v11.9.0 Summary of Changes

Difference Comparison for CSF v11.8.0 to v11.9.0

HITRUST

Table of Contents

Changes for Library Version - v11.8.0 to v11.9.0

Library Version: v11.9.0

Change Count: 1

Field	Content
Name	v11.*8*9.0

Changes for Control Objective - v11.8.0 to v11.9.0

Control Objective: 09.02 Control Third-Party Service Delivery

Change Count: 2

Field	Content
Name	09.02 Control Third -Party Service Delivery
Description	To ensure that third -party service providers maintain security requirements and levels of service as part of their service delivery agreements.

Changes for Question Requirement - v11.8.0 to v11.9.0

Question Requirement: 19.06dFedRAMPOrganizational.2 / 2478.0

Change Count: 1

Field	Content
BaselineUniqueId	19.09*m***6d**FedRAMPOrganizational.*6***2**

Question Requirement: 1704.03b1Organizational.2 / 0394.1

Change Count: 5

Field	Content
BaselineUniqueId	1704.03b1Organizational.*1*2
RequirementStatement	The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization*. R*, **including** risks a*ssessments***rising from changes in vulnerability exploitability and threat conditions, and** are to be performed at planned intervals *and*, when major changes occur in the environment, and *the***when changes in exploitability or threat conditions materially affect risk. Risk assessment** results **are** reviewed annually.
IllustrativeProcedureImplemented	For example, examine the results of the most recent risk assessment and determine if the results were reviewed and documented*. C* **and** confirm that the assessment was reviewed by management and is performed at least annually. Further, ensure that the risk assessment was performed in a manner consistent with the organization's risk management procedures and that it identified information security risks to the organization*. Further*, **including risks arising from changes in vulnerability exploitability and threat conditions (i.e., a change that is likely to impact the security or privacy posture of the information system). Additionally**, select a sample of major changes which have occurred in the environment and ensure that risk assessments were performed and/or updated for each.
IllustrativeProcedureMeasured	For example, measures indicate the number of risk assessments performed in accordance with the organization's policies. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization performs risk assessments in a consistent way**, including risks arising from changes in vulnerability exploitability and threat conditions,** and at planned intervals, *and* when there are major changes to the organization's environment, **and when changes in exploitability or threat conditions materially affect risk,** and reviews the risk assessment results annually.
CrossVersionId	0394.*0***1**

Question Requirement: 1903.06d1Organizational.3456711 / 0569.0

Change Count: 2

Field	Content
RequirementStatement	Covered and/or confidential information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs. Exceptions to encryption requirements are authorized by management and documented. *Encryp***Data protec**tion is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures **that account for cryptographic algorithm strength and lifecycle status**. For full-disk encryption, logical access is independent of O/S access. Decryption keys are not tied to user accounts. If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.
IllustrativeProcedureImplemented	For example, examine evidence t*hat***o confirm** covered and/or confidential information at rest is encrypted via one-way hashes, truncation, or strong cryptography and key-management practices **that account for cryptographic algorithm strength and lifecycle status**. Further, if full disk encryption is used, confirm that decryption keys are not associated to user accounts. For instances where encryption of covered and/or confidential information is noted, examine evidence to confirm that the rationale is documented and was reviewed by management and if alternative compensating controls other than encryption are approved and reviewed annually by the CISO. *Further***Additionally**, ensure that for full-disk encryption: logical access is independent of O/S access and decryption is not tied to user accounts.

Question Requirement: 1781.10a1Organizational.23 / 1227.0

Change Count: 3

Field	Content
RequirementStatement	Specifications for *the* security control requirements include security controls to be incorporated in the information system **to address common, complex, and context-dependent weaknesses**, and supplemented by manual controls as needed. *Further, s***S**ecurity control requirements **addressing such weaknesses** are considered when evaluating software packages, **whe***i*ther developed or purchased.
IllustrativeProcedureImplemented	For example, **examine documentation to confirm** information security requirements are identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds*. R*, **and the r**esults of the identification *is***are** documented and reviewed by all stakeholders. *S***Further, s**elect a sample of software packages that were developed or purchased and confirm that the organization assessed security controls that were incorporated in the information system **to address common, complex, and context-dependent weaknesses** and the supplementation of manual controls if required.

IllustrativeProcedureMeasured	For example, the measure(s) indicate the number of software packages that were developed or purchased where the specifications for the security control requirements were not identified, as a percent of software packages that were developed or purchased. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* information system specifications for security control requirements state that security controls are to be incorporated in the information system **to address common, complex, and context-dependent weaknesses**, supplemented by manual controls as needed, and these considerations are also applied when evaluating software packages, developed or purchased.

Question Requirement: 01.00aNIST80053Organizational.40 / 2641.0

Change Count: 1

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

Question Requirement: 12.06iFFIECCATOrganizational.3 / 2567.0

Change Count: 1

Field	Content
BaselineUniqueId	12.06i*CMS***FFIECCAT**Organizational.*1***3**

Question Requirement: 16.12dLISOrganizational.2 / 1543.0

Change Count: 1

Field	Content
BaselineUniqueId	16.12d*TJC***LIS**Organizational.2

Question Requirement: 19419.13jHIPAAOrganizational.1 / 1718.0

Change Count: 2

Field	Content
RequirementStatement	The *covered entity, or equivalent,***organization** makes reasonable efforts to limit requests for PHI to, or from, another covered entity, business associate, or equivalent, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Exceptions include, but are not limited to, treatment, requests by the individual, or uses or disclosures pursuant to a valid authorization, required by law, or required for compliance with other requirements (for example, disclosures made to the Secretary of Health and Human Services).
IllustrativeProcedureMeasured	For example, the metric could indicate the number of excessive disclosures contrary to the requirements specified in applicable law, as a percentage of all disclosures. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the *covered entity, or equivalent,***organization** makes reasonable efforts to limit requests for PHI to, or from, another covered entity, business associate, or equivalent, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Question Requirement: 19.13hNYDOHOrganizational.2 / 2537.0

Change Count: 1

Field	Content
BaselineUniqueId	19.13h*CMS***NYDOH**Organizational.*1***2**

Question Requirement: 19.09zAISecOrganizational.1 / 2866.0

Change Count: 1

Field	Content
RequirementStatement	The organization limits the release of technical AI project details, including specific information on the technical architecture of the overall AI system; datasets used for training, testing, validating, and tuning of confidential and/or closed-source AI models; datasets used for prompt augmentation via RAG (if performed); algorithm(s) used to create confidential and/or closed-source AI models; architecture of confidential and/or closed-source AI models; *language model tools used such as agents***agents, skills,** and plugins (if used); safety and security checkpoints built into the AI system; and information on teams developing and supporting the AI system.

Question Requirement: 17.05gNYDOHOrganizational.2 / 0492.0

Change Count: 1

Field	Content
BaselineUniqueId	17*53*.05g*CMS***NYDOH**Organizational.*1***2**

Question Requirement: 19.10cNIST80053System.4 / 1909.0

Change Count: 1

Field	Content
BaselineUniqueId	19*196*.10c*CMS***NIST80053**System.*35***4**

Question Requirement: 191013.13bCCPAOrganizational.7 / 1937.0

Change Count: 1

Field	Content
RequirementStatement	Businesses which sell personal information to third- parties are required to provide a reasonably accessible notice to consumers that: provide a clear and conspicuous link on its website homepage, titled “Limit the Use of My Sensitive Personal Information,” which enables the consumer, or person authorized, to opt-out of the sale of personal information–the business may not require a consumer to open an account to exercise their opt-out right; include a description of the consumer’s rights and a separate link to the “Limit the Use of My Sensitive Personal Information” webpage in its online privacy notice or in any California-specific privacy notice; ensure that anyone who handles consumer inquiries knows the relevant requirements; refrain from selling information of a consumer who has opted-out; respect the consumer’s decision to opt-out for at least 12 months before seeking authorization to selling information again; and use personal information provided in an opt-out request only for complying with the request.

Question Requirement: 12148.06i1Organizational.2 / 2121.1

Change Count: 4

Field	Content
BaselineUniqueId	12148.06i1Organizational.*1***2**
RequirementStatement	The organization**, based on a formally documented assessment of risk,** determines which of the following auditable events require auditing on a continuous basis *in response to specific situations*: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; *and* override of access control mechanisms**; and other auditable events indicative of exploitation of technical vulnerabilities (e.g., unexpected outbound connections, unexpected inter-process injection, suspicious scheduled execution)**.
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization**, based on a formally documented assessment of risk,** determine**s**d which pre-defined auditable events required auditing on a continuous basis *in response to specific situations*.

CrossVersionId	2121.*0*1

Question Requirement: 1428.05k1Organizational.2 / 0523.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that the organization identified and mandated the implementation of information security controls to address supplier access to the organizations information and information assets.

Question Requirement: 19.13iNYDOHOrganizational.2 / 2287.0

Change Count: 1

Field	Content
BaselineUniqueId	19*314*.13iN*IST80053***YDOH**Organizational.2

Question Requirement: 19.13qNYDOHOrganizational.3 / 2666.0

Change Count: 1

Field	Content
BaselineUniqueId	19.13q*CMS***NYDOH**Organizational.*1***3**

Question Requirement: 13.02eCMSOrganizational.7 / 2078.0

Change Count: 1

Field	Content
BaselineUniqueId	13*105*.02e*NYDOH***CMS**Organizational.*9***7**

Question Requirement: 1710.03a2Organizational.3 / 0384.1

Change Count: 5

Field	Content
BaselineUniqueId	1710.03a2Organizational.*2***3**
RequirementStatement	The organization evaluates, and manages risk prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, **whenever exploitability or threat conditions materially change,** or at a minimum annually.
IllustrativeProcedureImplemented	For example, select a sample of security incidents and confirm whether a new risk was introduced to the organization **or if there's a material change in the threat conditions (i.e., a change that is likely to impact the security or privacy posture of the information system)**. Examine evidence to confirm that the organization evaluated and implemented actions to manage the risk.

IllustrativeProcedureMeasured	For example, measures indicate the number of risks identified by the organization and the percentage of which have been evaluated and managed *at least***prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, whenever exploitability or threat conditions materially change, or at a minimum** annually. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization evaluates and manages risk prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, **whenever exploitability or threat conditions materially change,** or at a minimum annually.
CrossVersionId	0384.*0***1**

Question Requirement: 01.00aVAD6500Organizational.4 / 1978.0

Change Count: 1

Field	Content
BaselineUniqueId	01*940*.00a*NIST80053***VAD6500**Organizational.*19***4**

Question Requirement: 01.00aFedRAMPOrganizational.24 / 2460.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00aFedRAMPOrganizational.*15***24**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity policy training controls. **The organization ensures the system and information integrity policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the system and information integrity policy and procedures.** The organization reviews and updates the current system and information integrity policy at least annually, and system and information integrity policy and training procedures at least annually or whenever a significant change occurs.
CrossVersionId	2460.*0***1**

Question Requirement: 01.00aNIST80053Organizational.27 / 2430.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.*13***27**

RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the system and services acquisition policy and associated *system and services acquisition control***controls. The organization ensures the system and services acquisition policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the system and services acquisition policy and procedure**s. The organization reviews and updates the current system and services acquisition policy at least annually*,* and system and services acquisition procedures at least annually or whenever a significant change occurs.
CrossVersionId	2430.*0***1**

Question Requirement: 01.00aNIST80053Organizational.28 / 2393.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.*19***28**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the system maintenance policy and associated controls. **The organization ensures the system maintenance policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the system maintenance policy and procedures.** The organization reviews and updates the current system maintenance policy at least annually*,* and system maintenance procedures at least annually or whenever a significant change occurs.
CrossVersionId	2393.*0***1**

Question Requirement: 01.00aNIST80053Organizational.20 / 2390.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.*5***20**

RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the media protection policy and associated *media protection control***controls. The organization ensures the media protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the media protection policy and procedure**s. The organization reviews and updates the current media protection policy at least annually*,* and media protection procedures at least annually or whenever a significant change occurs.
CrossVersionId	2390.*0***1**

Question Requirement: 01.00aNIST80053Organizational.21 / 2389.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.*7***21**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the personnel security policy and associated *personnel security control***controls. The organization ensures the personnel security policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the personnel security policy and procedure**s. The organization reviews and updates the current personnel security policy at least annually*,* and personnel security procedures at least annually or whenever a significant change occurs.
CrossVersionId	2389.*0***1**

Question Requirement: 01.00aNIST80053Organizational.24 / 2381.1

Change Count: 3

Field	Content
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.**2**4

RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the security planning policy and associated *security planning control***controls. The organization ensures the security planning policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the security planning policy and procedure**s. The organization reviews and updates the current security planning policy **at least** annually*,* and security planning procedures at least annually or whenever a significant change occurs.
CrossVersionId	2381.*0***1**

Question Requirement: 01.00aNIST80053Organizational.33 / 2379.1

Change Count: 3

Field	**Content**
BaselineUniqueId	01.00a*FedRAMP***NIST80053**Organizational.3**3**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles an identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the identification and authentication policy and associated *identification and authentication control***controls. The organization ensures the identification and authentication policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the identification and authentication policy and procedure**s. The organization reviews and updates the current identification and authentication policy **at least** annually and identification and authentication procedures at least annually or whenever a significant change occurs.
CrossVersionId	2379.*0***1**

Question Requirement: 19180.09z1Organizational.2 / 1103.1

Change Count: 3

Field	Content
RequirementStatement	The organization trains individuals to ensure that publicly posted information does not contain nonpublic information. If the organization permits the posting of **nonpublic** information onto a publicly accessible information system **(e.g., online forum, social media platform, public repository, or AI service where the organization cannot control downstream access, use, retention, or disclosure)**, it designates individuals authorized to post the information.
IllustrativeProcedureImplemented	For example, *examine the list of individuals with acces***select a sample of employees and examine evidence (e.g., training materials, training acknowledgement) to confirm they have received training to ensure that publicly posted information does not contain nonpublic information. Further, if the organization permit**s t*o***he** post**ing of nonpublic** information onto *a* publicly accessible information system*. Confirm that the individuals on the list are designated and authorized by the organization. Further, select a sample of users and examine evidence (e.g., training materials, training acknowledgement) to confirm that they have received training to ensure that publicly posted information does not contain nonpublic***s (e.g., online forum, social media platform, public repository, or AI service where the organization cannot control downstream access, use, retention, or disclosure), examine documentation to confirm designated individuals were authorized to post the** information.
IllustrativeProcedureMeasured	For example, measures indicate the *number of unauthorized users that have access to post information onto a publicly accessible information system, as a percentage of all users. A further measure could indicate the number of individuals that have not received training to ensure that publicly posted information does not contain nonpublic***percentage of employees who did not receive training to ensure that publicly posted information does not contain nonpublic information. A further measure could indicate the number of individuals posting nonpublic information onto a publicly accessible** information **system**. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization*,* trains individuals to ensure that publicly *accessible***posted** information does not contain nonpublic information *and designates individuals authorized to post information onto a publicly accessible information system*.

Question Requirement: 01.04aNYDOHOrganizational.3 / 2255.0

Change Count: 1

Field	Content
BaselineUniqueId	01*282*.04a*DGF***NYDOH**Organizational.*1***3**

Question Requirement: 01.02bNYDOHOrganizational.4 / 2512.0

Change Count: 1

Field	Content
BaselineUniqueId	01.02bCMSNYDOHOrganizational.24

Question Requirement: 01.02aNYDOHOrganizational.2 / 2250.0

Change Count: 1

Field	Content
BaselineUniqueId	01277.02aDGFNYDOHOrganizational.12

Question Requirement: 14.05kOWASPOrganizational.2 / 3342.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measurements could indicate the number of software, tools, and datasets that aren' not in compliance. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization uses automated license management tools for real-time monitoring of licensing compliance using Bill of Materials (BOMs).

Question Requirement: 01.00aISO27001Organizational.3 / 1975.0

Change Count: 1

Field	Content
BaselineUniqueId	01937.00aNISTT80053O27001Organizational.203

Question Requirement: 01.00aVAD6500Organizational.3 / 1974.0

Change Count: 1

Field	Content
BaselineUniqueId	01936.00aNIST80053VAD6500Organizational.213

Question Requirement: 01.00aVAD6500Organizational.2 / 1968.0

Change Count: 1

Field	Content
BaselineUniqueId	01930.00aNIST80053VAD6500Organizational.23

Question Requirement: 01.00aNIST80053Organizational.47 / 0005.0

Change Count: 1

Field	Content
BaselineUniqueId	01101.00aFFIECISNIST80053Organizational.147

Question Requirement: 11.01cAISecSystem.8 / 3057.0

Change Count: 1

Field	Content
RequirementStatement	The organization restricts the ability to interact with the production AI model through APIs, the AI application, and *language model tools such as agents***agents, skills,** and plugins (if used). This access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews), and authentication.

Question Requirement: 11.01cAISecSystem.5 / 3054.0

Change Count: 3

Field	Content
RequirementStatement	The organization restricts the data (e.g., databases, document repositories, embeddings) access and capabilities (e.g., messaging) granted to generative AI models (including through *language model tools such as agents***agents, skills,** and plugins) following the least privilege principle. This access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews), and authentication.
IllustrativeProcedureImplemented	For example, review the AI model to ensure the organization restricts the data (e.g., databases, document repositories, embeddings) access and capabilities (e.g., messaging) granted to generative AI models (including through *language model tools such as agents***agents, skills,** and plugins) following the least privilege principle. Further, confirm this access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews) and authentication.
IllustrativeProcedureMeasured	For example, measures indicate if the organization restricts the data (e.g., databases, document repositories, embeddings) access and capabilities (e.g., messaging) granted to generative AI models (including through *language model tools such as agents***agents, skills,** and plugins) following the least privilege principle. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews) and authentication.

Question Requirement: 17.10aNYDOHOrganizational.9 / 1250.0

Change Count: 1

Field	Content
BaselineUniqueId	17*103*.10a*CMS***NYDOH**Organizational.*2***9**

Question Requirement: 08.01i1Organizational.2 / 0117.0

Change Count: 1

Field	Content
BaselineUniqueId	08*02*.01i1Organizational.2

Question Requirement: 14.05kAISecOrganizational.1 / 3051.0

Change Count: 3

Field	Content
RequirementStatement	Agreements between the organization and external commercial providers of AI system components and services clearly communicate the organization's AI security requirements, including agreements with providers of AI models, datasets, software packages, platforms and computing infrastructure, *language model tools such as agents***agents, skills,** and plugins, and contracted AI system-related services (e.g., outsourced AI system development), as applicable.
IllustrativeProcedureImplemented	For example, review a sample of agreements between the organization and external commercial providers of AI system components and services to evidence these documents clearly communicate the organization's AI security requirements. Further, confirm that agreements are in place with all providers of AI models, datasets, software packages, platforms and computing infrastructure, *language model tools such as agents* **agents, skills,** and plugins, and contracted AI system-related services (e.g., outsourced AI system development), as applicable.
IllustrativeProcedureMeasured	For example, measures indicate if agreements between the organization and external commercial providers of AI system components and services clearly communicate the organization's AI security requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that agreements are in place with all providers of AI models, datasets, software packages, platforms and computing infrastructure, *language model tools such as agents***agents, skills,** and plugins, and contracted AI system-related services (e.g., outsourced AI system development), as applicable.

Question Requirement: 11.01INIST80053Organizational.3 / 0153.0

Change Count: 1

Field	Content
BaselineUniqueId	11*98*.01I*CMS***NIST80053**Organizational.*13*

Question Requirement: 12.09abHICPSystem.7 / 1170.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09ab*NIST80053***HICP**System.*87*

Question Requirement: 12.09abNYDOHSystem.10 / 1163.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09abN*IST80053***YDOH**System.*6***10**

Question Requirement: 17.10aCISOrganizational.2 / 2264.0

Change Count: 1

Field	Content
BaselineUniqueId	17*291*.10a*N***C**IS*T80053*Organizational.*1***2**

Question Requirement: 19.13kPHIPAOrganizational.26 / 1727.0

Change Count: 1

Field	Content
BaselineUniqueId	19*567*.13k*DeID***PHIPA**Organizational.*3***26**

Question Requirement: 11180.01c3System.6 / 0047.0

Change Count: 2

Field	Content
RequirementStatement	Access to management functions or administrative consoles for systems hosting virtualized systems is restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., *two***multi**-factor authentication, audit trails, **H**IP *address fil***S/NIPS, firewalls, Web application protection, antivirus, file in**tegri*ng, firewalls***ty monitoring**, and TLS encapsulated communications to the administrative consoles).
IllustrativeProcedureImplemented	For example, select of virtualized systems and confirm that access to the management console requires *two* **multi**-factor authentication. Further, for selected systems, examine the list of personnel with access to the management console and confirm that it is limited to appropriate personnel. Further, review whether technical controls are performed to confirm that virtualized operating systems include firewall (inbound/outbound), Host Intrusion Prevention System (HIPS), Network Intrusion Prevention System (NIPS), Web application protection, antivirus, file integrity monitoring, and log monitoring, etc. has been implemented.

Question Requirement: 11111.01q2System.4 / 0209.0

Change Count: 3

Field	Content
RequirementStatement	When PKI-based **or PKI-compatible** authentication is used, the information system validates certificates **or equivalent certificate credentials** by: constructing and verifying a certification path **or equivalent cryptographic validation path** to an accepted trust anchor, including checking certificate status information; enforcing access to**, or proof of possession of,** the corresponding private key; mapping the identity to the corresponding account of the individual or group; and implementing a local cache of revocation**, status, or equivalent validation** data to support path discovery *and***, proof** validation *in case of an inability to access***, and credential validation when** revocation **or status** information **cannot be accessed** via the network.
IllustrativeProcedureImplemented	For example, observe the usage of PKI-based **or PKI-compatible** authentication and confirm that the certificate **or equivalent certificate credentials** is valid and issued by an appropriate authority. Further, review the technical specification for the PKI-based **or PKI-compatible** authentication mechanism and confirm that it addressed each element of the requirements stipulated in the requirement statement.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of valid certificates that have been appropriately constructed and verified in accordance with the organization's policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that when PKI-based **or PKI-compatible** authentication is used, the information system validates certificates **or equivalent certificate credentials** by constructing and verifying a certification path **or equivalent cryptographic validation path** to an accepted trust anchor, including checking certificate status information; enforcing access to**, or proof of possession of,** the corresponding private key; mapping the identity to the corresponding account of the individual or group; and implementing a local cache of revocation **status, or equivalent validation** data to support path discovery *and***, proof** validation *in case of an inability to access***, and credential validation when** revocation **or status** information **cannot be accessed** via the network.

Question Requirement: 14.05jFFIECCATOrganizational.4 / 0517.0

Change Count: 1

Field	Content
BaselineUniqueId	14*62*.05jFFIEC*IS***CAT**Organizational.*1***4**

Question Requirement: 14.05jFFIECCATOrganizational.3 / 0518.0

Change Count: 1

Field	Content
BaselineUniqueId	14*63*.05jFFIEC*IS***CAT**Organizational.*2***3**

Question Requirement: 1407.05k2Organizational.1 / 0528.0

Change Count: 2

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

Question Requirement: 1406.05k2Organizational.2 / 0522.1

Change Count: 3

Field	Content
RequirementStatement	The standard agreement with third- parties includes: the information security policy; procedures to protect organizational assets, including information, software, and hardware; any required physical protection controls and mechanisms; controls to ensure protection against malicious software; procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software and hardware) has occurred; controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement; confidentiality, integrity, availability, and any other relevant property of the assets; restrictions on copying and disclosing information, and using confidentiality agreements; user and administrator training in methods, procedures, and security; ensuring user awareness for information security responsibilities and issues; provision for the transfer of personnel, where appropriate; responsibilities regarding hardware and software installation and maintenance; a clear reporting structure and agreed reporting formats; a clear and specified process of change management; the different reasons, requirements, and benefits that make the access by the third -party necessary; permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; an authorization process for user access and privileges; a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use; a statement that all access that is not explicitly authorized is forbidden; a process for revoking access rights or interrupting the connection between systems.
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that each requirement as noted in the requirement statement has been defined and included into the agreement.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-party agreements that satisfy the identified security requirements in accordance with the organization's policies, as a percentage of all third-party agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that a standard agreement with third- parties is defined and includes the required security controls in accordance with the organization's security policies.

Question Requirement: 1432.05k2Organizational.7 / 0527.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, contractors, or third-party users provided through an organization and confirm that appropriate screening was conducted in accordance with the organization's policy. Further: Select a sample of instances in which contractors were provided through an organization and examine the contract to ensure it (a) clearly specifies all responsibilities for screening, (b) notification procedures for screening, (c) notification procedures to follow when screening has not been completed, and (d) notification procedures when screening results give cause for doubt or concern.

Question Requirement: 1431.05k2Organizational.6 / 0526.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that personnel security requirements have been defined. Confirm that security roles and responsibilities for third-party providers are coordinated and aligned with internal security roles and responsibilities.

Question Requirement: 1430.05k2Organizational.5 / 0525.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that a review was performed to ensure that the agreement is understood. Further, examine evidence to confirm that an indemnity clause has been defined in the agreement.

Question Requirement: 1429.05k2Organizational.4 / 0524.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that the organization identified requirements to address information risks. Further, examine evidence to confirm that the agreement includes an acknowledgement that the third-party (e.g., a service provider) is responsible for the security of the data the third-party possesses or otherwise stores, processes, or transmits on behalf of the organization.

Question Requirement: 1406.05k2Organizational.3 / 0522.2

Change Count: 3

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

IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-party agreements that satisfy the identified security requirements in accordance with the organization's policies, as a percentage of all third-party agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that a standard agreement with third- parties is defined and includes the required security controls in accordance with the organization's security policies.

Question Requirement: 1516.11c2Organizational.7 / 1460.1

Change Count: 2

Field	Content
RequirementStatement	The organization implements a formal incident response program, which includes the definition of specific phases for incident response and accounts for and prepares the organization for a variety of incidents (e.g., system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered and/or confidential information, system misuse, unauthorized WAPs, *and* identity theft, **ransomware, data breach, insider threat, and system outage**). In addition to normal contingency plans, the program also covers: analysis and identification of the cause of the incident; containment; increased monitoring of system use; and planning and implementation of corrective action to prevent recurrence.
IllustrativeProcedureImplemented	For example, *obtain and* examine the **organization's** incident response program*, which includes the incident response policies and procedures, and determine if a variety of common incidents are identified and that the steps the organization will take in response to each incident have been formally defined* **and related incident response documentation, including playbooks, to confirm the organization implemented a formal incident response program that defined specific phases for incident response and addressed a variety of incident types (e.g., system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered and/or confidential information, system misuse, unauthorized WAPs, identity theft, ransomware, data breach, insider threat, and system outage) and covered analysis and identification of the cause of the incident, containment, increased monitoring of system use, and planning and implementation of corrective action to prevent recurrence. Further, confirm each playbook included clear, step-by-step actions, assigned roles and responsibilities, escalation paths, communication requirements, containment, eradication, recovery steps, and post-incident activities to ensure a consistent and effective response**.

Question Requirement: 19.05eCCPAOrganizational.2 / 0478.0

Change Count: 1

Field	Content
BaselineUniqueId	19*130*.05e*NIST80053***CCPA**Organizational.*1***2**

Question Requirement: 01.02cNYDOHOrganizational.2 / 0323.0

Change Count: 1

Field	Content
BaselineUniqueId	01.02cN*IST80053***YDOH**Organizational.2

Question Requirement: 01.05aNYDOHOrganizational.2 / 0441.0

Change Count: 1

Field	Content
BaselineUniqueId	01.05aN*IST80053***YDOH**Organizational.*4***2**

Question Requirement: 01.00aNIST80053Organizational.39 / 2640.0

Change Count: 1

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

Question Requirement: 01.00aNIST80053Organizational.38 / 2632.0

Change Count: 1

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

Question Requirement: 08.09nNYDOHOrganizational.6 / 0996.0

Change Count: 1

Field	Content
BaselineUniqueId	08.09n*CMS***NYDOH**Organizational.6

Question Requirement: 08.09nNYDOHOrganizational.7 / 2592.0

Change Count: 1

Field	Content
BaselineUniqueId	08.09n*CMS***NYDOH**Organizational.*3***7**

Question Requirement: 08.09nNYDOHOrganizational.5 / 0992.0

Change Count: 1

Field	Content
BaselineUniqueId	08*89*.09n*CMS***NYDOH**Organizational.*1***5**

Question Requirement: 11.02gSEC530Organizational.2 / 0374.0

Change Count: 1

Field	Content
BaselineUniqueId	11*151*.02g*CMS***SEC530**Organizational.2

Question Requirement: 1404.05i3Organizational.1 / 0503.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties and examine evidence to determine if appropriate due diligence procedures were carried out. Examine evidence such as interviews, document review, checklists, review certifications (e.g., HITRUST) or other remote means to confirm that due diligence activities took place. Further, confirm that an non-disclosure agreement was executed as part of the due diligence process.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-parties where appropriate due diligence and execution of a non-disclosure agreement were performed, as a percent of all third-party agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that due diligence of the external party includes interviews, document review, checklists, certification reviews (e.g., HITRUST) or other remote means.

Question Requirement: 17.05dCMSOrganizational.3 / 2298.0

Change Count: 1

Field	Content
BaselineUniqueId	17.05d*NIST80053***CMS**Organizational.*2***3**

Question Requirement: 15.11bVAD6500Organizational.2 / 1458.0

Change Count: 1

Field	Content
BaselineUniqueId	15.11b*NIST80053***VAD6500**Organizational.*3***2**

Question Requirement: 16.12cCMSOrganizational.14 / 1515.0

Change Count: 1

Field	Content
BaselineUniqueId	16.12c*NIST80053***CMS**Organizational.*7***14**

Question Requirement: 19.06dVAD6500Organizational.3 / 2105.0

Change Count: 1

Field	Content
BaselineUniqueId	19*132*.06d*NYDOH***VAD6500**Organizational.*1***3**

Question Requirement: 19618.13kHIPAAOrganizational.31 / 1638.0

Change Count: 3

Field	Content
RequirementStatement	PHI may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities, as required by HIPAA § 164.512(k)(2). Based on the complexity of the entity, policy elements to consider include, but are not limited to, whether the purpose for the disclosure is to conduct lawful intelligence, for counter-intelligence, and/or for other national security activities authorized by the National Security Act.
IllustrativeProcedureImplemented	For example, inquire of management if PHI is disclosed to authorized federal officials. Obtain and review a representative sample of PHI disclosed to federal officials to determine if the purposes are appropriate and reasonable. Based on the complexity of the entity, elements to consider include, but are not limited to, whether the purpose for the disclosure is to conduct lawful intelligence, for counter-intelligence, and/or for other national security activities authorized by the National Security Act, as specified in HIPAA § 164.512(k)(2). Examine security and privacy incident reports to determine if PHI has been disclosed to federal officials inappropriately. Interview a representative sample of personnel responsible for handling patient/client information to determine if written or ad hoc procedures are followed consistently. Interview legal personnel to determine if the organization has been, is currently, or reasonably expects to be involved in litigation or state investigation for a failure to comply with the regulatory criteria for disclosing PHI to authorized federal officials as required by HIPAA § 164.512(k)(2). Review complaints from an ethics and/or compliance hotline to determine if there are complaints about inappropriate or unauthorized uses or disclosures of PHI to federal officials. Interview human resources personnel to determine if workforce members have been disciplined for uses or disclosures of PHI to federal officials that were not compliant with the regulatory requirements for such uses or disclosures. Examine related legal and HR documentation, if available.
IllustrativeProcedureMeasured	For example, measures indicate the number of inappropriate disclosures of PHI to a federal official as a percentage of all disclosures. Non-compliance with the policy requirements could be part of a broader metric that considers all unauthorized disclosures, regardless of type, if unauthorized disclosures of PHI to federal officials as required by HIPAA 64.512(k)(2) can be discerned. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity discloses PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities.

Question Requirement: 12100.09ab2System.15 / 1152.0

Change Count: 3

Field	Content
RequirementStatement	The organization monitors the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise *and* **(e.g., exploitation of technical vulnerabilities) and to** help confirm the system is functioning in an optimal, resilient, and secure state.
IllustrativeProcedureImplemented	For example, examine evidence that the organization has implemented automated tools (e.g., DLP, SIEM, **EDR, NDR, IDS,** NetFlow) on various information systems, such as applications, operating systems, databases, network devices DMZ, including physical access to identify irregularities or anomalies **that are indicators of a system malfunction or compromise (e.g. unexpected service failures, abnormal resource utilization, unauthorized process execution, anomalous network communications, unusual logical or physical access activity)**.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of information systems containing covered and/or confidential information monitored through the use of automated tools, along with the percentage of information systems not compliant with this requirement. A further measure can indicate the number of irregularities or anomalies detected as part of the monitoring process. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization monitors the information system to identify irregularities or anomalies that are indicators of a system malfunction or compromise **(e.g., exploitation of technical vulnerabilities)** and help confirm the system is functioning in an optimal, resilient, and secure state.

Question Requirement: 06.09bFTISystem.2 / 2153.0

Change Count: 1

Field	Content
BaselineUniqueId	06*181*.09b*NYDOH***FTI**System.*10***2**

Question Requirement: 17.03aNYDOHOrganizational.5 / 2671.0

Change Count: 1

Field	Content
BaselineUniqueId	17.03a*CMS***NYDOH**Organizational.5

Question Requirement: 07.07aFTIOrganizational.4 / 2292.0

Change Count: 1

Field	Content
BaselineUniqueId	07*319*.07a*NIST80053***FTI**Organizational.*1***4**

Question Requirement: 07.10mNYDOHOrganizational.10 / 1404.0

Change Count: 1

Field	Content
BaselineUniqueId	07*47*.10m*CMS***NYDOH**Organizational.*7***10**

Question Requirement: 15.11aC5Organizational.2 / 1436.0

Change Count: 1

Field	Content
BaselineUniqueId	15.11a*NIST80053***C5**Organizational.*6***2**

Question Requirement: 15.11aHIPAAOrganizational.12 / 1434.0

Change Count: 1

Field	Content
BaselineUniqueId	15.11a*NIST80053***HIPAA**Organizational.*7***12**

Question Requirement: 11.01eNYDOHSystem.3 / 0103.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01eN*IST80053***YDOH**System.*2***3**

Question Requirement: 12.09aaC5System.3 / 1125.0

Change Count: 1

Field	Content
BaselineUniqueId	12*48*.09aaC*MS***5**System.*4***3**

Question Requirement: 1434.05kFTIOrganizational.23 / 0534.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the contracts or SLA to confirm that security policies and procedures have been defined and documented for how FTI is stored, handled, and accessed inside the cloud based on IRS Publication 1075. Confirm that the SLA at a minimum meet the requirements as stated in the requirement statement.

Question Requirement: 1433.05kFTIOrganizational.5 / 0533.1

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the acquisition contracts to confirm that they contain appropriate language from IRS Pub 1075, Safeguarding Contract Language. Further, confirm that the contracts contain organization-defined security and privacy controls and comply with the requirements specified in IRS Pub 1075.

Question Requirement: 12.09abLISSystem.3 / 1150.0

Change Count: 1

Field	Content
BaselineUniqueId	12*103*.09ab*Texas***LIS**System.*1***3**

Question Requirement: 19.13hNYDOHOrganizational.3 / 2294.0

Change Count: 1

Field	Content
BaselineUniqueId	19*321*.13hN*IST80053***YDOH**Organizational.*2***3**

Question Requirement: 19.13tSEC530Organizational.2 / 2075.0

Change Count: 1

Field	Content
BaselineUniqueId	19.13t*NYDOH***SEC530**Organizational.*4***2**

Question Requirement: 07.10bSEC530System.3 / 1270.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10b*NIST800***SEC**53**0**System.3

Question Requirement: 10.01d1System.10 / 2361.0

Change Count: 3

Field	Content
RequirementStatement	P*assword policies applicable to the organization's information systems***olicies governing the authentication mechanisms used by the organization's information systems (e.g., passwords or passwordless mechanisms such as passkeys)** are documented and enforced through technical controls.

IllustrativeProcedureImplemented	For example, obtain and inspect the organization's documented p*assword policies***olicies governing the authentication mechanisms used by the organization's information systems (e.g., passwords or passwordless mechanisms such as passkeys)** and compare them to the *password policie***authentication mechanism**s technically enforced within the organization's system(s).
IllustrativeProcedureMeasured	For example, measures indicate the percentage of organizational systems that are compliant/non-compliant with the organization's p*assword policie***olicies governing the authentication mechanisms used by the organization's information system**s.

Question Requirement: 1003.01d1System.3 / 0069.0

Change Count: 3

Field	Content
RequirementStatement	User identities are verified prior to performing password resets **or binding passwordless authenticators (e.g., passkeys) to user accounts**.
IllustrativeProcedureImplemented	For example, select a sample of help desk tickets or requests to perform a password request. *E* **or binding a passwordless authenticator to a user account and e**xamine evidence to confirm that help desk technician or administrator verified and documented the user's identity prior to resetting the user's password*. If* **or binding** the password *rese***less authenticator to the user's account. Further, if the authenticator managemen**t function is automated, observe a user reset his/her password **or bind the passwordless authenticator to their account** and determine if he/she must confirm his/her identity prior to the *password reset***automated process resolving**.
IllustrativeProcedureMeasured	For example, measures indicate the number of *password rese* **authenticator managemen**t requests where the user's identi***f*****t** y was not verified as a percentage of all *password rese* **authenticator managemen**t requests. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that user identities are verified prior to performing password resets **or binding passwordless authenticators to user accounts**.

Question Requirement: 0913.09s1Organizational.2 / 1055.1

Change Count: 3

Field	Content
BaselineUniqueId	0913.09s1Organizational.*5***2**

RequirementStatement	Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security *(TLS) 1.2 or la* **configured with NIST-approved algorithms, such as TLS v1.3 or TLS v1.2 with approved cipher sui**te*r***s**; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TLS VPNs: SSL Portal VPN; SSL Tunnel VPN.
CrossVersionId	1055.*0*1

Question Requirement: 0903.10f1Organizational.1 / 1289.0

Change Count: 4

Field	Content
RequirementStatement	Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required **, including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms**), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).
IllustrativeProcedureImplemented	For example, select a sample of transmissions of covered and/or confidential data across communication lines and *inspect***examine** evidence to confirm that the transmissions are encrypted based on pre-defined criteria. Further, select a sample of instances in which covered and/or confidential information is stored on removable mobile/removable media and inspect evidence to confirm that the media is encrypted based on pre-determined criteria. *Further***Additionally**, determine if encryption policies and procedures address: the required level of protection (e.g., the type and strength of the encryption algorithm required**, including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms**); and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).
UseInBasic	*Fals***True**
BasicAlternativeLanguage	**Is encryption used to protect covered and/or confidential information transported by mobile or removable media and across communication lines? Do encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required, including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes)?**

Question Requirement: 1007.01d2System.2 / 0076.0

Change Count: 3

Field	Content
RequirementStatement	All passwords a*re encryp***nd secrets associated with passwordless authenticators are cryptographically protec**ted during transmission and storage.
IllustrativeProcedureImplemented	For example, select a sample of systems/applications and examine evidence to confirm that passwords a*re transmitted or stored in an encrypted format.* **nd secrets associated with passwordless authenticators are cryptographically protected during transmission and storage.**
IllustrativeProcedureMeasured	For example, measures indicate the number of systems/applications that are compliant/non-compliant with the organization**'**s *passw***authenticato***r**d* policy that ensures passwords a*re transmitted or stored in encrypted format***nd secrets associated with passwordless authenticators are cryptographically protected during transmission and storage**. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that passwords a*re encryp***nd secrets associated with passwordless authenticators are cryptographically protec**ted during transmission and storage on all system components.

Question Requirement: 14.05iFFIECCATOrganizational.2 / 0507.0

Change Count: 1

Field	Content
BaselineUniqueId	14*59*.05iFFIEC*IS***CAT**Organizational.*1***2**

Question Requirement: 12.09aaNIST80053System.11 / 2397.1

Change Count: 3

Field	Content
BaselineUniqueId	12.09aa*FedRAMP***NIST80053**System.1*0***1**

RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles an audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the audit and accountability policy and associated controls. **The organization ensures the audit and accountability policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.** The organization reviews and updates the current audit and accountability policy at least annually*,* and audit and accountability procedures at least annually or whenever a significant change occurs.
CrossVersionId	2397.*0***1**

Question Requirement: 08.00aNIST80053Organizational.25 / 2396.1

Change Count: 3

Field	**Content**
BaselineUniqueId	08.00a*FedRAMP***NIST80053**Organizational.*9***25**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the system and communications protection policy and associated *system and communications protection control***controls. The organization ensures the system and communications protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the system and communications protection policy and procedure**s. The organization reviews and updates the current system and communications protection policy at least annually*,* and system and communications protection procedures at least annually or whenever a significant change occurs.
CrossVersionId	2396.*0***1**

Question Requirement: 0201.09j1Organizational.124 / 0873.0

Change Count: 3

Field	Content
RequirementStatement	Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-*virus and anti-spyware soft***mal**ware are addressed via a network-based malware detection (NBMD) solution.
IllustrativeProcedureImplemented	For example, select a sample of endpoint devices (desktops, laptops, servers, BYOD, etc.)*, determine if* **to confirm** anti-malware software is installed, operating**,** and up-to-date. *E* **Further, e**xamine the configuration settings for the anti-malware software and confirm that it is centrally managed and that definition files are automatically downloaded and pushed out to clients when updates are available. *Further***Additionally**, confirm that the software has been configured to perform (a) automated periodic scans to detect and remove any malicious code; (b) compile information on file reputations or have administrators manually push updates to all machines; and (c) verify that each system has received its signature update via automated means. Further, inspect evidence to confirm that the checks carried out by malicious code detection and repair software include checking: files on electronic or optical media when inserted; electronic mail attachments; downloads; Web traffic; and files received over networks. Further, inspect evidence that malware checks of electronic mail attachments and downloads are carried out at different places (e.g., at email servers, on endpoints, and when entering the network). *Further* **Also**, select a sample of bring your own device (BYOD) devices and ensure that anti-malware software is in use (where supported).

IllustrativeProcedureMeasured	For example, measures indicate the percentage of endpoint devices (desktops, laptops, servers, etc.) that appropriately have anti-malware software installed and in operation, as a percentage of all endpoint devices. A further measure(s) could indicate the number of malware detected and blocked by the installed anti-malware solutions. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that anti-*virus and anti-spy***mal**ware *are***is** installed, operating and updated on all devices to conduct periodic scans of the system to identify and remove unauthorized software. This anti-malware software offers a centralized infrastructure that compiles information on file reputations, or the organization requires administrators to manually push updates to all machines. After applying an update, automated systems verify that each applicable system has received its signature update.

Question Requirement: 02962.09j1Organizational.6 / 1989.1

Change Count: 5

Field	Content
BaselineUniqueId	02962.09j1Organizational.*5***6**
RequirementStatement	The organization**, based on a formally documented assessment of risk,** augments endpoint protection strategies with additional **risk-appropriate** solutions—including those built into the operating system if available—to mitigate exploitation of unknown **and context-dependent** vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).
IllustrativeProcedureImplemented	For example, *but not limited to,* obtain and examine the endpoint protection policy and procedures, and examine evidence to confirm that the organization has**, based on a formally documented assessment of risk,** augmented endpoint protection strategies with additional **organization-determined risk-appropriate (i.e. allowlisting for privileged workstations, or sanitation protocols for remote workstations)** solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, has targeted the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins). These solutions typically include i) using application sandboxing/micro-virtualization; ii) leveraging built-in operating system exploit mitigation if available, such as Windows Defender Exploit Guard (WDEG) *and*, Microsoft Enhanced Mitigation Experience Toolkit (EMET)**, Data Execution Prevention / No-Execute (DEP/NX), or Address Space Layout Randomization (ASLR)**; and/or iii) implementing third-party endpoint protection products that provide*s* exploit mitigation capability beyond more traditional antivirus (i.e., whitelisting/blacklisting) strategies, often referred to as Next Generation Endpoint Protection.

IllustrativeProcedureMeasured	For example, measures indicate the number of attacks on endpoints where the augmented endpoint protection solution has successfully mitigated when traditional antivirus failed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization *has augmented*, **based on a formally documented assessment of risk, augments** endpoint protection strategies with additional **risk-appropriate** solutions—including those built into the operating system if available—to mitigate exploitation of unknown **and context-dependent** vulnerabilities where traditional antivirus may be ineffective; and where applicable, *has* target*ed* the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).
CrossVersionId	1989.*0***1**

Question Requirement: 07.10bAISecSystem.1 / 2948.0

Change Count: 3

Field	Content
RequirementStatement	Before *they***inputs** are processed by the model, the *AI system actively***organization implements controls to** filter*s user* **all** inputs (regardless of modality or source, including **inputs received from other information systems and any associated** attachments) for suspicious and/or unexpected values or patterns which could be adversarial or malicious in nature.
IllustrativeProcedureImplemented	For example, review the AI system configurations to ensure that *user***all** inputs (regardless of modality or source, including **inputs received from other information systems and any associated** attachments) are actively filtered before they reach the model.
IllustrativeProcedureMeasured	For example, measures indicate if the organization checks *user***all** inputs (regardless of modality or source, including **inputs received from other information systems and any associated** attachments) for anomalies and filters suspicious and/or unexpected values or patterns which could be adversarial or malicious in nature. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the identified anomalous entries are removed.

Question Requirement: 07.10mAISecOrganizational.6 / 2870.0

Change Count: 1

Field	Content
RequirementStatement	To find potentially exploitable vulnerabilities, the organization inspects downloaded AI software assets before use—including models (e.g., such as those sourced from online model zoos); software packages used to create, train, and/or deploy models (e.g., python packages); and *language model tools such as agents***agents, skills,** and plugins (if used). The organization (4) acts upon the results, as necessary.

Question Requirement: 07.10mAISecOrganizational.2 / 3048.0

Change Count: 3

Field	Content
RequirementStatement	To help ensure that unsafe assets are not introduced into the AI system, the organization checks the cryptographic hashes and/or digital signatures on downloaded AI models; software packages (e.g., those for model creation, training, and/or deployment); datasets (e.g., training datasets); and *language model tools (e.g., agents,***agents, skills, and** plugins*)* before use, as applicable.
IllustrativeProcedureImplemented	For example, review the AI system to ensure the organization verifies the cryptographic hashes and/or digital signatures on downloaded AI models, software packages (e.g., those for model creation, training, and/or deployment), datasets (e.g., training datasets), and *language model tools (e.g., agents,* **agents, skills, and** plugins*)* before use, as applicable.
IllustrativeProcedureMeasured	For example, measures indicate if the organization verifies the cryptographic hashes and/or digital signatures on downloaded AI models, software packages (e.g., those for model creation, training, and/or deployment), datasets (e.g., training datasets), and *language model tools (e.g., agents,***agents, skills, and** plugins*)* before use, as applicable.

Question Requirement: 10.01dLISSystem.3 / 0068.0

Change Count: 1

Field	Content
BaselineUniqueId	10*22*.01d*MAS***LI**SSystem.*1***3**

Question Requirement: 09.09mNIST80053Organizational.11 / 2169.0

Change Count: 1

Field	Content
BaselineUniqueId	09*197*.09mN*YDOH***IST80053**Organizational.*7***11**

Question Requirement: 07.10mCMSOrganizational.6 / 2210.0

Change Count: 1

Field	Content
BaselineUniqueId	07*238*.10m*NYDOH***CMS**Organizational.*5***6**

Question Requirement: 07.10mFFIECCATOrganizational.10 / 2207.0

Change Count: 1

Field	Content
BaselineUniqueId	07*235*.10m*NYDOH***FFIECCAT**Organizational.*2***10**

Question Requirement: 08.09mLISOrganizational.5 / 0928.0

Change Count: 1

Field	Content
BaselineUniqueId	08.09m*CM*LISOrganizational.*9*5

Question Requirement: 08.01mNIST80053Organizational.4 / 0169.0

Change Count: 1

Field	Content
BaselineUniqueId	08*07*.01m*CMS*NIST80053Organizational.*1*4

Question Requirement: 10.01dFedRAMPSystem.5 / 2323.0

Change Count: 1

Field	Content
BaselineUniqueId	10.01d*NIST800171*FedRAMPSystem.*1*5

Question Requirement: 16.00aNIST80053Organizational.18 / 2423.1

Change Count: 3

Field	Content
BaselineUniqueId	16.00a*FedRAMP*NIST80053Organizational.1*9*8
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the contingency planning policy and associated cont*ingency planning control*rols. The organization ensures the contingency planning policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the contingency planning policy and procedures. The organization reviews and updates the current contingency planning policy at least annually or whenever a significant change occurs, and contingency planning procedures at least annually or whenever a significant change occurs.
CrossVersionId	2423.*0*1

Question Requirement: 15.00aNIST80053Organizational.29 / 2473.1

Change Count: 3

Field	Content
BaselineUniqueId	15.00a*FedRAMP*NIST80053Organizational.*17*29

RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles an incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the incident response policy and associated *incident response control***controls. The organization ensures the incident response policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the incident response policy and procedure**s. The organization reviews and updates the current incident response policy at least annually*,* and incident response procedures at least annually or whenever a significant change occurs.
CrossVersionId	2473.*0***1**

Question Requirement: 17.00aNIST80053Organizational.22 / 2395.1

Change Count: 3

Field	Content
BaselineUniqueId	17.00a*FedRAMP***NIST80053**Organizational.*8***22**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the risk assessment policy and associated *risk assessment control***controls. The organization ensures the risk assessment policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the risk assessment policy and procedure**s. The organization reviews and updates the current risk assessment policy at least annually*,* and risk assessment procedures at least annually or whenever a significant change occurs.
CrossVersionId	2395.*0***1**

Question Requirement: 1412.09f3System.1 / 0849.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures service reports produced by the third - parties be reviewed, and regular progress meetings are arranged as required by the agreements. The organization ensures third-party audit trails, records of third-party security events, records of third-party operational problems, records of third-party failures, and records of third-party tracing of faults and disruptions related to service delivery are reviewed. Information about information security incidents are provided to the incident response team. This information is reviewed by the third-party that experienced the incident and the organization which the third-party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above.

Question Requirement: 13.02eHIPAAOrganizational.2 / 0342.0

Change Count: 1

Field	Content
BaselineUniqueId	13.02e*NIST80053***HIPAA**Organizational.*6***2**

Question Requirement: 09.10gNYDOHOrganizational.2 / 2468.0

Change Count: 1

Field	Content
BaselineUniqueId	09.10g*CMS***NYDOH**Organizational.2

Question Requirement: 17.03bFFIECCATOrganizational.2 / 0403.0

Change Count: 1

Field	Content
BaselineUniqueId	17*123*.03bFFIEC*IS***CAT**Organizational.2

Question Requirement: 17.03bFFIECCATOrganizational.3 / 0402.0

Change Count: 1

Field	Content
BaselineUniqueId	17*122*.03bFFIEC*IS***CAT**Organizational.*1***3**

Question Requirement: 06.10hNIST80053System.3 / 2202.0

Change Count: 1

Field	Content
BaselineUniqueId	06*230*.10hN*YDOH***IST80053**System.*2***3**

Question Requirement: 09.09vADHICSOrganizational.2 / 1037.0

Change Count: 1

Field	Content
BaselineUniqueId	09.09v*CFRPart11***ADHICS**Organizational.2

Question Requirement: 0911.09s2Organizational.6 / 1052.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of information exchanges with third- parties and confirm that the agreement formally defines terms and conditions for authorized individuals to access the information system from external information systems or process, store or transmit organization-controlled information using external information systems.

Question Requirement: 0816.01w1System.1 / 0244.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of systems and applications and determine if the sensitivity of the system/application rationale is documented and approved by *management***the application/system owner**. Further, examine evidence to confirm that a record of all systems and their sensitivity has been documented.

Question Requirement: 12.09aeNIST800171System.2 / 1212.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09aeNIST800*53***171**System.2

Question Requirement: 11.01jSEC530Organizational.2 / 0136.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01j*NIST800***SEC**53**0**Organizational.*3***2**

Question Requirement: 07.10m1Organizational.3 / 2367.0

Change Count: 2

Field	Content
RequirementStatement	Information systems are *periodically* scanned to proactively *(annually at minimum)* identify technical vulnerabilities **at a frequency based on the organization's formally documented assessment of risk (annually at minimum)**.
IllustrativeProcedureImplemented	For example, select a sample of systems and confirm that they have been proactively scanned for vulnerabilities in accordance with the organization's *defined vulnerability scanning frequency***formally documented assessment of risk** (at a minimum within the past year).

Question Requirement: 07.10m1Organizational.6 / 2317.2

Change Count: 4

Field	Content
BaselineUniqueId	07.10m1Organizational.*2***6**
RequirementStatement	The organization deploys automated software update tools *in order to ensure that systems are running the most recent security updates provided by the software vendor, and installs software updates manually for systems that do not support automated software updat***to apply vendor security updates, installs software updates manually for systems that do not support automated software updates, and installs vendor security updates within formally documented, risk-tiered remediation timefram**es.
IllustrativeProcedureImplemented	For example, select a sample of systems that support automated security updating and confirm that automated security updating is enabled **for vendor security updates**. Further, select a sample of systems that do not support automatic security updating and confirm the organization performs *and tracks* the manual installation of these systems **within formally documented, risk-tiered remediation timeframes**.
CrossVersionId	2317.*1***2**

Question Requirement: 0709.10m1Organizational.8 / 1369.1

Change Count: 5

Field	Content
BaselineUniqueId	0709.10m1Organizational.*1***8**
RequirementStatement	Once a potential technical vulnerability has been identified, the organization identifies the associated risks *and the actions to be taken. Further, the organization performs the necessary actions to correct identified technical vulnerabilities in a timely manner***, determines the appropriate response based on exploitability and severity, and performs the necessary actions to remediate the vulnerability within formally documented, risk-tiered remediation timeframes**.

IllustrativeProcedureImplemented	For example, select a sample of system vulnerabilities identified by the organization and examine evidence to confirm that a risk assessment was performed to identify associated risks. Further, confirm that **the organizac**tion's *plans were identified a***response considered exploitation probability i**nd **i**ca*rried out, such as patching. Confirm that all evidence was formally documented***tors (e.g. EPSS, CISA KEV, or similar threat exploitation advisory) and took into account severity. Additionally, confirm the vulnerability was remediated within the formally documented, risk-tiered remediation timeframe**.
IllustrativeProcedureMeasured	For example, measures indicate the number of technical vulnerabilities in the organization's information systems that have/haven't been corrected, as a percentage all vulnerabilities. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to *verify that***confirm once a potential** technical vulnerabilit*ies are***y has been** identified, *evaluated for***the organization identifies the associated** risk**s**, *and corrected in a timely manner***determines the appropriate response based on exploitability and severity, and performs the necessary actions to remediate the vulnerability within formally documented, risk-tiered remediation timeframes**.
CrossVersionId	1369.*0***1**

Question Requirement: 0778.10m1Organizational.5 / 1398.0

Change Count: 3

Field	**Content**
RequirementStatement	The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been *remediated in a timely manner***effectively remediated within formally documented, risk-tiered remediation timeframes**.
IllustrativeProcedureImplemented	For example, examine evidence t*hat***o confirm** the organization documents and tracks vulnerabilities identified through vulnerability scans. *S***Further, s**elect a sample of vulnerabilities identified through previous scans and confirm whether the vulnerability has been addressed *or***and effectively remediated within a formally documented, risk-tiered remediation timeframe or has been** accepted by management. *Further***Additionally**, select a sample of risks accepted by management and examine formal evidence that acceptance was reviewed on a periodic basis.

IllustrativeProcedureMeasured	For example, measures indicate the number of vulnerability scans that were not followed up with a "back-to-back" scan to ensure vulnerabilities were e*ither addressed or accepted from previous scan***ffectively remediated within formally documented, risk-tiered remediation timeframe**s. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to *verify that* **confirm** the organization **regularly** compares the results from *back-to-back***consecutive** vulnerability scans to verify that vulnerabilities *were addressed either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities are periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk***have been effectively remediated within formally documented, risk-tiered remediation timeframes**.

Question Requirement: 0715.10m1Organizational.7 / 1375.1

Change Count: 4

Field	Content
BaselineUniqueId	0715.10m1Organizational.*4***7**
RequirementStatement	Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.*2***3** or later **or TLS v1.2 with approved cipher suites**, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).
IllustrativeProcedureImplemented	For example, select a sample of systems and review its configuration settings. *C* **and c**onfirm that insecure services, such as NetBIOS, file-sharing, Telnet, FTP, etc. have been disabled. */***Further, i**f any insecure services are enabled, confirm that security features such as SSH, S-FTP, TLS v1.*2***3** or later **or TLS v1.2 with approved cipher suites**, or IPsec VPN have been enabled. *R***Additionally, r**eview of hardened system images can confirm enabled/disabled services, protocols, and daemons.
CrossVersionId	1375.*0***1**

Question Requirement: 14.09eFedRAMPSystem.3 / 2161.0

Change Count: 1

Field	Content
BaselineUniqueId	14*189*.09e*NYDOH***FedRAMP**System.*2***3**

Question Requirement: 14.05kFFIECCATOrganizational.2 / 2909.0

Change Count: 3

Field	Content
RequirementStatement	The standard agreement with third- parties stipulates the geographic limits on where data can be stored or transmitted.
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that geographic limits on where data can be stored or transmitted was stipulated.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of third-party agreements which stipulate geographic limits on where data can be stored or transmitted. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify the standard agreement with third- parties stipulates the geographic limits on where data can be stored or transmitted.

Question Requirement: 15.12eCMSOrganizational.3 / 2241.0

Change Count: 1

Field	Content
BaselineUniqueId	15*269*.12e*NYDOH***CMS**Organizational.*4***3**

Question Requirement: 18.08bFedRAMPOrganizational.3 / 2320.0

Change Count: 1

Field	Content
BaselineUniqueId	18.08b*NIST800171***FedRAMP**Organizational.*1***3**

Question Requirement: 19.13aNYDOHOrganizational.3 / 2290.0

Change Count: 1

Field	Content
BaselineUniqueId	19*317*.13aN*IST80053***YDOH**Organizational.*1***3**

Question Requirement: 19.13aNYDOHOrganizational.2 / 2293.0

Change Count: 1

Field	Content
BaselineUniqueId	19*320*.13aN*IST80053***YDOH**Organizational.2

Question Requirement: 14.10lVAD6500Organizational.2 / 1367.0

Change Count: 1

Field	Content
BaselineUniqueId	14*48*.10l*CMS***VAD6500**Organizational.*1***2**

Question Requirement: 11.01aNIST80053Organizational.4 / 2494.1

Change Count: 3

Field	Content
BaselineUniqueId	11.01a*FedRAMP***NIST80053**Organizational.*1***4**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. **The organization ensures the access control policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.** The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.
CrossVersionId	2494.*0***1**

Question Requirement: 08.01mHICPOrganizational.3 / 1901.0

Change Count: 1

Field	Content
BaselineUniqueId	08.01m*NIST80053***HICP**Organizational.*2***3**

Question Requirement: 11.01qAISecSystem.2 / 3386.0

Change Count: 0

Field	Content
New Question Requirement	11.01qAISecSystem.2 / 3386.0

Question Requirement: 09.09yAISecOrganizational.2 / 3385.0

Change Count: 0

Field	Content
New Question Requirement	09.09yAISecOrganizational.2 / 3385.0

Question Requirement: 08.01wAISecSystem.3 / 3384.0

Change Count: 0

Field	Content
New Question Requirement	08.01wAISecSystem.3 / 3384.0

Question Requirement: 07.10mAISecOrganizational.7 / 3383.0

Change Count: 0

Field	Content
New Question Requirement	07.10mAISecOrganizational.7 / 3383.0

Question Requirement: 12.09abAISecSystem.7 / 3382.0

Change Count: 0

Field	Content
New Question Requirement	12.09abAISecSystem.7 / 3382.0

Question Requirement: 11.01cAISecSystem.10 / 3381.0

Change Count: 0

Field	Content
New Question Requirement	11.01cAISecSystem.10 / 3381.0

Question Requirement: 06.10cAISecSystem.2 / 3380.0

Change Count: 0

Field	Content
New Question Requirement	06.10cAISecSystem.2 / 3380.0

Question Requirement: 11.10eAISecSystem.3 / 3379.0

Change Count: 0

Field	Content
New Question Requirement	11.10eAISecSystem.3 / 3379.0

Question Requirement: 12.09aaOASystem.1 / 3378.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaOASystem.1 / 3378.0

Question Requirement: 1713.03c2Organizational.3 / 0417.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate whether a monitoring process is in place to help management ensure corrective action/mitigation plans are developed pursuant to relevant policies or procedures. For example, the metric could indicate the number of data breaches in which the policy was not followed as a percentage of all reported data breach incidents during a specific time period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization mitigates any harmful effect that is known to the organization of a use or disclosure of PII by the organization or its third-parties, in violation of its policies and procedures.

Question Requirement: 06.00aNIST80053Organizational.17 / 2463.1

Change Count: 3

Field	Content
BaselineUniqueId	06.00a*FedRAMP***NIST80053**Organizational.1*6***7**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the configuration management policy and associated con*figuration management control*trols. **The organization ensures the configuration management policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the configuration management policy and procedure**s. The organization reviews and updates the current configuration management policy at least annually*,* and configuration management procedures at least annually or whenever a significant change occurs.
CrossVersionId	2463.*0***1**

Question Requirement: 14.09tISO27001Organizational.2 / 1073.0

Change Count: 3

Field	Content
BaselineUniqueId	14.09t*DEID***ISO27001**Organizational.*3***2**
IllustrativeProcedureImplemented	For example, select a sample of third- parties where a transfer of business information is required. Confirm that an exchange and data sharing agreement is in place that defines the minimum set of controls and standards to protect information and physical media in transit. Select a sample of physical media in transit and confirm that it was transported in accordance with such exchange agreements.

IllustrativeProcedureMeasured	For example, measures indicate the number of third- parties that transport physical media for the organization where an appropriate exchange agreement is not in place, as a percentage of such third- parties. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization formally manages the protection of information and physical media in transit, and the requirements are referenced in such exchange agreements.

Question Requirement: 01.02c3Organizational.3 / 0317.0

Change Count: 1

Field	Content
BaselineUniqueId	01*52*.02c*23*Organizational.*13*

Question Requirement: 14.05iADHICSOrganizational.2 / 3145.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties and examine evidence to determine if appropriate due diligence procedures were carried out to ensure the third-party did not seek to use the entity's data for their own advantages or requirements.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-parties where appropriate due diligence were performed, as a percent of all third-party agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm due diligence of the third-party ensures they do not seek to use the entity's data for their own advantages or requirements.

Question Requirement: 02.09jLISOrganizational.2 / 0876.0

Change Count: 1

Field	Content
BaselineUniqueId	02.09j*N*LIS*T80053*Organizational.*42*

Question Requirement: 01.05bVAD6500Organizational.2 / 2085.0

Change Count: 1

Field	Content
BaselineUniqueId	01*112*.05b*NYDOH***VAD6500**Organizational.2

Question Requirement: 15.11cADHICSOrganizational.6 / 2220.0

Change Count: 1

Field	Content
BaselineUniqueId	15*248*.11c*NYDOH***ADHICS**Organizational.*2***6**

Question Requirement: 11.01vNIST80053System.3 / 2067.0

Change Count: 1

Field	Content
BaselineUniqueId	11*994*.01vN*YDOH***IST80053**System.*4***3**

Question Requirement: 1402.05i2Organizational.4 / 0500.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select sample of third- parties, which require remote access or transfer of covered information and examine evidence to confirm that remote access connections (e.g., VPN) and transfer of covered information is encrypted (e.g., AES 256).

Question Requirement: 1401.05i2Organizational.3 / 0499.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties and examine evidence to determine if a contract has been signed and maintained, due diligence was performed prior to signing, and acceptance of the adequacy of the controls in place was provided and appropriately reviewed.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-parties where appropriate due diligence and review of security controls were performed prior to the signing of the contract, as a percentage of all third-party agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that access to the organizations information and systems by external parties is not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations.

Question Requirement: 191007.13bCCPAOrganizational.3 / 1933.0

Change Count: 1

Field	Content
RequirementStatement	Businesses that sell information to third- parties disclose in their notices to consumers that they have the right to opt-out.

Question Requirement: 1705.03b2Organizational.2 / 1905.1

Change Count: 4

Field	Content
BaselineUniqueId	1705.03b2Organizational.*1*2
RequirementStatement	A formal, documented process is in place for identifying risks and performing risk assessments. The formal, documented process is in place for identifying risks and performing risk assessments includ***es*****ing**: the criteria for the evaluation; the categorization of risks; communicating the results of the risk assessments to the affected parties*,* and to management. The organization: updates the results of a comprehensive risk assessment every two years; updates the results of a comprehensive risk assessment whenever there is a significant change to the information system or operational environment **and whenever exploitability or threat conditions materially change**; assesses a subset of the security controls within every 365 days during continuous monitoring; reviews the risk assessment results annually. Information security risk assessments require knowledge of: external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously; the types of accounts offered by the organization and the methods the organization provides to open and access its accounts; incident histories and actual case impact scenarios; systems architectures**; and relevant exploitability and threat information**.
IllustrativeProcedureImplemented	For example, examine the results of the most recent comprehensive risk assessment and determine if it occurred within the past two years **or sooner if a significant change occurred to the information system or operational environment or if exploitability or threat conditions materially changed (i.e., a change that is likely to impact the security or privacy posture of the information system)**. Further, examine the risk assessment **to confirm it** included an evaluation of external environmental factors, types of accounts, access methods, system architectures *and*, recent security incidents**, and relevant exploitability and threat information**.
CrossVersionId	1905.*0***1**

Question Requirement: 1807.08b2Organizational.56 / 0706.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of facilities and observe employees, visitors, and third- parties throughout each facility and determine if identification (e.g., badge) is clearly visible. Further, inspect the visitor access log to evidence that visitors are given a badge or access device that identifies them as non-employees and surrender the badge or device before leaving the facility or upon expiration.

IllustrativeProcedureMeasured	For example, measures indicate the percentage of employees and visitors that have appropriately been assigned visible identification in accordance with the organization's policy, as a percentage of all employees and visitors. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that visible identification that clearly identifies the individual is required to be worn by employees, visitors, contractors and third- parties.

Question Requirement: 11.01cAISecSystem.11 / 3387.0

Change Count: 0

Field	Content
New Question Requirement	11.01cAISecSystem.11 / 3387.0

Question Requirement: 02.09mNYDOHOrganizational.8 / 2547.0

Change Count: 1

Field	Content
BaselineUniqueId	02.09m*CMS***NYDOH**Organizational.*5***8**

Question Requirement: 01.02dHICPOrganizational.2 / 2251.0

Change Count: 1

Field	Content
BaselineUniqueId	01*278*.02d*DGF***HICP**Organizational.*1***2**

Question Requirement: 15.11cSEC530Organizational.3 / 1471.0

Change Count: 1

Field	Content
BaselineUniqueId	15*50*.11c*CMS***SEC530**Organizational.*2***3**

Question Requirement: 12.09abNYDOHSystem.9 / 2572.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09ab*CMS***NYDOH**System.*6***9**

Question Requirement: 1414.09g1System.1 / 0853.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of service agreements and confirm that requirements have been formally defined for third-parties to use appropriate change management procedures defined by the organization. Select a sample of changes to a third-party service or organizational system and confirm that the change was compliant with the procedures defined by the third-party and the organization.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of changes to a third-party service or organizational system that are compliant/non-compliant with the organization's change management policy and procedures. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that third- parties coordinate, manage, and communicate changes to the services they provide to the organization.

Question Requirement: 0226.09k1Organizational.2 / 0896.0

Change Count: 3

Field	Content
RequirementStatement	The organization implements and regularly updates mobile code protection, including anti-*virus and anti-spy***mal**ware.
IllustrativeProcedureImplemented	For example, select a sample of endpoint devices (desktops, laptops, servers, BYOD, etc.)*, determine if* **and examine evidence to confirm** anti-malware software is installed, operating and up-to-date and that it protects against mobile code. *E***Further, e**xamine the configuration settings for the anti-malware software and confirm that definition files are automatically downloaded and pushed out to clients when updates are available.
IllustrativeProcedureMeasured	For example, measures indicate the number of endpoint devices (desktops, laptops, servers, etc.) that appropriately have anti-malware software installed and protect against mobile code, as a percentage of all endpoint devices. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization implements and regularly updates mobile code protection, including anti-*virus and anti-spy***mal**ware.

Question Requirement: 06.09b1System.2 / 2368.1

Change Count: 3

Field	Content
RequirementStatement	Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, **risk-assessed, security-**tested, and approved.

IllustrativeProcedureImplemented	For example, select a sample of **all** changes made to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) and confirm that they were documented, *tested* **risk-assessed (i.e. provided a classification based on factors such as criticality of services/systems affected by the change) against a formally documented change-risk methodology, security-tested (e.g., using risk-appropriate vulnerability scanning, configuration validation, secure code review, or regression testing)**, and approved.
CrossVersionId	2368.*0***1**

Question Requirement: 17.07dISO27001Organizational.2 / 0657.0

Change Count: 1

Field	Content
BaselineUniqueId	17.07d*N*IS*T80053***O27001**Organizational.*4***2**

Question Requirement: 11.01qFFIECCATSystem.2 / 0219.0

Change Count: 1

Field	Content
BaselineUniqueId	11*115*.01q*CMS***FFIECCAT**System.*4***2**

Question Requirement: 11.01INIST80053Organizational.5 / 0154.0

Change Count: 1

Field	Content
BaselineUniqueId	11*99*.01I*CMS***NIST80053**Organizational.*2***5**

Question Requirement: 06.10hAISecSystem.6 / 3045.0

Change Count: 2

Field	Content
RequirementStatement	Documentation of the overall AI system discusses the creation, operation, and lifecycle management of any models, datasets (including data used for training, tuning, and prompt enhancement via RAG), configurations (e.g., metaprompts), *language model tools such as agents***agents, skills,** and plugins maintained by the organization, as applicable. Documentation of the overall AI system also describes the tooling resources (e.g., AI platforms, model engineering environments), system and computing resources, and human resources needed for the development and operation of the AI system.

IllustrativeProcedureImplemented	For example, review the overall AI system documentation to confirm it discusses the creation, operation, and lifecycle management of any models, datasets (including data used for training, tuning, and prompt enhancement via RAG), configurations (e.g., metaprompts), *language model tools such as agents***agents, skills,** and plugins maintained by the organization, as applicable. Further, confirm the documentation of the overall AI system also describes the tooling resources (e.g., AI platforms, model engineering environments), system and computing resources, and human resources needed for the development and operation of the AI system.

Question Requirement: 06.10hAISecSystem.5 / 3044.0

Change Count: 3

Field	Content
RequirementStatement	Changes to language model tools such as agents**, skills,** and plugins are consistently documented, tested, and approved in accordance with the organization's software change control policy prior to deployment.
IllustrativeProcedureImplemented	For example, select a sample of the language model **tool** change documentation to confirm all changes were documented. Further, confirm that the language model **tool** change documentation includes testing and approval information in accordance with the organization's software change control policy, prior to deployment.
IllustrativeProcedureMeasured	For example, measures indicate percentage of the organization's language model **tools** that received changes without documentation. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all language model **tool** changes are consistently documented, tested, and approved in accordance with the organization's software change control policy prior to deployment.

Question Requirement: 06.06hPCIOrganizational.2 / 0616.0

Change Count: 1

Field	Content
BaselineUniqueId	06.06h*NIST80053***PCI**Organizational.*3***2**

Question Requirement: 14.05i1Organizational.3 / 3207.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures all third- parties with access to the organization's information or information systems meet contractual commitments for information security. The organization reviews independent assessments or independent verifications of all third- parties with access to its information or information systems to determine compliance with contract provisions (e.g. security certification, attestation, audit report, or verification) at least annually.

Question Requirement: 19446.13kHIPAAOrganizational.38 / 1774.1

Change Count: 3

Field	Content
BaselineUniqueId	19446.13kHIPAAOrganizational.*1*38
RequirementStatement	Unless the organization is an issuer of long-term care policies, requirements have been defined for ensuring the health plan does not use or disclose PHI that is genetic information for underwriting purposes. *The organization or business associate will not sell PHI.*
CrossVersionId	1774.*0*1

Question Requirement: 14.09eC5System.1 / 3177.0

Change Count: 3

Field	Content
RequirementStatement	The cloud service provider's standard agreement with third-parties includes obligations to make third-party employees and subcontractors aware of the specific security requirements of the cloud provider and train third-party employees generally in the subject of information security.
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the related third-party agreements to confirm the elements stipulated in the requirement statement were defined and included in the agreement.
IllustrativeProcedureMeasured	For example, the measures could indicate the percentage of the cloud service provider's agreements with third- parties which contain the identified security requirements. Reviews, tests, or audits are completed by the cloud service provider to measure the effectiveness of the implemented controls and to confirm the cloud service provider's standard agreement with third- parties includes obligations to make third-party employees and subcontractors aware of the specific security requirements of the cloud provider and train third-party employees generally in the subject of information security.

Question Requirement: 19.13INYDOHOrganizational.3 / 2674.0

Change Count: 1

Field	Content
BaselineUniqueId	19.13l*CMS***NYDOH**Organizational.*1***3**

Question Requirement: 17.03aSEC530Organizational.2 / 0390.0

Change Count: 1

Field	Content
BaselineUniqueId	17*114*.03a*DEID***SEC530**Organizational.*1***2**

Question Requirement: 19.06dADHICSOrganizational.4 / 3139.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine the organization's system/network diagram and confirm the cloud environment was physically hosted within the UAE. Further, select a sample of third-parties the organization has extended access to and examine their associated access rights to confirm that they were unable to access data stored in the cloud environment from outside of the UAE.

Question Requirement: 02.10bNIST80053System.3 / 3361.0

Change Count: 0

Field	Content
New Question Requirement	02.10bNIST80053System.3 / 3361.0

Question Requirement: 18.08dNIST80053Organizational.3 / 3360.0

Change Count: 0

Field	Content
New Question Requirement	18.08dNIST80053Organizational.3 / 3360.0

Question Requirement: 01.01bNIST80053System.2 / 3359.0

Change Count: 0

Field	Content
New Question Requirement	01.01bNIST80053System.2 / 3359.0

Question Requirement: 01.01bNIST80053System.1 / 3358.0

Change Count: 0

Field	Content
New Question Requirement	01.01bNIST80053System.1 / 3358.0

Question Requirement: 01.01aNIST80053Organizational.5 / 3357.0

Change Count: 0

Field	Content
New Question Requirement	01.01aNIST80053Organizational.5 / 3357.0

Question Requirement: 12.09aaNIST80053System.10 / 3356.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaNIST80053System.10 / 3356.0

Question Requirement: 12.09aaNIST80053System.9 / 3355.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaNIST80053System.9 / 3355.0

Question Requirement: 12.09aaNIST80053System.8 / 3354.0

Change Count: 0

Field	Content
New Question Requirement	12.09aaNIST80053System.8 / 3354.0

Question Requirement: 01.02dADHICSOrganizational.1 / 3353.0

Change Count: 0

Field	Content
New Question Requirement	01.02dADHICSOrganizational.1 / 3353.0

Question Requirement: 01.09aFFIECCATSystem.2 / 0816.0

Change Count: 1

Field	Content
BaselineUniqueId	01.09a*NIST80053***FFIECCAT**System.2

Question Requirement: 01.05dFedRAMPOrganizational.3 / 2091.0

Change Count: 1

Field	Content
BaselineUniqueId	01*118*.05d*NYDOH***FedRAMP**Organizational.*2***3**

Question Requirement: 01.05bNYDOHOrganizational.4 / 0463.0

Change Count: 1

Field	Content
BaselineUniqueId	01.05bN*IST80053***YDOH**Organizational.*3***4**

Question Requirement: 06.10kFFIECCATOrganizational.3 / 1356.0

Change Count: 1

Field	Content
BaselineUniqueId	06.10k*CMS***FFIECCAT**Organizational.*11***3**

Question Requirement: 08.09mPCIOrganizational.3 / 0940.0

Change Count: 1

Field	Content
BaselineUniqueId	08.09m*NIST80053***PCI**Organizational.*6***3**

Question Requirement: 08.09mHICPOrganizational.5 / 1958.0

Change Count: 1

Field	Content
BaselineUniqueId	08*923*.09m*NIST80053***HICP**Organizational.*2***5**

Question Requirement: 07.10mNIST800172Organizational.6 / 1389.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10mNIST800*53***172**Organizational.*4***6**

Question Requirement: 0706.10b1System.2 / 1263.3

Change Count: 4

Field	Content
RequirementStatement	The organization develops applications *based on***in accordance with** secure coding guidelines to prevent*:* common**,** co*ding vulnerabilities in software development processes; injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); buffer overflow (Validate buffer boundaries and truncate input strings); insecure cryptographic storage (Prevent cryptographic flaws); insecure communications (Properly encrypt all authenticated and sensitive communications); improper error handling (Do not leak information via error messages); broken* **mplex, and context-dependent coding vulnerabilities, including those associated with injection flaws, buffer overflow, insecure cryptographic storage, insecure communications, improper error handling,** authentication*/* **and** session*s (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user); cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and any other input-validation vulnerability listed in the OWASP Top 10* **management weaknesses, cross-site scripting (XSS), access control, and any other weakness addressed by OWASP**.
IllustrativeProcedureImplemented	For example, obtain and examine the secure coding guidelines *and determine***to confirm** if methods for preventing common**, complex, and context-dependent** vulnerabilities (e.g., injection flaws, buffer overflow, insecure cryptographic **storage** and communications, improper error handling**, authentication and session management weaknesses, cross-site scripting (XSS), access control, and any other weakness addressed by OWASP**) are identified and defined.
IllustrativeProcedureMeasured	For example, measures indicate the number of organization developed applications that are developed according to secure coding guidelines, as a percentage of all organization developed applications. Further, the metric could include the number of common**, complex, and context-dependent** coding vulnerabilities identified as part of development or annual testing. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that applications developed by the organization are based on secure coding guidelines to prevent *common vulnerabilities, or undergo appropriate testing* **preventing common, complex, and context-dependent vulnerabilities**.
CrossVersionId	1263.*1***3**

Question Requirement: 1218.09ab3System.8 / 1157.1

Change Count: 5

Field	Content
BaselineUniqueId	1218.09ab3System.*47***8**
RequirementStatement	Automated tools support near real-time analysis of events and maintain an audit log to track prohibited sources and services. Information systems provide near real-time alerts for the presence of malicious code, unauthorized export of information, signaling to an external information system, *or* potential intrusions**, and indicators of exploitation of technical vulnerabilities**.
IllustrativeProcedureImplemented	For example, examine evidence that the organization has implemented audit and monitoring solutions to support near real-time analysis of events, which include the presence of malicious code, unauthorized export of information, signaling to an external information system, *or* potential intrusions**, or indicators of exploitation of technical vulnerabilities (e.g. repeated requests containing exploit strings or payload patterns such as SQL injection syntax, unexpected process execution after a service request, authentication or privilege anomalies immediately following vulnerability activity)**. This can be confirmed through examination of automated mechanisms, such as DLP, SIEM, IPS, and IDS to confirm the systems are configured to perform real-time (or near real-time) analysis.
IllustrativeProcedureMeasured	For example, measures indicate the percentage information systems that has implemented automated tools to support near real-time analysis of events, along with the percentage of systems that are not being monitored. A further measure could indicate the number of alerts generated based on the real-time analysis of the audit and monitoring solution. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that automated systems support near real-time analysis and alerting of events (e.g., malicious code, potential intrusions**, indicators of exploitation of technical vulnerabilities**) and integrate intrusion detection into access and flow control mechanisms.
CrossVersionId	1157.*0***1**

Question Requirement: 1216.09ab3System.12 / 1155.0

Change Count: 3

Field	Content
RequirementStatement	Automated systems are used to review monitoring activities on a daily basis for those servers that perform security functions (e.g., IDS/IPS) for: all security events; logs of all critical system components; and logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). System records are reviewed daily for initialization sequences, log-ons and errors, system processes and performance, and system resources utilization. The results of system record reviews are used to determine anomalies **and indicators of exploitation** on demand.
IllustrativeProcedureImplemented	For example, examine evidence that the organization has implemented automated audit log and monitoring solutions (e.g., SIEM, IDS/IPS, etc.) to monitor the following: (i) all security events; (ii) logs of all critical system components; (iii) logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS); and, (iv) system records are reviewed daily for initialization sequences, log-ons and errors, system processes and performance, and system resources utilization, and the results are used to determine anomalies **and indicators of exploitation (e.g. repeated requests containing exploit strings or payload patterns such as SQL injection syntax, unexpected process execution after a service request, authentication or privilege anomalies immediately following vulnerability activity)** on demand.
IllustrativeProcedureMeasured	For example, measures indicate the percentage servers that perform security functions that are monitored and reviewed using automated tools, along with servers that do not meet this requirement. A further measure could indicate the number of anomalies detected as part of the daily review of system records. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls *and***,** to confirm that automated systems are used to review monitoring activities of security systems (e.g., IPS/IDS) and system records on a daily basis, and **to** identify and document anomalies **and indicators of exploitation**.

Question Requirement: 1219.09ab3System.9 / 1161.1

Change Count: 5

Field	Content
BaselineUniqueId	1219.09ab3System.*10***9**
RequirementStatement	The information system is able to automatically process audit records for events of interest**, including indicators of technical vulnerability exploitation,** based on selectable criteria.

IllustrativeProcedureImplemented	For example, examine the audit log server/database/software configuration and examine evidence to confirm that auditing can be performed on defined information system components based on defined selectable event criteria. Events of interest**, including indicators of technical vulnerability exploitation (e.g. repeated requests containing exploit strings or payload patterns such as SQL injection syntax, unexpected process execution after a service request, authentication or privilege anomalies immediately following vulnerability activity),** can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. Examine evidence to confirm that the organization has implemented automated tools to automatically process audit records, such as SIEM and DLP) on various information systems.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of system audit records that automatically processed based on defined selectable event criteria, along with the percentage of audit records that are not processed automatically. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the information system is able to automatically process audit records for events of interest**, including indicators of technical vulnerability exploitation,** based on selectable criteria.
CrossVersionId	1161.*0***1**

Question Requirement: 11.01qFTISystem.9 / 0222.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01q*NIST80053***FTI**System.*6***9**

Question Requirement: 11.01qNYDOHSystem.10 / 2314.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01qN*IST80053***YDOH**System.*2***10**

Question Requirement: 11.11aHIPAAOrganizational.12 / 1923.0

Change Count: 1

Field	Content
BaselineUniqueId	11*1015.11aCCP*.**11aHIPA**AOrganizational.1**2**

Question Requirement: 11.01cAISecSystem.9 / 3058.0

Change Count: 3

Field	Content
RequirementStatement	The organization restricts all access to AI engineering environments; code used to create, train, and/or deploy AI models; and code of *language model tools such as agents* **agents, skills,** and plugins (if used) following the least privilege principle. This access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews), and authentication (which calls for multi-factor authentication or a similar level of protection).
IllustrativeProcedureImplemented	For example, review the AI system to ensure the organization restricts all access to AI engineering environments; code used to create, train, and/or deploy AI models; and code of *language model tools such as agents***agents, skills,** and plugins (if used) following the least privilege principle. Further, confirm this access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews) and authentication (which calls for multi-factor authentication or a similar level of protection).
IllustrativeProcedureMeasured	For example, measures indicate if the organization restricts all access to AI engineering environments; code used to create, train, and/or deploy AI models; and code of *language model tools such as agents***agents, skills,** and plugins (if used) following the least privilege principle. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that access is controlled in accordance with the organization's policies regarding access management (including approvals, revocations, periodic access reviews) and authentication (which calls for multi-factor authentication or a similar level of protection).

Question Requirement: 1270.09ad1System.2 / 1216.1

Change Count: 5

Field	Content
BaselineUniqueId	1270.09ad1System.*1*2
RequirementStatement	The organization ensures *that* proper logging is enabled in order to audit **operator and** administrator activities. *The organization ensur* **and detect indicators of exploitation of technical vulnerabilitie**s, system administrator logs a*nd operator logs are reviewed on a regular bas***re reviewed at a formally documented frequency based on an assessment of risk, and system operator logs are reviewed at a formally documented frequency based on an assessment of risk**.

IllustrativeProcedureImplemented	For example, select a sample of systems and confirm that operator and system administrator activity is logged. This can be confirmed through review of the audit logs generated. Further, select a sample of audit log reviews to confirm that system administrator and operator logs are reviewed on a *regular basis***formally documented frequency based on an assessment of risk to detect indicators of exploitation of technical vulnerabilities (e.g. repeated requests containing exploit strings or payload patterns such as SQL injection syntax, unexpected process execution after a service request, authentication or privilege anomalies immediately following vulnerability activity)**.
IllustrativeProcedureMeasured	For example, measures indicate the number of organization systems where operator and system administrator activity is not logged, as a percentage of all systems. A further metric could indicate the number of system administrator and operator activities that are not reviewed, as a percentage of such activities. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization ensures proper logging is enabled in order to audit **operator and** administrator activities*;* and *system administrator and operator logs are reviewed on a regular bas***detect indicators of exploitation of technical vulnerabilities, system administrator logs are reviewed at a formally documented frequency based on an assessment of risk, and system operator logs are reviewed at a formally documented frequency based on an assessment of risk**.**
CrossVersionId	1216.*0***1**

Question Requirement: 1563.11d1Organizational.2 / 1490.0

Change Count: 3

Field	**Content**
RequirementStatement	The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises**, including for incidents involving exploitation of technical vulnerabilities**. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.
IllustrativeProcedureImplemented	For example, select a sample of information security incidents and confirm that the organization performed an assessment to identify information gained and lessons learned from the evaluations. *E***Further, e**xamine evidence to confirm the organization subsequently incorporated lessons learned into incident response procedures, training, and testing exercises, **including for incidents involving exploitation of technical vulnerabilities,** and implements the resulting changes accordingly.

IllustrativeProcedureMeasured	For example, measures indicate the number of security incidents where the organization did not evaluated incident to obtain lessons learned, as a percentage of all information security incidents. Further, the measure could indicate the number of information security incidents where lessons learned were evaluated but not incorporated into incident response procedures and training and testing exercises, as a percentage of all information security incidents. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, training, and testing exercises, **including for incidents involving exploitation of technical vulnerabilities,** and implements the resulting changes accordingly.

Question Requirement: 1560.11d1Organizational.1 / 1487.0

Change Count: 3

Field	Content
RequirementStatement	The information gained from the evaluation of information security incidents is used to identify recurring *or*, high-impact**, or vulnerability-exploitation-related** incidents, and update the incident response and recovery strategy.
IllustrativeProcedureImplemented	For example, select a sample of information security incidents and confirm that the organization performed an assessment to identify information gained and lessons learned from the evaluations. *E***Further, e**xamine evidence to confirm that the organization has implemented mechanisms, (e.g., manual, or automated) to help identify *high-impact***recurring, high-impact, or vulnerability-exploitation-related** incidents, monitor, and quantify the types, volumes, and costs of information security incidents.
IllustrativeProcedureMeasured	For example, measures indicate the number of recurring *or*, high-impact**, or vulnerability-exploitation-related** incidents identified and evaluated, as a percentage of all information security incidents. Further, the measure could indicate the number of information security incidents that are not being monitored in order to quantify the types, volumes, and costs, as a percentage of all information security incidents. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the information gained from the evaluation of information security incidents is used to identify recurring *or*, high-impact**, or vulnerability-exploitation-related** incidents, and update the incident response and recovery strategy.

Question Requirement: 15.11aNYDOHOrganizational.5 / 1443.0

Change Count: 1

Field	Content
BaselineUniqueId	15*79*.11a*DEID***NYDOH**Organizational.*2***5**

Question Requirement: 19.05iCMSOrganizational.2 / 2100.0

Change Count: 1

Field	Content
BaselineUniqueId	19*127*.05i*NYDOH***CMS**Organizational.*1***2**

Question Requirement: 08.01wAISecSystem.2 / 3389.0

Change Count: 0

Field	Content
New Question Requirement	08.01wAISecSystem.2 / 3389.0

Question Requirement: 13.02eOAOrganizational.1 / 3377.0

Change Count: 0

Field	Content
New Question Requirement	13.02eOAOrganizational.1 / 3377.0

Question Requirement: 06.09iOASystem.1 / 3376.0

Change Count: 0

Field	Content
New Question Requirement	06.09iOASystem.1 / 3376.0

Question Requirement: 09.09yOAOrganizational.1 / 3375.0

Change Count: 0

Field	Content
New Question Requirement	09.09yOAOrganizational.1 / 3375.0

Question Requirement: 15.10mOAOrganizational.1 / 3374.0

Change Count: 0

Field	Content
New Question Requirement	15.10mOAOrganizational.1 / 3374.0

Question Requirement: 11.01cOASystem.2 / 3373.0

Change Count: 0

Field	Content
New Question Requirement	11.01cOASystem.2 / 3373.0

Question Requirement: 07.10bOASystem.1 / 3372.0

Change Count: 0

Field	Content
New Question Requirement	07.10bOASystem.1 / 3372.0

Question Requirement: 11.01cOASystem.1 / 3371.0

Change Count: 0

Field	Content
New Question Requirement	11.01cOASystem.1 / 3371.0

Question Requirement: 12.09abOASystem.1 / 3370.0

Change Count: 0

Field	Content
New Question Requirement	12.09abOASystem.1 / 3370.0

Question Requirement: 15.11cOAOrganizational.1 / 3369.0

Change Count: 0

Field	Content
New Question Requirement	15.11cOAOrganizational.1 / 3369.0

Question Requirement: 19.13kHIPAAOrganizational.38 / 3368.0

Change Count: 0

Field	Content
New Question Requirement	19.13kHIPAAOrganizational.38 / 3368.0

Question Requirement: 06.10kNIST80053Organizational.4 / 3367.0

Change Count: 0

Field	Content
New Question Requirement	06.10kNIST80053Organizational.4 / 3367.0

Question Requirement: 12.09abNIST80053System.9 / 3366.0

Change Count: 0

Field	Content
New Question Requirement	12.09abNIST80053System.9 / 3366.0

Question Requirement: 09.09sNIST80053Organizational.4 / 3365.0

Change Count: 0

Field	Content
New Question Requirement	09.09sNIST80053Organizational.4 / 3365.0

Question Requirement: 06.13aNIST80053Organizational.4 / 3364.0

Change Count: 0

Field	Content
New Question Requirement	06.13aNIST80053Organizational.4 / 3364.0

Question Requirement: 06.13aNIST80053Organizational.3 / 3363.0

Change Count: 0

Field	Content
New Question Requirement	06.13aNIST80053Organizational.3 / 3363.0

Question Requirement: 01.01pNIST80053System.3 / 3362.0

Change Count: 0

Field	Content
New Question Requirement	01.01pNIST80053System.3 / 3362.0

Question Requirement: 03.09qCMSOrganizational.3 / 2177.0

Change Count: 1

Field	Content
BaselineUniqueId	03*205*.09q*NYDOH***CMS**Organizational.*4***3**

Question Requirement: 06.09bLISSystem.3 / 0820.0

Change Count: 1

Field	Content
BaselineUniqueId	06.09b*N***L**IS*T800171*System.3

Question Requirement: 09.09sFTIOrganizational.6 / 1060.0

Change Count: 1

Field	Content
BaselineUniqueId	09*17*.09s*CMS***FTI**Organizational.*1***6**

Question Requirement: 10.01dNYDOHSystem.3 / 2608.0

Change Count: 1

Field	Content
BaselineUniqueId	10.01d*CMS***NYDOH**System.*7***3**

Question Requirement: 19922.06f1Organizational.2 / 1954.1

Change Count: 3

Field	Content
RequirementStatement	The encryption policy addresses the type and strength of the encryption algorithm *and when*, **including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms, and when encryption should be** used to protect the confidentiality of information. The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards.
IllustrativeProcedureImplemented	For example, but not limited to, obtain and examine the encryption policy and procedures, and examine evidence to confirm that the organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards when used to protect the confidentiality of information. **Further, inspect the encryption policy and procedures and confirm consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms were documented.**
CrossVersionId	1954.*0***1**

Question Requirement: 19522.13r1Organizational.2 / 1873.0

Change Count: 2

Field	Content
RequirementStatement	Requirements for the use of subcontractors to process PII is specified in the contract between the PII processor and the PII controller. PII controllers and PII processors agree via contractual means that PII is not shared with third- parties without advanced notice, unless specifically permitted in the contract. A confidentiality clause is included, binding both upon the provider and any of its employees with access the PII.
IllustrativeProcedureMeasured	For example, measures indicate the number of times PII is shared with third- parties without advanced notices over a specific time-period.

Question Requirement: 11.02iTXRAMPOrganizational.3 / 2392.0

Change Count: 1

Field	Content
BaselineUniqueId	11.02i*CMS***TXRAMP**Organizational.*2***3**

Question Requirement: 11.01pSEC530System.2 / 2517.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01p*CMS***SEC530**System.*3***2**

Question Requirement: 1444.09t1Organizational.12 / 1072.0

Change Count: 3

Field	Content
RequirementStatement	Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions. The exchange and data sharing agreements also specify organization policies including: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys **or quantum-resistant cryptographic mechanisms**; and escrow agreements.

IllustrativeProcedureImplemented	For example, select a sample of third- parties where a transfer of business information is required*. C* **and c**onfirm that an exchange and data sharing agreement is in place that defines the minimum set of controls on responsibility, procedures, technical standards, and solutions. Further, examine the exchange agreement and confirm that the agreement also specifies the organization's policies which include the following: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys **or quantum-resistant cryptographic mechanisms**; and escrow agreements.
IllustrativeProcedureMeasured	For example, measures indicate the number of third- parties where a transfer of business information is required which do not have an appropriate exchange agreement in place, as a percentage of such third- parties. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that exchange agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions, as well as organizational policies.

Question Requirement: 1561.11c1Organizational.3 / 1488.1

Change Count: 5

Field	**Content**
BaselineUniqueId	1561.11c1Organizational.*4***3**
RequirementStatement	The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); *procedures* defin*ing***ed** roles and responsibilities; incident handling procedures (business and technical); communication*; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation)* **and escalation procedures; reporting and retention requirements; and coordination with the organization's vulnerability management, security monitoring, and forensic capabilities**.

IllustrativeProcedureImplemented	For example, examine the organization's incident response and handling policy and confirm that procedures have been defined and documented and includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). *C***Further, confirm c** omponents of the incident handling capability include: policy (setting corporate direction) and procedures defining roles and responsibilities; incident handling procedures (business and technical); communication*; reporting and retention; and references* **and escalation procedures; reporting and retention requirements; and coordinates with** the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation *). S***, security monitoring). Additionally, s**elect a sample of security incidents, and confirm that they were handled in accordance with the organization's incident handling capability. For example, incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Examine evidence to confirm that effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function).
IllustrativeProcedureMeasured	For example, measures indicate the number of security incidents that were not appropriately handed in accordance with the organization's policies, as a percentage of all security incidents. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization implements an incident handling capability for security incidents that address *es (i)***: a** policy (setting corporate direction) *and procedures***;** defin*ing***ed** roles and responsibilities; *(ii)* incident handling procedures (business and technical); *(iii)* communication*; (iv) reporting and retention; and (v) references to a vulnerability management program* **and escalation procedures; reporting and retention requirements; and coordination with the organization's vulnerability management, security monitoring, and forensic capabilities**.
CrossVersionId	1488.*0***1**

Question Requirement: 1589.11c1Organizational.4 / 1462.1

Change Count: 5

Field	**Content**
BaselineUniqueId	1589.11c1Organizational.*5***4**
RequirementStatement	The organization tests and/or exercises its incident response capability *regularly***at least annually, and more frequently based on a formally documented assessment of risk, for scenarios identified in the organization's documented risk assessment (e.g., the exploitation of technical vulnerabilities)**.

IllustrativeProcedureImplemented	For example, obtain and examine the incident response testing policy and procedures and examine evidence to confirm that it defines the frequency of testing **based on a formally documented assessment of risk but is at least annually**, tests the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency, and documents the results of incident response tests/exercises. *S* **Further, s**elect a sample of tests performed by the organization, and through review of the results confirm that the test *met all requirements as stipulated in the requirement state* **includes all scenarios identified in the organization's documented risk assess**ment.
IllustrativeProcedureMeasured	For example, measures indicate the number of incident response tests and exercises 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 that the organization test**s** and/or exercise its incident response capability *regularly* **at least annually, and more frequently based on a formally documented assessment of risk, for scenarios identified in the organization's documented risk assessment (e.g., the exploitation of technical vulnerabilities)**.
CrossVersionId	1462.*0***1**

Question Requirement: 19.06dPHIPAOrganizational.2 / 2109.0

Change Count: 1

Field	Content
BaselineUniqueId	19*136*.06d*NYDOH***PHIPA**Organizational.*5***2**

Question Requirement: 19.06dCMSOrganizational.3 / 2107.0

Change Count: 1

Field	Content
BaselineUniqueId	19*134*.06d*NYDOH***CMS**Organizational.*9***3**

Question Requirement: 06.10jAISecSystem.1 / 3041.0

Change Count: 1

Field	Content
RequirementStatement	AI assets, including code to create, train, and/or deploy AI models; training datasets; fine-tuning datasets; RAG datasets (if used); configurations of pipelines used to create, train, and/or deploy AI models; code used by *language model tools such as agents***agents, skills,** and plugins (if used); and models are versioned and tracked.

Question Requirement: 08.01oSEC530Organizational.2 / 1980.0

Change Count: 1

Field	Content
BaselineUniqueId	08*946*.01o*NIST800***SEC**53**0**Organizational.*1***2**

Question Requirement: 09.09sADHICSOrganizational.2 / 1051.0

Change Count: 2

Field	Content
BaselineUniqueId	09.09s*NIST80053***ADHICS**Organizational.*7***2**
IllustrativeProcedureImplemented	For example, select a sample of information exchanges with third- parties and confirm that information exchange requirements have been defined and that all requirements as stipulated in the requirement statement are implemented and operating effectively.

Question Requirement: 1189.01jPCIOrganizational.1 / 0144.0

Change Count: 2

Field	Content
RequirementStatement	The organization incorporates multi-factor authentication for remote access originating from outside the network by personnel (including users and administrators) and all third-parties (including vendor access for support and maintenance).
IllustrativeProcedureMeasured	For example, measures indicate the number or percentage of remote users that are compliant/non-compliant with the organization's policy to ensure that remote access requires multi-factor authentication. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization incorporates multi-factor authentication for remote access originating from outside the network by personnel (including users and administrators) and all third- parties (including vendor access for support and maintenance).

Question Requirement: 07.10mNYDOHOrganizational.8 / 1412.0

Change Count: 1

Field	Content
BaselineUniqueId	07*85*.10m*FFIECIS***NYDOH**Organizational.*1***8**

Question Requirement: 07.06hAISecOrganizational.1 / 3036.0

Change Count: 2

Field	Content
RequirementStatement	The organization performs security assessments (e.g., AI red teaming, penetration testing) of the AI system which include consideration of AI-specific security threats (e.g., poisoning, model inversion**, goal override**) prior to deployment of new models, prior to deployment of new or significantly modified supporting infrastructure (e.g., migration to a new cloud-based AI platform), regularly (at least annually) thereafter. The organization takes appropriate risk treatment measures (including implementing any additional countermeasures) deemed necessary based on the results.
IllustrativeProcedureImplemented	For example, select a sample of security reports to confirm that security assessments (e.g., AI red teaming, penetration testing) of the AI system which include consideration of AI-specific security threats (e.g., poisoning, model inversion**, goal override**), are conducted at least annually. Further, confirm that assessments are conducted prior to deployment of new and/or changed models, and that appropriate risk treatment measures (including implementing any additional countermeasures) deemed necessary based on the results, are implemented.

Question Requirement: 0701.07a1Organizational.6 / 0626.3

Change Count: 4

Field	Content
BaselineUniqueId	0701.07a1Organizational.*7***6**
RequirementStatement	The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; *and* approved bring your own device (BYOD) equipment**; and cryptographic asset inventory components (e.g., algorithms, protocols, certificates, keys, and cryptographic libraries)**.

IllustrativeProcedureImplemented	For example, examine evidence to confirm that an inventory of all assets (e.g., spreadsheet, database) and services, including information is documented. *C***Further, c**onfirm that the inventory for each asset includes all systems and system components (e.g. desktops, servers, network equipment, printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, mobile phones, tablets, laptops, BYOD equipment, and *other portable electronic device***cryptographic asset inventory component** s) connected to the network and the network devices themselves.
CrossVersionId	0626.*1***3**

Question Requirement: 0704.07a1Organizational.9 / 0633.2

Change Count: 2

Field	Content
RequirementStatement	The asset inventory includes the: unique identifier and/or serial number of the IT asset; information system of which the component is a part; type of information system component (e.g., server, desktop, application); manufacturer/model information of the IT asset; operating system type *and***,** version */service pack***, build/release, and patch** level of the IT asset; presence of virtual machines; application software version/license information; physical location (e.g., building/room number) of the IT asset; logical location (e.g., IP address, position with the IS architecture) of the IT asset; Media access control (MAC) address of the IT asset; data ownership and custodian by position and role; operational status of the IT asset; primary and secondary administrators of the IT asset; and primary user of the IT asset.
IllustrativeProcedureImplemented	For example, select a sample of assets from the asset inventory and confirm that it includes the required information as noted within the requirement statement (e.g., unique identifier, which component, etc.). *C***Further, c**onfirm that this information is accurate and current.

Question Requirement: 11.01cNIST80053System.3 / 2040.0

Change Count: 1

Field	Content
BaselineUniqueId	11*967*.01cN*YDOH***IST80053**System.*63*

Question Requirement: 17.03bNYDOHOrganizational.6 / 0397.0

Change Count: 1

Field	Content
BaselineUniqueId	17*19*.03b*CMS***NYDOH**Organizational.*123***6**

Question Requirement: 11.01jNYDOHOrganizational.4 / 0134.0

Change Count: 1

Field	Content
BaselineUniqueId	11*81*.01j*CMS***NYDOH**Organizational.*1***4**

Question Requirement: 11.01eFedRAMPSystem.2 / 0101.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01e*NIST800171***FedRAMP**System.*3***2**

Question Requirement: 11.01bPCISystem.3 / 2538.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01b*CMS***PCI**System.3

Question Requirement: 0633.10j1System.1 / 1329.0

Change Count: 3

Field	Content
RequirementStatement	Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) are strictly controlled, in order to prevent the introduction of unauthorized functionality *and to avoi***, security-impacting changes, an**d unintentional changes.
IllustrativeProcedureImplemented	For example, *any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Access restrictions for change also include software libraries. C***c**onfirm that access restrictions have been implemented to strictly control access to program source code. This can include, for example, physical and logical access controls to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems). **Any changes to the hardware, software, and/or firmware components of information systems (i.e. role requirement changes, hard-coded bypasses, and password complexity rule changes) can potentially have significant effects on the overall security of the systems. Access restrictions for change also include software libraries.**

IllustrativeProcedureMeasured	For example, measures indicate the number of unintentional changes or unauthorized functionality due to inadequate control of access to program source code, as a percentage of such development activities. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that access to program source code and associated items is strictly controlled in order to prevent the introduction of unauthorized functionality *and to avoi*, **security-impacting changes, an**d unintentional changes.

Question Requirement: 06.09bVAD6500System.2 / 2160.0

Change Count: 1

Field	Content
BaselineUniqueId	06*188*.09b*NYDOH***VAD6500**System.*10***2**

Question Requirement: 07.10mNYDOHOrganizational.11 / 1399.0

Change Count: 1

Field	Content
BaselineUniqueId	07*42*.10m*CMS***NYDOH**Organizational.1**1**

Question Requirement: 07.07aNIST80053Organizational.4 / 2137.0

Change Count: 1

Field	Content
BaselineUniqueId	07*164*.07aN*YDOH***IST80053**Organizational.*3***4**

Question Requirement: 09.01nCMSOrganizational.4 / 2048.0

Change Count: 1

Field	Content
BaselineUniqueId	09*975*.01n*NYDOH***CMS**Organizational.4

Question Requirement: 07.07aFFIECCATOrganizational.2 / 0642.0

Change Count: 1

Field	Content
BaselineUniqueId	07*27*.07a*CMS***FFIECCAT**Organizational.*34***2**

Question Requirement: 17.03dC5Organizational.2 / 1984.0

Change Count: 1

Field	Content
BaselineUniqueId	17.03d*NIST80053***C5**Organizational.2

Question Requirement: 12.09aaNYCRR500System.3 / 1124.0

Change Count: 1

Field	Content
BaselineUniqueId	12*47*.09aa*CMS***NYCRR500**System.3

Question Requirement: 16.12cNYDOHOrganizational.14 / 1524.0

Change Count: 1

Field	Content
BaselineUniqueId	16*52*.12c*CMS***NYDOH**Organizational.*3***14**

Question Requirement: 13.00aNIST80053Organizational.23 / 2388.1

Change Count: 3

Field	Content
BaselineUniqueId	13.00a*CMS***NIST80053**Organizational.*5***23**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the security awareness and training policy and associated *security awareness and training controls.* **controls. The organization ensures the security awareness and training policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the security awareness and training policy and procedures.** The organization reviews and updates the current security awareness and training policy at least annually or whenever a significant change occurs, and security awareness and training procedures at least annually or whenever a significant change occurs.
CrossVersionId	2388.*0***1**

Question Requirement: 11.01aCMSOrganizational.4 / 2031.0

Change Count: 1

Field	Content
BaselineUniqueId	11*958*.01a*NYDOH***CMS**Organizational.*7***4**

Question Requirement: 11.01aNIST80053Organizational.7 / 2028.0

Change Count: 1

Field	Content
BaselineUniqueId	11*955*.01aN*YDOH***IST80053**Organizational.*4***7**

Question Requirement: 16.09lNYDOHOrganizational.3 / 0916.0

Change Count: 1

Field	Content
BaselineUniqueId	16*28*.09l*CMS***NYDOH**Organizational.*1***3**

Question Requirement: 1836.08a3Organizational.1 / 0690.0

Change Count: 3

Field	Content
RequirementStatement	The organization ensures information assets and facilities it manages are physically separated from those managed by third- parties.
IllustrativeProcedureImplemented	For example, perform a tour of the organization's facilities and identify the locations where third- parties perform work. Confirm through observation that information assets and facilities managed by the organization are physically separated (e.g., barriers, doors, walls) from those managed by third- parties.
IllustrativeProcedureMeasured	For example, the measure(s) could indicate number of information assets and facilities, of which a percentage are not physically separated (e.g., barriers, doors, walls) between information assets and facilities managed by the organization and third- parties. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that information assets and facilities managed by the organization are physically separated from those managed by third- parties.

Question Requirement: 1535.11b1Organizational.12 / 1457.0

Change Count: 3

Field	Content
RequirementStatement	The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including **suspicious or unusual system activity,** violations of workforce rules of behavior**,** and acceptable use agreement **violations**, to their management and/or directly to their service provider as quickly as possible *in order to prevent information security incidents*.

IllustrativeProcedureImplemented	For example, examine evidence to confirm that employees, contractors, and third-party users are aware to report incident and event information**, including suspicious or unusual system activity, violations of workforce rules of behaviors, and acceptable use violations,** to management. This can be confirmed through evidence of formal training or acknowledgement of the organization's information security policies or acceptable use agreements as long as it contains provisions on how to report incident and event information. *S* **Further, s**elect a sample of information security incidents and examine evidence to confirm that it was appropriately reported to management. *Further***Additionally**, examine the reporting mechanism used by the organization to report incidents and event information and confirm that employees are aware of this mechanism and that it is *easy to use and widely accessible to all employees***available through a channel that's known to all employees, contractors, and third-party users and can be reached without prior authorization**.
IllustrativeProcedureMeasured	For example, measures indicate the number of employees, contractors, and third-party users that are not aware on how to report incident and event information, as a percentage of all employees. Further, the measure could indicate the number of information security events not appropriately reported by the organization's employees, contractors, and third-party users, as a percentage of all information security events. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization has an easy-to-use, available, and widely-accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including **suspicious or unusual system activity,** violations of workforce rules of behavior**,** and acceptable use agreement **violations**, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.

Question Requirement: 1416.10l1Organizational.1 / 1365.0

Change Count: 2

Field	**Content**
RequirementStatement	Where software development is outsourced, formal contracts are in place to address: licensing arrangements; code ownership; intellectual property rights; certification of the quality and accuracy of the work; rights of access for the audit of the quality and accuracy of work; escrow arrangements; quality and security functionality requirements for the developed code**, including the identification and remediation of technical vulnerabilities**; and security testing and evaluation prior to installation.

IllustrativeProcedureImplemented	For example, select a sample of outsourced software development contracts and confirm that the following have been formally defined and addressed: licensing arrangements, code ownership, intellectual property rights, certification, and rights of access for the audit of the quality and accuracy of work, escrow arrangements, quality and security functionality requirements for the developed code **(including the identification and remediation of technical vulnerabilities)**, and security testing and evaluation prior to installation.

Question Requirement: 1272.09ae1System.13 / 1218.0

Change Count: 3

Field	Content
RequirementStatement	Faults reported by users or by system programs related to problems with information processing or communications systems**, including anomalous conditions that may indicate exploitation of technical vulnerabilities,** are logged. Error logging is enabled if this system function is available.
IllustrativeProcedureImplemented	For example, select a sample of systems and examine evidence to confirm that error logging has been enabled. This can be confirmed through review of system configurations or evidence that error logs are generated. Further, examine evidence to confirm that faults reported by users or systems are logged, manually or electronically**, such that they can be utilized for the detection of indicators of exploitation of technical vulnerabilities**.
IllustrativeProcedureMeasured	For example, measures indicate the number of systems which do not have error logging enabled, as a percentage of the organization's systems. A further measure could indicate the percentage of faults reported by users or systems that are not appropriately logged, as a percentage of all faults. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* faults reported by users related to problems with information processing or communications systems**, including anomalous conditions that may indicate exploitation of technical vulnerabilities,** are logged; and, if the system function is available, error logging is enabled on the system.

Question Requirement: 12101.09ab1System.2 / 1148.1

Change Count: 4

Field	Content
RequirementStatement	The organization specifies**, based on a formally documented assessment of risk,** how often audit logs are reviewed, how the reviews are documented, *and* the specific roles and responsibilities of the personnel conducting the reviews, *including***and** the professional certifications or other qualifications required.

IllustrativeProcedureImplemented	For example, examine written policies, procedures, standards, or guidelines to confirm that the organization**, based on a formally documented assessment of risk,** specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.
IllustrativeProcedureMeasured	For example, measures indicate the number of reviews performed on audit logs. A further measure could indicate the number of audit logs and the percentage of those that are reviewed and documented by qualified personnel. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm *that* the organization *reviews audit logs and***specifies, based on a formally documented assessment of risk, how often audit logs are reviewed, how** the reviews are documented, *and* the specific roles and responsibilities of the personnel conducting the reviews, *including***and** the professional certifications or other qualifications required.
CrossVersionId	1148.*0***1**

Question Requirement: 16.09lAISecOrganizational.1 / 3067.0

Change Count: 3

Field	**Content**
RequirementStatement	Backup copies of the following AI assets are created: training, test, and validation datasets; code used to create, train, and/or deploy AI models; tuning data; models; *language model tools (e.g., plugins, agents)***agents, skills, and plugins**; AI system configurations (e.g., metaprompts); and prompt enhancement data for RAG, as applicable. These backups are managed in accordance with the organization's policies addressing backups of data and software.
IllustrativeProcedureImplemented	For example, review the AI system to ensure backup copies of AI assets are created and include training, test, and validation datasets, code used to create, train, and/or deploy AI models, tuning data, models, *language model tools (e.g., plugins, agents)***agents, skills, and plugins**, AI system configurations (e.g., metaprompts), prompt enhancement data for RAG. Further, confirm the backups are managed in accordance with the organization's policies addressing backups of data and software.
IllustrativeProcedureMeasured	For example, measures indicate if backup copies of AI assets are created and include training, test, and validation datasets, code used to create, train, and/or deploy AI models, tuning data, models, *language model tools (e.g., plugins, agents)* **agents, skills, and plugins**, AI system configurations (e.g., metaprompts), prompt enhancement data for RAG. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that backups are managed in accordance with the organization's policies addressing backups of data and software.

Question Requirement: 14.09fAISecSystem.1 / 3049.0

Change Count: 2

Field	Content
RequirementStatement	The organization performs an evaluation of the security posture of any external commercial providers of AI system components, including AI models; datasets; software packages (e.g., those for model creation, training, and/or deployment); platforms and computing infrastructure; and *language model tools such as agents***agents, skills,** and plugins, as applicable. This evaluation is performed during onboarding of the provider and on a routine basis thereafter in accordance with the organization's supplier oversight processes.
IllustrativeProcedureMeasured	For example, measures indicate if the organization performs an evaluation of the security posture of any external commercial providers of AI system components, including AI models, datasets, software packages (e.g., those for model creation, training, and/or deployment), platforms and computing infrastructure, and *language model tools such as agents***agents, skills,** and plugins, as applicable. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all external commercial providers of AI system components are evaluated.

Question Requirement: 12.09abAISecSystem.5 / 3063.0

Change Count: 3

Field	Content
RequirementStatement	The organization performs monitoring, on at least a monthly basis, for suspicious manipulation of AI-related datasets; AI models; AI-relevant code (e.g., code used to create, train, and/or deploy AI models, code of *language model tools such as agents***agents, skills,** and plugins); and AI-relevant configurations (e.g., metaprompts) that might compromise the AI system's performance or security.
IllustrativeProcedureImplemented	For example, review the AI system to ensure the organization performs monitoring, on at least a monthly basis, for suspicious manipulation of AI-related datasets; AI models; AI-relevant code (e.g., code used to create, train, and/or deploy AI models, code of *language model tools such as agents***agents, skills,** and plugins); and AI-relevant configurations (e.g., metaprompts) that might compromise the AI system's performance or security.
IllustrativeProcedureMeasured	For example, measures indicate if the organization performs monitoring, on at least a monthly basis, for suspicious manipulation of AI-related datasets; AI models; AI-relevant code (e.g., code used to create, train, and/or deploy AI models, code of *language model tools such as agents***agents, skills,** and plugins); and AI-relevant configurations (e.g., metaprompts) that might compromise the AI system's performance or security.

Question Requirement: 15.11eCMSOrganizational.3 / 2224.0

Change Count: 1

Field	Content
BaselineUniqueId	15*252*.11e*NYDOH***CMS**Organizational.3

Question Requirement: 11.01qCMSSystem.7 / 2057.0

Change Count: 1

Field	Content
BaselineUniqueId	11*984*.01q*NYDOH***CMS**System.*117*

Question Requirement: 1505.11a2Organizational.6 / 1427.0

Change Count: 1

Field	Content
RequirementStatement	Formal information security event reporting procedures to support the corporate direction (policy) are established, set out the action to be taken on receipt of a report of an information security event, set out the treating of breach as discovered, set out the timeliness of reporting and response, set out the time required for system administrators and other personnel to report anomalous events to the incident handling team, set out the mechanisms for such reporting, and set out the kind of information that is included in the incident notification. Formal information security event reporting also includes notifying internal stakeholders (in accordance with all legal or regulatory requirements for involving them in computer incidents), notifying external stakeholders (in accordance with all legal or regulatory requirements for involving them in computer incidents), notifying the appropriate Community Emergency Response Team, and notifying law enforcement agencies (in accordance with all legal or regulatory requirements for involving them in computer incidents). Given the importance of Information Security Incident Handling, a policy is established to set the direction of management. Employees and other workforce members, including third- parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion.

Question Requirement: 11.01pSRSystem.2 / 0192.0

Change Count: 1

Field	Content
BaselineUniqueId	11*102*.01p*2***SR**System.2

Question Requirement: 1620.09l2Organizational.5 / 0905.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of third- parties that are performing backup services where a service level agreement is not in place, as a percentage of such third- parties. A further measure could indicate the number of service level agreements that do not contain the appropriate detailed protections to control confidentiality, integrity, and availability of the backup information, as a percentage of service level agreements with third- parties performing backup services. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, when the backup service is delivered by the third-party, the service level agreement includes the detailed protections to control confidentiality, integrity, and availability of the backup information.

Question Requirement: 14912.05kSROrganizational.2 / 1949.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that business continuity and/or disaster recovery requirements as noted in the requirement statement has been defined and included into the agreement. Further, verify that the requirements have been implemented in accordance with the supplier agreement and/or organizational policies, and working as intended.
IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-party agreements that satisfy the business continuity and/or disaster recovery requirements in accordance with the organization's policies, as a percentage of all third-party agreements. Reviews, tests, or audits are completed by the supplier to measure the effectiveness of the implemented controls and to verify that a standard agreement with third- parties is defined and includes the required security controls in accordance with the organization's security policies.

Question Requirement: 14908.05kSROrganizational.1 / 1948.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm that each requirement as noted in the requirement statement has been defined and included into the agreement. Further, verify that each requirement has been implemented in accordance with the supplier agreement and/or organizational policies, and working as intended.

IllustrativeProcedureMeasured	For example, the metric could indicate the number of third-party agreements that satisfy the identified security requirements in accordance with the organization's policies, as a percentage of all third-party agreements. Reviews, tests, or audits are completed by the supplier to measure the effectiveness of the implemented controls and to verify that a standard agreement with third- parties is defined and includes the required security controls in accordance with the organization's security policies.

Question Requirement: 18.00aNIST80053Organizational.21 / 2413.1

Change Count: 3

Field	Content
BaselineUniqueId	18.00a*FedRAMP***NIST80053**Organizational.*1***21**
RequirementStatement	The organization develops, documents, and disseminates to organization-defined personnel or roles a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. **The organization ensures the physical and environmental protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines and designates an organization-defined official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures.** The organization reviews and updates the current physical and environmental protection policy at least annually, and physical and environmental protection procedures at least annually or whenever a significant change occurs.
CrossVersionId	2413.*0***1**

Question Requirement: 07.10mPCIOrganizational.7 / 1401.0

Change Count: 1

Field	Content
BaselineUniqueId	07*44*.10m*CMS***PCI**Organizational.*34***7**

Question Requirement: 16.12cNIST80053Organizational.12 / 2232.0

Change Count: 1

Field	Content
BaselineUniqueId	16*260*.12cN*YDOH***IST80053**Organizational.*8***12**

Question Requirement: 1118.01j2Organizational.124 / 0126.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of remote access points that are not encrypted over VPN or private line. Further, the metric includes the number of remote access sessions accessing organization systems by third- parties (e.g., vendors) Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that organizations implement encryption (e.g., VPN solutions or private lines) and logs remote access to the organization's network by employees, contractors or third-party (e.g., vendors).

Question Requirement: 1114.01h1Organizational.123 / 0114.0

Change Count: 3

Field	Content
RequirementStatement	Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are **immediately** removed from *printers, copiers, and facsimile machines immediately***document processing devices (e.g., printers, copiers, scanners, or multifunction devices)**. When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).
IllustrativeProcedureImplemented	For example, tour the organization's facilities and observe users' desks, computer monitors, printers, fax machines, and copiers to *identify***confirm**: if covered and/or critical business information is openly available and unattended (especially when the office is vacated); if workstations are protected by key locks, passwords, or other controls when not in use; if documents containing covered and/or critical business information are **immediately** removed from *printers, copiers and fax machin***document processing devices (e.g., printers, copiers, scanners, or multifunction devic**es**)**; and if workstations are protected by a user authentication method that conceals information previously visible on the display when unattended (e.g., screen saver). Further, observe the process by which documents are transported through interoffice mail and confirm that covered or critical information is concealed during transit (e.g., using opaque envelopes).

IllustrativeProcedureMeasured	For example, the measure(s) indicate the percentage of users that are compliant/non-compliant with the organization's clear desk and clear screen policies to ensure the protection of covered or critical business information. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, *printers, copiers, fax machines, and computer monitors* **computer monitors, and document processing devices (e.g., printers, copiers, scanners, or multifunction devices)** .

Question Requirement: 14.05kADHICSOrganizational.7 / 3141.0

Change Count: 3

Field	Content
RequirementStatement	The standard agreement with third- parties addresses requirements in case of sub-contracting, ensures the third parties process data only for agreed upon purpose and duration, ensures the third- parties delete the data once the purpose is accomplished, ensures the third- parties notify the organization in case of an appointment of sub-contractors, ensures the third- parties notify the organization in case of processing covered and/or confidential information beyond agreed time period.
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement and confirm the elements stipulated in the requirement statement were defined and included into the agreement.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of third-party agreements that satisfy the elements stipulated in the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm standard agreements with third- parties address the elements stipulated in the requirement statement.

Question Requirement: 14.05kADHICSOrganizational.9 / 3147.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement to confirm if changes followed a formal change management process that included the elements stipulated in the requirement statement.

Question Requirement: 14.05kADHICSOrganizational.8 / 3146.0

Change Count: 3

Field	Content
RequirementStatement	Agreements with third- parties include termination clauses which address data conversion to a standardized format by the third -party, based on industry standard and agreement with the organization, removal of data from the third-party's environment, after an agreed period of time, migration of data to the organization’s environment, handover of all backup copies of data to the organization, disconnecting all existing integration on behalf of the organization, cooperation with the new onboarded third-party (if any) for the required integration and data migration, knowledge handover to the new third-party or the organization's stakeholders, based on an agreed approach.
IllustrativeProcedureImplemented	For example, select a sample of third- parties, and examine the third-party agreement to confirm the inclusion of termination clauses which addressed the elements stipulated in the requirement statement.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of third-party agreements which excluded the stipulated clauses. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm agreements with third- parties include termination clauses which address the elements stipulated in the requirement statement.

Question Requirement: 18.08jNIST80053Organizational.3 / 0798.0

Change Count: 1

Field	Content
BaselineUniqueId	18*116*.08j*CMS***NIST80053**Organizational.*4***3**

Question Requirement: 08.01wAISecSystem.4 / 3388.0

Change Count: 0

Field	Content
New Question Requirement	08.01wAISecSystem.4 / 3388.0

Changes for Authoritative Source Document - v11.8.0 to v11.9.0

Authoritative Source Document: India Digital Personal Data Protection Act

Change Count: 0

Field	Content
New Authoritative Source Document	India Digital Personal Data Protection Act

Authoritative Source Document: FedRAMP 20x Key Security Indicators

Change Count: 0

Field	Content
New Authoritative Source Document	FedRAMP 20x Key Security Indicators

Authoritative Source Document: OWASP Top 10 For Agentic Applications

Change Count: 0

Field	Content
New Authoritative Source Document	OWASP Top 10 For Agentic Applications

Authoritative Source Document: OWASP Top 10 for LLM Applications 2025

Change Count: 0

Field	Content
New Authoritative Source Document	OWASP Top 10 for LLM Applications 2025

Authoritative Source Document: NIST SP 800-137

Change Count: 0

Field	Content
New Authoritative Source Document	NIST SP 800-137

Authoritative Source Document: Commonwealth of Virginia ITRM (SEC530)

Change Count: 0

Field	Content
New Authoritative Source Document	Commonwealth of Virginia ITRM (SEC530)

Authoritative Source Document: ISO/IEC 29100:2024

Change Count: 0

Field	Content
New Authoritative Source Document	ISO/IEC 29100:2024

Authoritative Source Document: BSI Cloud Computing Compliance Controls Catalogue (C5)

Change Count: 0

Field	Content
New Authoritative Source Document	BSI Cloud Computing Compliance Controls Catalogue (C5)

Authoritative Source Document: CMS ARC-AMPE

Change Count: 0

Field	Content
New Authoritative Source Document	CMS ARC-AMPE

Authoritative Source Document: Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)

Change Count: 0

Field	Content
New Authoritative Source Document	Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)

Authoritative Source Document: Strategies to Mitigate Cybersecurity Incidents (Australia)

Change Count: 0

Field	Content
New Authoritative Source Document	Strategies to Mitigate Cybersecurity Incidents (Australia)

Authoritative Source Document: NIST SP 800-53 r5.2.0 (2026 Update)

Change Count: 0

Field	Content
New Authoritative Source Document	NIST SP 800-53 r5.2.0 (2026 Update)

Authoritative Source Document: UK Cyber Assessment Framework

Change Count: 0

Field	Content
New Authoritative Source Document	UK Cyber Assessment Framework

Authoritative Source Document: UK Data Security and Protection Toolkit

Change Count: 0

Field	Content
New Authoritative Source Document	UK Data Security and Protection Toolkit

Authoritative Source Document: APRA Cross-Industry Prudential Standards 230

Change Count: 0

Field	Content
New Authoritative Source Document	APRA Cross-Industry Prudential Standards 230

Changes for Factor Type - v11.8.0 to v11.9.0

Factor Type: Compliance - Agentic AI

Change Count: 0

Field	Content
New Factor Type	Compliance - Agentic AI

Changes for Factor - v11.8.0 to v11.9.0

Factor: Compliance - HITRUST Reg: Compliance Factors - OWASP Top 10 for Agentic Applications 2026

Change Count: 0

Field	Content
New Factor	Compliance - HITRUST Reg: Compliance Factors - OWASP Top 10 for Agentic Applications 2026

Factor: Compliance - Agentic AI - No

Change Count: 0

Field	Content
New Factor	Compliance - Agentic AI - No

Factor: Compliance - Agentic AI - Yes

Change Count: 0

Field	Content
New Factor	Compliance - Agentic AI - Yes