Field	Content
BaselineUniqueId	1686.12eFTINIST80053Organizational.12

Question Requirement: 1532.11aFTIOrganizational.12 / 1444.0

Change Count: 1

Field	Content
RequirementStatement	Any data incident potentially involving FTI is immediately reported to the appropriate Treasury Inspector General for the Tax Administration (TIGTA) field office and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification of a possible issue involving FTI. The organization documents in a data incident report the following aspect of the incident to the extent it is known at the time: Name of organization and organization Point of Contact for resolving data incident with contact information; Date and time of the incident; Date and time the incident was discovered; How the incident was discovered; Description of the incident and the data involved, including specific data elements, if known; Potential number of FTI records involved; if unknown, provide a range if possible; Address where the incident occurred; IT involved (e.g., laptop, server, mainframe). FTI is not included in the data Incident report. Reports are sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email.

Question Requirement: 10.01dFTISystem.4 / 2588.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of IT devices using a personal identification number (PIN) as an authenticator for MFA and examine evidence to confirm if any devices are not configured for a minimum PIN length of eight (8) digits. Confirm also that configuration enforces complex sequences (e.g., 73961548 – no repeating digits and no sequential digits). Examine the last distribution of the acceptable use policy that includes IT devices using a personal identification number (PIN) as an authenticator for MFA and confirm it specifies to not store the PIN with the SmartCard and to not share PINs.

Question Requirement: 10.01dNIST800171System.3 / 0091.0

Change Count: 1

Field	Content
BaselineUniqueId	1035.01dFTINIST800171System.3

Question Requirement: 04.01xNYDOHOrganizational.3 / 0278.0

Change Count: 1

Field	Content
BaselineUniqueId	0412.01xFTINYDOHOrganizational.13

Question Requirement: 11.01tFedRAMPSystem.4 / 0241.0

Change Count: 1

Field	Content
BaselineUniqueId	11129.01tFTIedRAMPSystem.24

Question Requirement: 11.01qFTISystem.7 / 2636.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of information systems where users are not required to re-authenticate when switching to a privileged user role. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that users are required to re-authenticate when switching to a privileged user role.

Question Requirement: 18.08aNIST80053Organizational.2 / 0694.0

Change Count: 1

Field	Content
BaselineUniqueId	1840.08aFTINIST80053Organizational.2

Question Requirement: 11.09abNIST80053System.4 / 1181.0

Change Count: 1

Field	Content
BaselineUniqueId	11215.09abFedRAMPNIST80053System.34

Question Requirement: 11.09abCMSSystem.10 / 1180.0

Change Count: 1

Field	Content
BaselineUniqueId	11214.09abFedRAMPCMSSystem.210

Question Requirement: 12.09aaCMSSystem.13 / 1127.0

Change Count: 1

Field	Content
BaselineUniqueId	12102.09aaFedRAMPCMSSystem.713

Question Requirement: 12.09aaCMSSystem.12 / 1132.0

Change Count: 1

Field	Content
BaselineUniqueId	12107.09aaFedRAMPCMSSystem.712

Question Requirement: 12.09aaNIST80053System.5 / 1130.0

Change Count: 1

Field	Content
BaselineUniqueId	12105.09aaFedRAMPNIST80053System.75

Question Requirement: 18.09pNYDOHOrganizational.3 / 1013.0

Change Count: 1

Field	Content
BaselineUniqueId	18150.09pFedRAMPNYDOHOrganizational.13

Question Requirement: 09.10gCMSOrganizational.2 / 2468.0

Change Count: 1

Field	Content
BaselineUniqueId	09.10gFedRAMPCMSOrganizational.2

Question Requirement: 09.10gNIST80053Organizational.2 / 1299.0

Change Count: 1

Field	Content
BaselineUniqueId	0964.10gFedRAMPNIST80053Organizational.12

Question Requirement: 09.10dFTISystem.4 / 2484.0

Change Count: 1

Field	Content
BaselineUniqueId	09.10dFedRAMPTISystem.14

Question Requirement: 17.10aFedRAMPOrganizational.6 / 2462.1

Change Count: 4

Field	Content
BaselineUniqueId	17.10aFedRAMPOrganizational.56
CrossVersionId	2462.01
RequirementStatement	The organization reviews the development process, standards, tools, and tool options/configurations as neededdnnually and as dictated by the current threat posture to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization and service provider-defined security requirements.

IllustrativeProcedureImplemented	For example, examine evidence to confirm that the organization performed a review of the organization's development process, standards, tools, and tool options/configurations as needednnually and as dictated by the current threat posture. Examine the results of the review and confirm that the review assessed the development process, standards, tools, and tool options/configurations selected and employed, and it satisfied all applicable organization and service provider- defined security requirements.

Question Requirement: 12.09afFedRAMPSystem.4 / 2422.1

Change Count: 3

Field	Content
BaselineUniqueId	12.09afFedRAMPSystem.24
CrossVersionId	2422.01
RequirementStatement	The information system compares the internal information system clocks at least hourly with http://tf.nist.gov/tf-cgi/servers.cgi and synchronizes the internal system clocks to the authoritative time source when there is any time difference is greater than organization-defined time period.

Question Requirement: 12.09afNIST80053System.2 / 1225.0

Change Count: 1

Field	Content
BaselineUniqueId	12100.09afFedRAMPNIST80053System.12

Question Requirement: 15.12eFedRAMPOrganizational.9 / 2467.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, examine documented incident response test results to confirm the organization tested the incident response capability for the information system at least every six (6) months using organization-defined tests to determine the incident response effectiveness.
IllustrativeProcedureMeasured	For example, measures indicate the existence of documented incident response tests that meet the requirements stipulated in the requirement statement, as a percentage of all incident response tests. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization tests the incident response capability for the information system at least every six (6) months using organization-defined tests to determine the incident response effectiveness and documents the results.

Question Requirement: 16.12eCMSOrganizational.3 / 2458.0

Change Count: 1

Field	Content
BaselineUniqueId	16.12eFedRAMPCMSOrganizational.63

Question Requirement: 16.12cFTIOrganizational.3 / 1537.0

Change Count: 1

Field	Content
BaselineUniqueId	1698.12cFedRAMPTIOrganizational.3

Question Requirement: 16.12cNIST80053Organizational.8 / 1536.0

Change Count: 1

Field	Content
BaselineUniqueId	1697.12cFedRAMPNIST80053Organizational.28

Question Requirement: 15.11cFTIOrganizational.4 / 1473.0

Change Count: 1

Field	Content
BaselineUniqueId	1582.11cFedRAMPTIOrganizational.14

Question Requirement: 15.11cFedRAMPOrganizational.8 / 2466.1

Change Count: 4

Field	Content
BaselineUniqueId	15.11cFedRAMPOrganizational.78
CrossVersionId	2466.01
RequirementStatement	The organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability, describes the structure and organization of the incident response capability, provides a high-level approach for how the incident response capability fits into the overall organization, meets the unique requirements of the organization, which relate to mission, size, structure, and functions, defines reportable incidents, provides metrics for measuring the incident response capability within the organization, defines the resources and management support needed to effectively maintain and mature an incident response capability, anddresses the sharing of incident information, is reviewed and approved by organization-defined personnel or roles at a minimum on an annual basis, and explicitly designates responsibility for incident response to organization-defined entities, personnel, or roles. The organization updates the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.

IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability, describes the structure and organization of the incident response capability, provides a high-level approach for how the incident response capability fits into the overall organization, meets the unique requirements of the organization, which relate to mission, size, structure, and functions, defines reportable incidents, provides metrics for measuring the incident response capability within the organization, defines the resources and management support needed to effectively maiaddresses the sharing of incidenta in and mature an incident response capability, andformation, is reviewed and approved by organization-defined personnel or roles at a minimum on an annual basis, and explicitly designates responsibility for incident response to organization-defined entities, personnel, or roles.

Question Requirement: 07.10mTXRAMPOrganizational.2 / 2428.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10mFedTXRAMPOrganizational.92

Question Requirement: 07.10mNIST80053Organizational.3 / 1411.0

Change Count: 1

Field	Content
BaselineUniqueId	0791.10mFedRAMPNIST80053Organizational.73

Question Requirement: 07.10mCISOrganizational.14 / 2444.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10mFedRAMPCISOrganizational.154

Question Requirement: 06.10kFedRAMPOrganizational.8 / 2441.0

Change Count: 1

Field	Content
RequirementStatement	The organization coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes at an organization-defined frequency and/or organization-defined configuration change conditions.

Question Requirement: 06.10kCMSOrganizational.11 / 1356.0

Change Count: 1

Field	Content
BaselineUniqueId	0679.10kFedRAMPCMSOrganizational.511

Question Requirement: 10.01dCMSSystem.8 / 0088.0

Change Count: 1

Field	Content
BaselineUniqueId	1039.01dFedRAMPCMSSystem.28

Question Requirement: 11.01bCISSystem.2 / 2369.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01bFedRAMPCISSystem.2

Question Requirement: 13.00aCMSOrganizational.5 / 2388.0

Change Count: 1

Field	Content
BaselineUniqueId	13.00aFedRAMPCMSOrganizational.35

Changes for Authoritative Source Document - v11.2.0 to v11.3.0

Authoritative Source Document: FedRAMP r5

Change Count: 0

Field	Content
New Authoritative Source Document	FedRAMP r5

Authoritative Source Document: Health Industry Cybersecurity Practices (HICP) v2023

Change Count: 0

Field	Content
New Authoritative Source Document	Health Industry Cybersecurity Practices (HICP) v2023

Authoritative Source Document: StateRAMP r5

Change Count: 0

Field	Content
New Authoritative Source Document	StateRAMP r5

Authoritative Source Document: 23 NYCRR 500 (2nd Amendment)

Change Count: 0

Field	Content
New Authoritative Source Document	23 NYCRR 500 (2nd Amendment)

Authoritative Source Document: Singapore Personal Data Protection Act (2023)

Change Count: 0

Field	Content
New Authoritative Source Document	Singapore Personal Data Protection Act (2023)

Authoritative Source Document: MITRE ATLAS

Change Count: 0

Field	Content
New Authoritative Source Document	MITRE ATLAS

Authoritative Source Document: OWASP AI Exchange

Change Count: 0

Field	Content
New Authoritative Source Document	OWASP AI Exchange

Authoritative Source Document: PCI DSS v4.0

Change Count: 0

Field	Content
New Authoritative Source Document	PCI DSS v4.0

Authoritative Source Document: TX-RAMP 2.0

Change Count: 0

Field	Content
New Authoritative Source Document	TX-RAMP 2.0

Authoritative Source Document: HHS Cybersecurity Performance Goals (CPGs)

Change Count: 0

Field	Content
New Authoritative Source Document	HHS Cybersecurity Performance Goals (CPGs)

Authoritative Source Document: NIST 800-172

Change Count: 0

Field	Content
New Authoritative Source Document	NIST 800-172

Authoritative Source Document: FFIEC Cybersecurity Assessment Tool

Change Count: 0

Field	Content
New Authoritative Source Document	FFIEC Cybersecurity Assessment Tool

Authoritative Source Document: CIS CSC v8.0

Change Count: 0

Field	Content
New Authoritative Source Document	CIS CSC v8.0

Authoritative Source Document: EU GDPR v2023

Change Count: 0

Field	Content
New Authoritative Source Document	EU GDPR v2023

Authoritative Source Document: NIST SP 800-53 r5

Change Count: 1

Field	Content
Version	r5.1.1

Changes for Factor Type - v11.2.0 to v11.3.0

Factor Type: Compliance - GDPR

Change Count: 0

Field	Content
New Factor Type	Compliance - GDPR

Factor Type: Compliance - FedRAMP r5

Change Count: 0

Field	Content
New Factor Type	Compliance - FedRAMP r5

Factor Type: Compliance - StateRAMP r5

Change Count: 0

Field	Content
New Factor Type	Compliance - StateRAMP r5

Factor Type: Compliance - HHS Cybersecurity Performance Goals

Change Count: 0

Field	Content
New Factor Type	Compliance - HHS Cybersecurity Performance Goals

Factor Type: Compliance - FFIEC CAT

Change Count: 0

Field	Content
New Factor Type	Compliance - FFIEC CAT

Factor Type: Compliance - CIS CSC v8.0

Change Count: 0

Field	Content
New Factor Type	Compliance - CIS CSC v8.0

Changes for Factor - v11.2.0 to v11.3.0

Factor: Compliance - StateRAMP r5 - Impact level: Moderate

Change Count: 0

Field	Content
New Factor	Compliance - StateRAMP r5 - Impact level: Moderate

Factor: Compliance - StateRAMP r5 - Impact level: Low

Change Count: 0

Field	Content
New Factor	Compliance - StateRAMP r5 - Impact level: Low

Factor: Compliance - HHS Cybersecurity Performance Goals - Enhanced Goals

Change Count: 0

Field	Content
New Factor	Compliance - HHS Cybersecurity Performance Goals - Enhanced Goals

Factor: Compliance - HHS Cybersecurity Performance Goals - Essential Goals

Change Count: 0

Field	Content
New Factor	Compliance - HHS Cybersecurity Performance Goals - Essential Goals

Factor: Compliance - FFIEC CAT - Innovative

Change Count: 0

Field	Content
New Factor	Compliance - FFIEC CAT - Innovative

Factor: Compliance - FFIEC CAT - Advanced

Change Count: 0

Field	Content
New Factor	Compliance - FFIEC CAT - Advanced

Factor: Compliance - FFIEC CAT - Intermediate

Change Count: 0

Field	Content
New Factor	Compliance - FFIEC CAT - Intermediate

Factor: Compliance - FFIEC CAT - Evolving

Change Count: 0

Field	Content
New Factor	Compliance - FFIEC CAT - Evolving

Factor: Compliance - FFIEC CAT - Baseline

Change Count: 0

Field	Content
New Factor	Compliance - FFIEC CAT - Baseline

Factor: Compliance - CIS CSC v8.0 - Implementation Group 3

Change Count: 0

Field	Content
New Factor	Compliance - CIS CSC v8.0 - Implementation Group 3

Factor: Compliance - CIS CSC v8.0 - Implementation Group 2

Change Count: 0

Field	Content
New Factor	Compliance - CIS CSC v8.0 - Implementation Group 2

Factor: Compliance - CIS CSC v8.0 - Implementation Group 1

Change Count: 0

Field	Content
New Factor	Compliance - CIS CSC v8.0 - Implementation Group 1

Factor: Compliance - GDPR - Data Controller

Change Count: 0

Field	Content
New Factor	Compliance - GDPR - Data Controller

Factor: Compliance - GDPR - Data Processor

Change Count: 0

Field	Content
New Factor	Compliance - GDPR - Data Processor

Factor: Compliance - FedRAMP r5 - High

Change Count: 0

Field	Content
New Factor	Compliance - FedRAMP r5 - High

Factor: Compliance - FedRAMP r5 - Moderate

Change Count: 0

Field	Content
New Factor	Compliance - FedRAMP r5 - Moderate

Factor: Compliance - FedRAMP r5 - Low

Change Count: 0

Field	Content
New Factor	Compliance - FedRAMP r5 - Low

Factor: Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-172

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-172

Factor: Compliance - HITRUST Reg: Compliance Factors - MITRE ATLAS

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - MITRE ATLAS

Factor: Compliance - HITRUST Reg: Compliance Factors - OWASP AI Exchange

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - OWASP AI Exchange

Factor: Compliance - HITRUST Reg: Compliance Factors - PCI DSS v4.0

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - PCI DSS v4.0

Factor: Compliance - HITRUST Reg: Compliance Factors - TX-RAMP 2.0

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - TX-RAMP 2.0

Factor: Compliance - HITRUST Reg: Compliance Factors - 23 NYCRR 500 Second Amendment

Change Count: 1

Field	Content
Selection	23 NYCRR 500 Second Amendment