v11.5.0 Summary of Changes

Difference Comparison for CSF v11.4.0 to v11.5.0

HITRUST

Table of Contents

Changes for Library Version View D T O - v11.4.0 to v11.5.0

Library Version View D T O: v11.5.0

Change Count: 1

Field	Content
Name	v11.*4*45**5**.0

Changes for Question Requirement Record - v11.4.0 to v11.5.0

Question Requirement Record: 1784.10aHICPOrganizational.2 / 1230.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written policies and procedures and confirm that,*examine written policies and procedures and confirm that,**measures indicate the number of commercial products assessed**measures indicate the number of commercial products assessed where the security functionality in a proposed product does not satisfy the specified requirement*, then*, then **and where** and where the risk**s** s introduced and associated controls *are*are**were not**were not reconsidered prior to purchasing the product*. Select a sample of instances of*. Select a sample of instances of**, as a percentage of products purchased. The measure helps identify whether the risk introduced and associated controls**, as a percentage of products purchased. The measure helps identify whether the risk introduced and associated controls w*h*here a *commercial product was purchased and confirm that an assessment was performed to ensure* commercial product was purchased and confirm that an assessment was performed to ensure**ccepted or mitigated prior to purchasing the product. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm** ccepted or mitigated prior to purchasing the product. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that**,**, where the security functionality in a proposed product d*id* id**oes**oes not satisfy the specified requirement, then the risk introduced and associated control *we* we**s a**s are reconsidered prior to purchasing the product.

Question Requirement Record: 02.09mHICPOrganizational.4 / 2336.0

Change Count: 1

Field	Content
RequirementStatement	The organization ensures the following basic endpoint protections are implemented: enable full-disk encryption on all endpoints; disable weak authentication hashes on endpoints; and restrict local administrative rights on endpoints to authorized individuals.

Question Requirement Record: 15.11cNIST80053Organizational.2 / 2784.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence to confirm counterfeit component detection techniques for system components are utilized. Further, select a sample of detected counterfeit components and examine evidence to confirm the counterfeit component was prevented from entering the system and was reported to the source of the counterfeit component, any organization-defined external reporting organizations, or any organization-defined personnel or roles.

Question Requirement Record: 01.00aNIST80053Organizational.45 / 2783.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence to confirm the organization reviewed and updated the supply chain risk management plan within the last year. Further, obtain the supply chain risk management plan and confirm it includes consideration for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the systems, system components or system services.
IllustrativeProcedureMeasured	For example, measures indicate whether the organization reviewed and updated the supply chain risk management plan within the last year. Further, measures indicate whether the supply chain risk management plan addresses the elements contained within the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization develops a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the systems, system components or system services, and reviews and updates the supply chain risk management plan annually or as required to address threat, organizational, or environmental changes.

Question Requirement Record: 01.04aNIST80053Organizational.3 / 2283.0

Change Count: 1

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

Question Requirement Record: 18.00aNIST80053Organizational.43 / 2664.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine the relevant physical and environmental protection policy and confirm that it is developed and documented to be consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines. Further, confirm the relevant physical and environmental protection policy addresses the organization's designation of an official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures.

Question Requirement Record: 19.13kNIST80053Organizational.1 / 2779.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures could indicate the number of individuals who were not provided with the required notifications when asked to disclose his or her Social Security number. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization, when processing Social Security numbers, eliminates unnecessary collection, maintenance, and use of Social Security numbers, explores alternatives to their use as a personal identifier, and informs any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Question Requirement Record: 18.08bNIST80053Organizational.10 / 0703.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of visitors that have been recorded, as a percentage of all visitors. Further, the metric could include the percentage of visitor logs that have been reviewed on a monthly basis 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 verify that a visitor log containing appropriate information is reviewed monthly and maintained for at least two years.

Question Requirement Record: 14.05kNIST80053Organizational.2 / 2306.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of contractual agreements that allow data to be provided to contractor's systems. Further, measures indicate the expected end date and date for the return of data to the organization. Additionally, measures could indicate the percentage of contractual agreements that have ended where data was not returned which are non-compliant as a percentage of all such agreements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the contractor system and data agreement process each year to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable organization-defined security requirements.

Question Requirement Record: 17.10aNIST80053Organizational.4 / 1260.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine the organization's systems diagrams to identify the organization's critical online resources. Confirm that redundant systems for the data warehouse have been employed. This can also be confirmed through review of disaster recovery or business continuity policies and procedures. Further examine, configuration settings from the redundant systems to confirm that automatic failover functionality has been enabled*examine the organization's systems diagrams to identify the organization's critical online resources. Confirm that redundant systems for the data warehouse have been employed. This can also be confirmed through review of disaster recovery or business continuity policies and procedures. Further examine, configuration settings from the redundant systems to confirm that automatic failover functionality has been enabled**measures indicate the number of critical online resources where redundant systems have not been implemented, as a percentage of the organization's critical online resources. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, for critical online resources, redundant systems in a data warehouse are employed with automatic failover capability**measures indicate the number of critical online resources where redundant systems have not been implemented, as a percentage of the organization's critical online resources. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, for critical online resources, redundant systems in a data warehouse are employed with automatic failover capability.

Question Requirement Record: 17291.10aNIST80053Organizational.1 / 2264.0

Change Count: 1

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

Question Requirement Record: 12.09aaNIST80053System.3 / 2311.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of information system configurations for auditing security and privacy attributes that are non-compliant as stipulated at the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness each year to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable organization-defined security requirements.

Question Requirement Record: 19.13kPHIPAOrganizational.19 / 2768.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of instances in which the organization receives PHI and examine evidence the Commissioner approved practices and procedures to protect the privacy of the individuals whose PHI it receives and to maintain the confidentiality of the information. Further, examine evidence to confirm the practices and procedures were followed during the analysis and linking with other data that the Minister required.

Question Requirement Record: 1787.10a2Organizational.1 / 1233.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *information security and privacy is integrated into the organizations project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g., a project for a core business proc*information security and privacy is integrated into the organizations project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g., a project for a core business proc**measures indicate the number of projects where privacy and security requirements were not addressed through the project management life cycle, as a percent of applicable projects. Reviews, t**measures indicate the number of projects where privacy and security requirements were not addressed through the project management life cycle, as a percent of applicable projects. Reviews, tes**t**ts, *IT, facility management and other supporting processes. Examine written policies and procedure*IT, facility management and other supporting processes. Examine written policies and procedure**or audits are completed by the organization to measure the effectiveness of the implemented control**or audits are completed by the organization to measure the effectiveness of the implemented controls and **to** to confirm that information security and privacy is addressed in all phases of the project management methodology *which include the following: (i) information security objectives are included in project objectives; and, (ii) an information security risk assessment is conducted at an early stage of the project to identify necessary controls* which include the following: (i) information security objectives are included in project objectives; and, (ii) an information security risk assessment is conducted at an early stage of the project to identify necessary controls.

Question Requirement Record: 1793.10a2Organizational.91011 / 1239.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written policies and procedures and confirm that the requirement definition phase includes: (i) consideration of system requirements for information security and the processes for implementing security and (ii) data classification and risk to information assets are assigned and approved (signed-off) by management to ensure appropriate controls will be considered and*examine written policies and procedures and confirm that the requirement definition phase includes: (i) consideration of system requirements for information security and the processes for implementing security and (ii) data classification and risk to information assets are assigned and approved (signed-off) by management to ensure appropriate controls will be considered and**measures indicate the percent of audit logs that are appropriately retained in accordance with the organization's policy, along with the percentage of audit logs that are non-compliant with the requirement. A further metric can include KPIs created to monitor and measure the retention of data, including audit logs. Reviews, tests, or audits should be completed by**measures indicate the percent of audit logs that are appropriately retained in accordance with the organization's policy, along with the percentage of audit logs that are non-compliant with the requirement. A further metric can include KPIs created to monitor and measure the retention of data, including audit logs. Reviews, tests, or audits should be completed by the *c*cor*rect project team members are involved. Select a sample of software development changes and examine the requirements definition document to confirm that (i) consideration of system requirements for information security and the processes for implementing*rect project team members are involved. Select a sample of software development changes and examine the requirements definition document to confirm that (i) consideration of system requirements for information security and the processes for implementing**ganization to measure the effectiveness of the implemented controls and to confirm that retention for audit logs are**ganization to measure the effectiveness of the implemented controls and to confirm that retention for audit logs are s**p**pec*urity were identified and (ii) data classification and risk to information asset*urity were identified and (ii) data classification and risk to information asset**ified by the organization and the log**ified by the organization and the logs *a*are *assigned and approved (signed-off) by management* assigned and approved (signed-off) by management**tained accordingly**tained accordingly.

Question Requirement Record: 1785.10a2Organizational.14 / 1231.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written policies and procedures and confirm*examine written policies and procedures and confirm **measures indicate the number of security risks identified** measures indicate the number of security risks identified that,, w*h*here *additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls. Select a sample of instances where a commercial product was purchased and confirm that an assessment was performed to identify*additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls. Select a sample of instances where a commercial product was purchased and confirm that an assessment was performed to identify**not mitigated through disabling of the additional functionality or implementation of additional controls, as a percentage of products implemented for a specified period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, where**not mitigated through disabling of the additional functionality or implementation of additional controls, as a percentage of products implemented for a specified period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that, where additional functionality *which*which**is supplied and**is supplied and causes a security risk*. Confirm that*. Confirm that**,**, the functionality *wa*wa**i**is disabled *and or additional controls were implemented to mitigate the risk*and or additional controls were implemented to mitigate the risk**or mitigated through the application of additional controls**or mitigated through the application of additional controls.

Question Requirement Record: 1783.10a2Organizational.13 / 1229.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written policies and procedures and confirm that purchased commercial product*examine written policies and procedures and confirm that purchased commercial product**measures indicate the number of processes, such as monitoring of activities, audit trail** measures indicate the number of processes, such as monitoring of activities, audit trails, **m***mand supplier contracts must follow the organization's formal acquisition process. Select a sample of instances of where a commercial*d supplier contracts must follow the organization's formal acquisition process. Select a sample of instances of where a commercial **agement supervision, where separation of duties have not been implemented, as a percent of processes to**agement supervision, where separation of duties have not been implemented, as a percent of processes to pro*du*du**te**tect *was purchased and confirm that it was purchased in accordance with the organization's acquisition policy and procedures. Further, select a sample of supplier*was purchased and confirm that it was purchased in accordance with the organization's acquisition policy and procedures. Further, select a sample of supplier**against the unauthorized or unintentional modification of information assets. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented**against the unauthorized or unintentional modification of information assets. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented contr*act*act**ol**ols and *confirm that security requirements were identified and defined with the contract*confirm that security requirements were identified and defined with the contract**to verify that separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems**to verify that separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems.

Question Requirement Record: 17.10k2Organizational.10 / 1241.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, system acceptance testing metrics could include listing the tests performed and indicating whether tests were passed/failed/remediated, a measure of the importance and nature of the associated system, as organizationally defined, and a measure of the level of testing independence, as organizationally defined. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the independent acceptance testing performed by the organization to ensure the system works as expected and only as expected is proportional to the importance and nature of the system (both for in-house and for outsourced developments).

Question Requirement Record: 18126.08k2Organizational.4 / 0810.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of security risks identified as part of the off-site location risk assessment where suitable controls were not implemented to mitigate the risk, as a percentage of risks identified. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that specification of controls for the protection of off-premises equipment take into consideration the security risks (e.g., of damage, theft, or eavesdropping), which may vary considerably between locations.

Question Requirement Record: 16.09l1Organizational.4 / 2326.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, observe the organization's facility and determine where offline backup media is stored. If an immutable backup solution is in place, examine configurations and *whitepapers to* whitepapers to**the technical controls that**the technical controls that support the backup cannot be modified or deleted.

Question Requirement Record: 1308.09j1Organizational.5 / 0875.1

Change Count: 1

Field	Content
RequirementStatement	The organization prohibits users from installing unauthorized software, including data and software from external networks, and disables any auto-run features which allow file execution without user authorization (such as when files are downloaded from the Internet or when removable media is inserted). Users are made aware and trained on requirements relating to prohibition of installing unauthorized software, including data and software from external networks.

Question Requirement Record: 0913.09s1Organizational.5 / 1055.0

Change Count: 1

Field	Content
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 later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and T*S*SL**S** S VPNs: SSL Portal VPN; SSL Tunnel VPN.

Question Requirement Record: 11.01p1System.5 / 2364.0

Change Count: 1

Field	Content
RequirementStatement	A policy applicable to the organization’s information systems addressing account lockout after consecutive unsuccessful login attempts is documented and enforced through technical controls.

Question Requirement Record: 18122.08k1Organizational.1 / 0806.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of the organization's network infrastructure, access points, wiring, conduits, and cabling used to process unencrypted FTI not within the control of authorized agency personnel. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that if encryption is not used to protect the transmission of FTI, the organization must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized organization personnel.

Question Requirement Record: 01.06gADHICSOrganizational.2 / 3121.0

Change Count: 0

Field	Content
New Question Requirement Record	01.06gADHICSOrganizational.2 / 3121.0

Question Requirement Record: 01.00aADHICSOrganizational.2 / 3120.0

Change Count: 0

Field	Content
New Question Requirement Record	01.00aADHICSOrganizational.2 / 3120.0

Question Requirement Record: 15.10mSCAOrganizational.3 / 3155.0

Change Count: 0

Field	Content
New Question Requirement Record	15.10mSCAOrganizational.3 / 3155.0

Question Requirement Record: 07.10mSCAOrganizational.2 / 3119.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mSCAOrganizational.2 / 3119.0

Question Requirement Record: 07.10bSCASystem.1 / 3118.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10bSCASystem.1 / 3118.0

Question Requirement Record: 18.08hSCAOrganizational.1 / 3117.0

Change Count: 0

Field	Content
New Question Requirement Record	18.08hSCAOrganizational.1 / 3117.0

Question Requirement Record: 11.09cSCAOrganizational.1 / 3116.0

Change Count: 0

Field	Content
New Question Requirement Record	11.09cSCAOrganizational.1 / 3116.0

Question Requirement Record: 17.10aSCAOrganizational.2 / 3115.0

Change Count: 0

Field	Content
New Question Requirement Record	17.10aSCAOrganizational.2 / 3115.0

Question Requirement Record: 01.10aSCAOrganizational.1 / 3114.0

Change Count: 0

Field	Content
New Question Requirement Record	01.10aSCAOrganizational.1 / 3114.0

Question Requirement Record: 17.03bSCAOrganizational.1 / 3113.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03bSCAOrganizational.1 / 3113.0

Question Requirement Record: 17.03aSCAOrganizational.1 / 3112.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03aSCAOrganizational.1 / 3112.0

Question Requirement Record: 08.09dSCASystem.1 / 3111.0

Change Count: 0

Field	Content
New Question Requirement Record	08.09dSCASystem.1 / 3111.0

Question Requirement Record: 07.04aSCAOrganizational.1 / 3110.0

Change Count: 0

Field	Content
New Question Requirement Record	07.04aSCAOrganizational.1 / 3110.0

Question Requirement Record: 14.09fSCASystem.1 / 3109.0

Change Count: 0

Field	Content
New Question Requirement Record	14.09fSCASystem.1 / 3109.0

Question Requirement Record: 07.10mSCAOrganizational.1 / 3108.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mSCAOrganizational.1 / 3108.0

Question Requirement Record: 07.07aSCAOrganizational.1 / 3107.0

Change Count: 0

Field	Content
New Question Requirement Record	07.07aSCAOrganizational.1 / 3107.0

Question Requirement Record: 14.05kSCAOrganizational.1 / 3106.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kSCAOrganizational.1 / 3106.0

Question Requirement Record: 12.09abSCASystem.1 / 3105.0

Change Count: 0

Field	Content
New Question Requirement Record	12.09abSCASystem.1 / 3105.0

Question Requirement Record: 17.06gSCAOrganizational.2 / 3104.0

Change Count: 0

Field	Content
New Question Requirement Record	17.06gSCAOrganizational.2 / 3104.0

Question Requirement Record: 11.01aNIS2Organizational.1 / 3103.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01aNIS2Organizational.1 / 3103.0

Question Requirement Record: 15.02fNIS2Organizational.1 / 3102.0

Change Count: 0

Field	Content
New Question Requirement Record	15.02fNIS2Organizational.1 / 3102.0

Question Requirement Record: 13.02cNIS2Organizational.1 / 3101.0

Change Count: 0

Field	Content
New Question Requirement Record	13.02cNIS2Organizational.1 / 3101.0

Question Requirement Record: 07.10mNIS2Organizational.1 / 3100.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mNIS2Organizational.1 / 3100.0

Question Requirement Record: 06.09bNIS2System.1 / 3099.0

Change Count: 0

Field	Content
New Question Requirement Record	06.09bNIS2System.1 / 3099.0

Question Requirement Record: 14.05kNIS2Organizational.1 / 3098.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kNIS2Organizational.1 / 3098.0

Question Requirement Record: 15.11dNIS2Organizational.1 / 3097.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11dNIS2Organizational.1 / 3097.0

Question Requirement Record: 01.00aCOBITOrganizational.2 / 3096.0

Change Count: 0

Field	Content
New Question Requirement Record	01.00aCOBITOrganizational.2 / 3096.0

Question Requirement Record: 01.00aCOBITOrganizational.1 / 3095.0

Change Count: 0

Field	Content
New Question Requirement Record	01.00aCOBITOrganizational.1 / 3095.0

Question Requirement Record: 16.09lAUSOrganizational.1 / 3093.0

Change Count: 0

Field	Content
New Question Requirement Record	16.09lAUSOrganizational.1 / 3093.0

Question Requirement Record: 09.10gNIS2Organizational.2 / 3092.0

Change Count: 0

Field	Content
New Question Requirement Record	09.10gNIS2Organizational.2 / 3092.0

Question Requirement Record: 01.03aCOBITOrganizational.1 / 3088.0

Change Count: 0

Field	Content
New Question Requirement Record	01.03aCOBITOrganizational.1 / 3088.0

Question Requirement Record: 13.02dCOBITOrganizational.2 / 3087.0

Change Count: 0

Field	Content
New Question Requirement Record	13.02dCOBITOrganizational.2 / 3087.0

Question Requirement Record: 12103.09abTexasSystem.1 / 1150.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of information systems audit logs that are aggregated and consolidated to be used by the SIEM, along with the percentage of systems that are not being monitored by the tool. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that information collected from multiple sources are aggregated for review.

Question Requirement Record: 1439.09eFTISystem.3 / 0844.1

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the measure(s) could track the number of locations where FTI is stored in order to evaluate "data sprawl" and help indicate whether FTI is located, operated, and accessed outside of the United States. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization restricts the location of information systems that receive, process, store, or transmit FTI as stipulated in organization requirements.

Question Requirement Record: 17106.10aCMSOrganizational.5 / 1253.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written development policies and proced*examine written development policies and proced**meas** measures *a*a**i**ind *confirm that it is required that the developer of the information system, system component, or information system service produce an acceptable design specification and security architecture. Select a sample of applicable development changes and confirm that an appropriate acceptable design specification and security architecture was formally documented and includes the following: (i) is consistent with, and supportive* confirm that it is required that the developer of the information system, system component, or information system service produce an acceptable design specification and security architecture. Select a sample of applicable development changes and confirm that an appropriate acceptable design specification and security architecture was formally documented and includes the following: (i) is consistent with, and supportive**icate the number of applicable development changes where an appropriate design specification and security architecture document was not produced, as a percentage of applicable development changes. Reviews, tests, or audits are completed by the organization to measure the effectiveness**icate the number of applicable development changes where an appropriate design specification and security architecture document was not produced, as a percentage of applicable development changes. Reviews, tests, or audits are completed by the organization to measure the effectiveness of,, the *organizations security architecture which is established within and is an integrated part of the organizations enterprise architecture; (ii) accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and, (iii) expresses how individual security functions, mechanisms, and services work together to provide required*organizations security architecture which is established within and is an integrated part of the organizations enterprise architecture; (ii) accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and, (iii) expresses how individual security functions, mechanisms, and services work together to provide required **implemented controls and to confirm that the organization requires the developer of the information system, system component, or information system service to produce an acceptable design**implemented controls and to confirm that the organization requires the developer of the information system, system component, or information system service to produce an acceptable design s**p**pec*urity capabilities and a unified approach to pro*urity capabilities and a unified approach to pro**ification and security archi**ification and security archi tect*ion*ion**ure**ure.

Question Requirement Record: 17105.10aCMSOrganizational.4 / 1252.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine evidence to confirm that the organization performed a review of the organization's development process, standards, tools, and tool options/configurations at least every three years. Examine the results of the review*examine evidence to confirm that the organization performed a review of the organization's development process, standards, tools, and tool options/configurations at least every three years. Examine the results of the review**measures indicate the number of System Acquisition (SA) and Configuration Management (CM) security controls identified as not being satisfied based on the annual review of the organization's development process, as a percent of all applicable security requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls**measures indicate the number of System Acquisition (SA) and Configuration Management (CM) security controls identified as not being satisfied based on the annual review of the organization's development process, as a percent of all applicable security requirements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and **to** to confirm that the *review assessed*review assessed**organization reviews**organization reviews the development process, standards, tools, **and tool options/configurations within three years to determine if the process, standards, tools,** and tool options/configurations within three years to determine if the process, standards, tools, and tool options/configurations selected and employed*, and it*, and it **can** can satisf*ied*ied**y**y all applicable System Acquisition (SA) and Configuration Management (CM) security controls.

Question Requirement Record: 17103.10aCMSOrganizational.2 / 1250.0

Change Count: 1

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

Question Requirement Record: 0962.10fPCIOrganizational.1 / 1292.1

Change Count: 4

Field	Content
RequirementStatement	The organization maintains and updates at least annually a documented description of the cryptographic architecture that includes: details of all algorithms, protocols, and keys used for the protection of **sensitive data (i.e.,** sensitive data (i.e., cardholder data**)**), including key strength and expiry date; description of the key usage for each key; inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management; active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use; and a documented strategy to respond to anticipated changes in cryptographic vulnerabilities.
IllustrativeProcedureImplemented	For example, examine the evidence to confirm that the organization formally documented its cryptographic architecture, including: (i) details of all algorithms, protocols, and keys used for the protection of **sensitive data (i.e.,** sensitive data (i.e., cardholder data**)**), including key strength and expiry date; (ii) description of the key usage for each key; and (iii) inventory of any HSMs and other SCDs used for key management.
IllustrativeProcedureMeasured	For example, measures indicate the number of components in the organization's cryptographic architecture that have/have not been formally documented as stipulated in the requirement statement, as a percentage of its cryptographic architecture. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization maintains and updates at least annually a documented description of the cryptographic architecture that includes: (i) details of all algorithms, protocols, and keys used for the protection of **sensitive data (i.e.,** sensitive data (i.e., cardholder data**)**), including key strength and expiry date (ii) description of the key usage for each key (iii) inventory of any hardware security modules (HSMs) and other secure cryptographic devices (SCDs) used for key management.
CrossVersionId	1292.*0*011

Question Requirement Record: 19502.13nGDPROrganizational.4 / 1859.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of individuals that were not advised of their opportunity to agree to, prohibit or restrict a use or disclosure at the time of the organization's first communication with the individual, as a percentage of all individuals whose PII is processed by the organization over a specified reporting period such as monthly or quarterly. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization informs individuals at the time of their first communication of the opportunity to agree to, prohibit or restrict an allowed use or disclosure, in advance of such use or disclosure.

Question Requirement Record: 18.09pFedRAMPOrganizational.3 / 2834.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *obtain and examine equipment maintenance and other relevant records to confirm sanitization equipment and sanitization processes have been tested to ensure sanitization is being achieved within at least the last six months*obtain and examine equipment maintenance and other relevant records to confirm sanitization equipment and sanitization processes have been tested to ensure sanitization is being achieved within at least the last six months**measures indicate the frequency at which the organization tests sanitization equipment and procedures to ensure that the sanitization is being achieved. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization tests sanitization equipment and procedures at least every six months to ensure that the intended sanitization is being achieved**measures indicate the frequency at which the organization tests sanitization equipment and procedures to ensure that the sanitization is being achieved. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization tests sanitization equipment and procedures at least every six months to ensure that the intended sanitization is being achieved.

Question Requirement Record: 1781.10a1Organizational.23 / 1227.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *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. Results of the identification are documented and reviewed by all stakeholders. Select a sample of software packages that were developed or purchased and confirm that the organization assessed security controls that wer*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. Results of the identification are documented and reviewed by all stakeholders. Select a sample of software packages that were developed or purchased and confirm that the organization assessed security controls that wer**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 b**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 *and the* and the**,**, supplement*ation of*ation of**ed by**ed by manual controls *if requir* if requir**as needed, and these considerations are also applied when evaluating software packages, developed or purchas**as needed, and these considerations are also applied when evaluating software packages, developed or purchased.

Question Requirement Record: 1535.11b1Organizational.12 / 1457.0

Change Count: 1

Field	Content
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 violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.

Question Requirement Record: 11.01e1System.2 / 2366.0

Change Count: 2

Field	Content
RequirementStatement	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).
IllustrativeProcedureImplemented	For example, select a sample of user accounts (including user, privileged, system, shared, and seeded accounts) and privileges (e.g., user-to-role assignments, user-to-object assignments) and confirm that they were reviewed in accordance with the organization's logical access review control frequency (and not more than one year ago).

Question Requirement Record: 0407.01y1Organizational.4 / 0285.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of teleworking sites that have been appropriately evaluated and authorized in accordance to the organization's policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that prior to authorizing teleworking, the physical security of the teleworking site is evaluated and any threats/issues identified are addressed.

Question Requirement Record: 13.02e1Organizational.6 / 2316.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of systems with automation configured to assign, perform and track phishing awareness training or all training including phishing awareness. Further, measures indicate the percentage of onboarding personnel who have completed training and those that have not within the timeframe stipulated in the organization policy. Reviews, tests, or audits are completed by the organization to measure the effectiveness each year to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable organization-defined security requirements.

Question Requirement Record: 07.07a1Organizational.8 / 2363.0

Change Count: 1

Field	Content
RequirementStatement	Organizational inventories of IT assets are periodically (annually at minimum) reviewed to ensure completeness and accuracy.

Question Requirement Record: 05.09mADHICSOrganizational.1 / 3158.0

Change Count: 0

Field	Content
New Question Requirement Record	05.09mADHICSOrganizational.1 / 3158.0

Question Requirement Record: 07.10dADHICSSystem.2 / 3153.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10dADHICSSystem.2 / 3153.0

Question Requirement Record: 07.10cADHICSSystem.2 / 3152.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10cADHICSSystem.2 / 3152.0

Question Requirement Record: 06.10kADHICSOrganizational.2 / 3151.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10kADHICSOrganizational.2 / 3151.0

Question Requirement Record: 15.11cADHICSOrganizational.4 / 3150.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11cADHICSOrganizational.4 / 3150.0

Question Requirement Record: 15.11aADHICSOrganizational.4 / 3149.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11aADHICSOrganizational.4 / 3149.0

Question Requirement Record: 15.11cADHICSOrganizational.3 / 3148.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11cADHICSOrganizational.3 / 3148.0

Question Requirement Record: 14.05kADHICSOrganizational.9 / 3147.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kADHICSOrganizational.9 / 3147.0

Question Requirement Record: 14.05kADHICSOrganizational.8 / 3146.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kADHICSOrganizational.8 / 3146.0

Question Requirement Record: 14.05iADHICSOrganizational.2 / 3145.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05iADHICSOrganizational.2 / 3145.0

Question Requirement Record: 19.06dADHICSOrganizational.4 / 3139.0

Change Count: 0

Field	Content
New Question Requirement Record	19.06dADHICSOrganizational.4 / 3139.0

Question Requirement Record: 19.13nADHICSOrganizational.2 / 3144.0

Change Count: 0

Field	Content
New Question Requirement Record	19.13nADHICSOrganizational.2 / 3144.0

Question Requirement Record: 19.13fADHICSOrganizational.2 / 3143.0

Change Count: 0

Field	Content
New Question Requirement Record	19.13fADHICSOrganizational.2 / 3143.0

Question Requirement Record: 19.13pADHICSOrganizational.2 / 3142.0

Change Count: 0

Field	Content
New Question Requirement Record	19.13pADHICSOrganizational.2 / 3142.0

Question Requirement Record: 14.05kADHICSOrganizational.7 / 3141.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kADHICSOrganizational.7 / 3141.0

Question Requirement Record: 19.13qADHICSOrganizational.4 / 3140.0

Change Count: 0

Field	Content
New Question Requirement Record	19.13qADHICSOrganizational.4 / 3140.0

Question Requirement Record: 19.13qADHICSOrganizational.3 / 3138.0

Change Count: 0

Field	Content
New Question Requirement Record	19.13qADHICSOrganizational.3 / 3138.0

Question Requirement Record: 09975.01nNYDOHOrganizational.4 / 2048.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the procedure to terminate or suspend network connections (i.e., a system to system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP) is implemented. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization terminates or suspends network connections (i.e., a system to system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP). Examine measure(s) that evaluate the organization's compliance with the network connection control policy and determine if the measures address implementation of the requirements stipulated in the requirement statement. For example, measures indicate the procedure to terminate or suspend network connections (i.e., a system-to-system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP) is implemented. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization terminates or suspends network connections (i.e., a system-to-system interconnection) upon issuance of an order by the CIO, CISO, or Senior Official for Privacy (SOP).

Question Requirement Record: 13997.02eNYDOHOrganizational.1 / 2070.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of users that have received incident response training within one month after assuming the role, after required system changes, and annually thereafter. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that information system users receive documented incident response training with a month, when required by information system changes, and annually thereafter.

Question Requirement Record: 19327.13cHIPAAOrganizational.4 / 1755.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of incidents in which an accounting of disclosures was not timely and/or provided as a percentage of all accountings of disclosure. Non-compliance with the policy requirements could be part of a broader metric that considers all deviations with respect to an accounting of disclosures regardless of type of failure. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the covered entity temporarily suspends an individual's right to receive an accounting of disclosures to a health oversight organization or law enforcement official for the time specified by such organization or official if it provides a written statement that such disclosure would impede its activities.

Question Requirement Record: 15.11aHIPAAOrganizational.5 / 2329.1

Change Count: 1

Field	Content
RequirementStatement	In the event of a breach of unsecured PHI, notification of the breach is made to the HHS Secretary without unreasonable delay and in accordance with §164.408(b) and (c) of HIPAA.

Question Requirement Record: 11.01vADHICSSystem.4 / 3137.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01vADHICSSystem.4 / 3137.0

Question Requirement Record: 11.01vADHICSSystem.3 / 3136.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01vADHICSSystem.3 / 3136.0

Question Requirement Record: 07.07aADHICSOrganizational.2 / 3135.0

Change Count: 0

Field	Content
New Question Requirement Record	07.07aADHICSOrganizational.2 / 3135.0

Question Requirement Record: 14.05kADHICSOrganizational.6 / 3134.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kADHICSOrganizational.6 / 3134.0

Question Requirement Record: 15.11aADHICSOrganizational.3 / 3133.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11aADHICSOrganizational.3 / 3133.0

Question Requirement Record: 14.09tADHICSOrganizational.2 / 3132.0

Change Count: 0

Field	Content
New Question Requirement Record	14.09tADHICSOrganizational.2 / 3132.0

Question Requirement Record: 19.06dADHICSOrganizational.3 / 3131.0

Change Count: 0

Field	Content
New Question Requirement Record	19.06dADHICSOrganizational.3 / 3131.0

Question Requirement Record: 19.06cADHICSOrganizational.2 / 3130.0

Change Count: 0

Field	Content
New Question Requirement Record	19.06cADHICSOrganizational.2 / 3130.0

Question Requirement Record: 06.10hADHICSSystem.2 / 3129.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10hADHICSSystem.2 / 3129.0

Question Requirement Record: 08.09nADHICSOrganizational.2 / 3128.0

Change Count: 0

Field	Content
New Question Requirement Record	08.09nADHICSOrganizational.2 / 3128.0

Question Requirement Record: 10.09nADHICSOrganizational.1 / 3127.0

Change Count: 0

Field	Content
New Question Requirement Record	10.09nADHICSOrganizational.1 / 3127.0

Question Requirement Record: 10.01dADHICSSystem.4 / 3126.0

Change Count: 0

Field	Content
New Question Requirement Record	10.01dADHICSSystem.4 / 3126.0

Question Requirement Record: 10.01dADHICSSystem.3 / 3125.0

Change Count: 0

Field	Content
New Question Requirement Record	10.01dADHICSSystem.3 / 3125.0

Question Requirement Record: 02.01nADHICSOrganizational.2 / 3124.0

Change Count: 0

Field	Content
New Question Requirement Record	02.01nADHICSOrganizational.2 / 3124.0

Question Requirement Record: 13.02eADHICSOrganizational.2 / 3123.0

Change Count: 0

Field	Content
New Question Requirement Record	13.02eADHICSOrganizational.2 / 3123.0

Question Requirement Record: 17.03aADHICSOrganizational.2 / 3122.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03aADHICSOrganizational.2 / 3122.0

Question Requirement Record: 01.03aISO31000Organizational.1 / 2826.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the measure(s) indicate whether risk management process documentation contains documented consideration of the required elements. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization, as part of the risk management process, considers the following when specifying risk criteria: the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible), how consequences (both positive and negative) and likelihood will be defined and measured, time-related factors, consistency in the use of measurements, how the level of risk is to be determined, how combinations and sequences of multiple risks will be taken into account, and the organization’s capacity.

Question Requirement Record: 18104.08bHIXOrganizational.1 / 0725.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of areas where the information system resides that are restricted to appropriate personnel, based on position or role, as a percentage of all areas where information is received, processed, stored, or transmitted. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization authorizes physical access to the facility where the information system resides and information is received, processed, stored, or transmitted, based on position or role.

Question Requirement Record: 19801.13eGDPROrganizational.7 / 1814.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of processing operations that produce legal or similarly significant effects that do not have, as a minimum, manual intervention in an automated decision making process. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that that, with limited exception, the organization ensures individuals are not subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly impacts the individual.

Question Requirement Record: 1589.11aGDPROrganizational.1 / 1446.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the notification times for all personal data breaches over a specified reporting period, such as monthly or quarterly, or could provide the number of notifications that were reported in phases as a percentage of all notifications over the reporting period.. Another example would be the number of notifications that did not include all the required reporting elements, as a percentage of all notifications. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the entity notifies the appropriate supervisory authority of personal data breaches without undue delay.

Question Requirement Record: 17109.10aFTIOrganizational.3 / 1258.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *for organizations using a consolidated data center, confirm that as part of the contract a Service Level Agreement (SLA) exists between the organization authorized to r*for organizations using a consolidated data center, confirm that as part of the contract a Service Level Agreement (SLA) exists between the organization authorized to r**measures indicate the number of consolidated data centers the organization is using where a Service Level Agreement (SLA) does not exist, as a percentage of contracts with consolidated data centers. Reviews, tests, or audits are completed by the organization to measure the eff**measures indicate the number of consolidated data centers the organization is using where a Service Level Agreement (SLA) does not exist, as a percentage of contracts with consolidated data centers. Reviews, tests, or audits are completed by the organization to measure the effec*e*e**t**tive *FTI and the data* FTI and the data**ness of the implemented**ness of the implemented c*e*e**o**ont*er. Examine the SLA to confirm that it contains metrics to monitor*er. Examine the SLA to confirm that it contains metrics to monitor**rols and to confirm that organizations using a consolidated data center implement appropriate**rols and to confirm that organizations using a consolidated data center implement appropriate controls *for*for **to ensure**to ensure the protection of FTI**, including a Service Level Agreement (SLA) between the organization authorized to receive FTI and the data center**, including a Service Level Agreement (SLA) between the organization authorized to receive FTI and the data center.

Question Requirement Record: 17107.10aFTIOrganizational.1 / 1256.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *examine written development policies and procedure*examine written development policies and procedure **measures indicate the number of information system acquisition contracts where security requirements and/or security specifications were not defined explicitly or by reference, as a percentage of such contracts. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented control** measures indicate the number of information system acquisition contracts where security requirements and/or security specifications were not defined explicitly or by reference, as a percentage of such contracts. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and **to** to confirm that *for*for**whenever information**whenever information systems contain*ing*ing FTI, the organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.

Question Requirement Record: 0133.05bFTIOrganizational.3 / 0465.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the me*tric*tric**asure(s)**asure(s) could indicate the number of inappropriate disclosures of FTI from the data warehouse(s) as a percentage of all disclosures (transactions/queries) or indicate the number of controls associated with the data warehouse(s) that are deficient (e.g., not in place, have failed or otherwise not operating as intended) as a percentage of all controls associated with the data warehouse(s).

Question Requirement Record: 1518.11c2Organizational.13 / 1463.0

Change Count: 1

Field	Content
RequirementStatement	Following an incident, audit trails and evidence *is*is**are**are collected and secured, as appropriate for: internal problem analysis; use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings (e.g., under computer misuse or data protection legislation); and negotiating for compensation from software and service suppliers. Actions to recover from security breaches and correct system failures are carefully and formally controlled. The procedures ensure that: only clearly identified and authorized personnel are allowed access to live systems and data; all emergency actions taken are documented in detail; damage is minimized through the containment of the incident, restoration of systems, and preservation of data and evidence; emergency action is reported to management and reviewed in an orderly manner; the integrity of business systems and controls is confirmed with minimal delay; and stakeholders are notified immediately when a safe and secure environment has been restored.

Question Requirement Record: 1103.01a2Organizational.3 / 0015.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, the measure(s) indicate the number of users that receive communication of the access control program. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that access controls are consistently managed for all systems and applications in networked and distributed environments based on the classification of the information and the risks to the information stored, processed, or transmitted.

Question Requirement Record: 1168.01e2System.2 / 0102.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of user account reviews performed by the organization for privileged and all other accounts. The metric also includes the number of accounts reviewed as a percentage of all accounts. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization reviews critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.

Question Requirement Record: 1310.01y2Organizational.1 / 0283.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of teleworking users that received training is prior to authorization as a percent of all teleworkers. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that personnel who telework are trained on the risks, controls implemented, and their responsibilities.

Question Requirement Record: 11154.02i2Organizational.3 / 0379.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of terminated employees/contractors accounts that have been restricted or removed 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 verify that access rights to information assets and facilities are reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors.

Question Requirement Record: 1581.02f2Organizational.4 / 0363.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of record and signature falsifications. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that individuals are held accountable and responsible for actions initiated under their electronic signatures.

Question Requirement Record: 1336.02e2Organizational.10 / 0336.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of security awareness and training sessions given per year. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization's security awareness and training program will identify how workforce members are provided security awareness and training content; identify the workforce members (including managers, senior executives, and as appropriate, business partners, vendors and contractors) who will receive security awareness and training content; describe the types of security awareness and training content that is reasonable and appropriate for its workforce members; how workforce members are provided security awareness and training content when there is a change in the organization's information systems; and how frequently security awareness and training content is provided to all workforce members.

Question Requirement Record: 06.10hUKAISystem.1 / 3157.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10hUKAISystem.1 / 3157.0

Question Requirement Record: 19.07eUKAIOrganizational.1 / 3156.0

Change Count: 0

Field	Content
New Question Requirement Record	19.07eUKAIOrganizational.1 / 3156.0

Question Requirement Record: 14.05kADHICSOrganizational.10 / 3154.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kADHICSOrganizational.10 / 3154.0

Question Requirement Record: 19.13fPHIPAOrganizational.4 / 2737.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of instances in which the organization received a request from an individual for access to a record of PHI and concluded that the record does not exist, cannot be found, or is not an applicable record. For each sampled instance, examine evidence to determine that a written notice was provided to the individual.

Question Requirement Record: 1852.08bFTIOrganizational.2 / 0721.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of facilities with access to FTI that are appropriately secured in accordance with the organization's policy, as a percentage of all areas with access to FTI. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify that the organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility in areas where FTI is received, processed, stored, or transmitted.

Question Requirement Record: 1798.10a3Organizational.2 / 1244.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *the control addresses actions taken by organizations in the design and development of information systems. Examine the written information security architecture policy and procedures and confirm that it: (i)*the control addresses actions taken by organizations in the design and development of information systems. Examine the written information security architecture policy and procedures and confirm that it: (i)**reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization develops an information security architecture for the information system that**reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization develops an information security architecture for the information system that describes**:**: the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; *(ii) describes* (ii) describes how the information security architecture is integrated into and supports the enterprise architecture; and*, (iii) describes*, (iii) describes any information security assumptions about, and dependencies on, external services.

Question Requirement Record: 1797.10a3Organizational.1 / 1243.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *the integration of information security requirements and associated security controls into*the integration of information security requirements and associated security controls into**measures indicate the number of security and privacy requirements not addressed in** measures indicate the number of security and privacy requirements not addressed in the organization*s*'**s** enterprise architecture *helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly rela* helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly rela**, as a percentage of such requirements. Reviews, tests, or audits are comple**, as a percentage of such requirements. Reviews, tests, or audits are completed *to* to**by**by the organization*s' mission/business processes. Examine written policies and procedure*s' mission/business processes. Examine written policies and procedure **to measure the effectiveness of the implemented control** to measure the effectiveness of the implemented controls and **to** to confirm that the organization develop*ed it*ed its enterprise architecture with consideration for information security and *privacy and* privacy and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

Question Requirement Record: 17101.10a3Organizational.6 / 1248.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of applicable development changes where developers did not satisfy the requirements as stipulated in the organization requirement statement. Measures also could indicate how such non-compliant requirements were mitigated and whether or not non-compliance was mitigated prior to deployment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of developer compliance with providing: a description of the functional properties of the security controls to be employed; and design and implementation information for the security controls to be employed that includes security-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security control implementation.

Question Requirement Record: 1135.02i3Organizational.1 / 0378.0

Change Count: 1

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

Question Requirement Record: 1817.08d3Organizational.12 / 0737.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of the organization's facility that have automated water detection mechanisms appropriately installed 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 verify that water detection devices/systems detected leaks or flooding.

Question Requirement Record: 1770.09i2System.4 / 0863.1

Change Count: 2

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

Question Requirement Record: 17.02dCOBITOrganizational.1 / 3086.0

Change Count: 0

Field	Content
New Question Requirement Record	17.02dCOBITOrganizational.1 / 3086.0

Question Requirement Record: 15.11aTBCCOrganizational.3 / 3085.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11aTBCCOrganizational.3 / 3085.0

Question Requirement Record: 15.11aTBCCOrganizational.2 / 3084.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11aTBCCOrganizational.2 / 3084.0

Question Requirement Record: 15.11aTBCCOrganizational.1 / 3083.0

Change Count: 0

Field	Content
New Question Requirement Record	15.11aTBCCOrganizational.1 / 3083.0

Question Requirement Record: 07.10mAUSOrganizational.1 / 3081.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mAUSOrganizational.1 / 3081.0

Question Requirement Record: 12.09aaNYDOHSystem.3 / 3080.0

Change Count: 0

Field	Content
New Question Requirement Record	12.09aaNYDOHSystem.3 / 3080.0

Question Requirement Record: 12.09aaNYDOHSystem.2 / 3079.0

Change Count: 0

Field	Content
New Question Requirement Record	12.09aaNYDOHSystem.2 / 3079.0

Question Requirement Record: 07.10mGovRAMPOrganizational.3 / 3076.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10m*State*State**Gov**GovRAMPOrganizational.*2*2**3**3

Question Requirement Record: 11.01qGovRAMPSystem.2 / 3075.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01q*State*State**Gov**GovRAMPSystem.*1*1**2**2

Question Requirement Record: 12.09hGovRAMPSystem.2 / 3074.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09h*State*State**Gov**GovRAMPSystem.*1*1**2**2

Question Requirement Record: 11.01bGovRAMPSystem.3 / 3073.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01b*State*State**Gov**GovRAMPSystem.*2*2**3**3

Question Requirement Record: 07.10mGovRAMPOrganizational.4 / 3072.0

Change Count: 1

Field	Content
BaselineUniqueId	07.10m*State*State**Gov**GovRAMPOrganizational.*1*1**4**4

Question Requirement Record: 12.09abGovRAMPSystem.2 / 3071.0

Change Count: 1

Field	Content
BaselineUniqueId	12.09ab*State*State**Gov**GovRAMPSystem.*1*1**2**2

Question Requirement Record: 11.01bGovRAMPSystem.4 / 3070.0

Change Count: 1

Field	Content
BaselineUniqueId	11.01b*State*State**Gov**GovRAMPSystem.*1*1**4**4

Question Requirement Record: 07.10eAISecSystem.1 / 3068.0

Change Count: 1

Field	Content
RequirementStatement	Unless specifically required, the AI system actively filters or otherwise prevents sensitive data (e.g., personal phone numbers) contained within generative AI model outputs from being shown to end users of the AI system.

Question Requirement Record: 11.01cAISecSystem.9 / 3058.0

Change Count: 1

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 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).

Question Requirement Record: 12.09abAISecSystem.3 / 3039.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, review the AI application to confirm it allows a human operator to evaluate AI model outputs before relying on them. Further, confirm the ability for human operators to intervene in AI model-initiated actions (e.g., sending emails, modifying records) if deemed necessary.

Question Requirement Record: 17.03dDORAOrganizational.2 / 3030.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of internal testers that have been approved by the appropriate authority. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization contracts internal testers for Threat Led Penetration Testing (TLPT), the organization ensures the use of the testers has been approved by the appropriate authority, the testers have sufficient dedicated resources, conflicts of interest are avoided throughout the design and execution phases of the test, the threat intelligence provider is external to the financial entity, and external testers are contracted at least every three tests.

Question Requirement Record: 15.09tDORAOrganizational.1 / 3028.0

Change Count: 2

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of information sharing arrangements and examine evidence to confirm the agreements defined the conditions for participation. Further, examine evidence the information sharing arrangements detailed, as necessary, the involvement of public authorities, the involvement of information security system third-party service providers, and the operational elements.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of information sharing arrangements that did not define the conditions for participation. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization's information sharing arrangements include documentation of the conditions for participation, the details on the involvement of public authorities as necessary, the involvement of information security system third-party service providers as necessary, and the operational elements, including the use of dedicated IT platforms as necessary.

Question Requirement Record: 14.09eDORASystem.1 / 3027.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of critical information system third-party service providers located in a third country that have not established a subsidiary in the European Union within the past 12 months. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm if services of a critical information system are provided by a third-party service provider in a third country, the organization ensures the third-party service provider has established a subsidiary in the European Union within the previous 12 months.

Question Requirement Record: 14.05kDORAOrganizational.5 / 3023.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of third-party providers of information system services for which the frequency of audits and inspections and the areas to be audited are documented. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization, using a risk-based process, determines and documents the frequency of audits and inspections and the areas to be audited at third-party providers of information system services.

Question Requirement Record: 19.13aCMSOrganizational.1 / 3008.0

Change Count: 1

Field	Content
RequirementStatement	The organization reviews all Privacy Act exemptions claimed for the system of records every 3 years to ensure they remain appropriate and necessary in accordance with law, they have been promulgated as regulations, and they are accurately described in the system of records notice.

Question Requirement Record: 10.01dCMSSystem.9 / 3007.0

Change Count: 1

Field	Content
RequirementStatement	The information system, for password-based authentication, meets or exceeds the following minimum password requirement: minimum length of eight characters for regular user passwords, and minimum length of 15 characters for administrator or privileged user passwords; minimum of three character(s) from the three character categories (A-Z, a-z, 0-9); and no reuse from last 12 passwords.

Question Requirement Record: 07.10mOWASPOrganizational.7 / 2988.0

Change Count: 3

Field	Content
RequirementStatement	The organization employs regularissszzation techniques (e.g., L1 or L2 regularization) to prevent overfitting of the model to the training data.
IllustrativeProcedureImplemented	For example, examine documentation to confirm the organization employed regularissszzation techniques (e.g., L1 or L2 regularization) to prevent overfitting of the model to the training data.
IllustrativeProcedureMeasured	For example, measures indicate the percentage of models for which regularissszzation techniques were employed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization employs regularissszzation techniques (e.g., L1 or L2 regularization) to prevent overfitting of the model to the training data.

Question Requirement Record: 19.13aTMRPAOrganizational.1 / 2986.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of electronic disclosures of PHI in which notice was not provided. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization, acting as a covered entity, provides notice to an individual for whom the organization creates or receives PHI if the individual's PHI is subject to electronic disclosure.

Question Requirement Record: 17.10kNIST80053Organizational.3 / 1240.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, *new and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. Select a sample of software development changes and examine the development records to ensure that testing (e.g., unit testing, static code analysis, data flow analysis, metrics analysis,*new and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. Select a sample of software development changes and examine the development records to ensure that testing (e.g., unit testing, static code analysis, data flow analysis, metrics analysis,**measures indicate the number of software development changes where testing was not performed during the development process, as a percentage of software development changes for a specified period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organizations developing software or systems**measures indicate the number of software development changes where testing was not performed during the development process, as a percentage of software development changes for a specified period. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organizations developing software or systems pe*e*er *code reviews) was performed* code reviews) was performed**form thorough testing and verification**form thorough testing and verification during the development process.

Question Requirement Record: 07.10eOWASPSystem.2 / 2963.0

Change Count: 2

Field	Content
RequirementStatement	The information system continuously validates AI model output against an appropriate test set to detect sudden changes or bias caused by attacks (e.g., data or model poisoning) **or gradual changes in behavior affecting security** or gradual changes in behavior affecting security.

IllustrativeProcedureMeasured	For example, measures indicate the percentage AI model outputs which were continuously validated. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the information system continuously validates AI model output against an appropriate test set to detect sudden changes or bias caused by attacks (e.g., data or model poisoning) **or gradual changes in behavior affecting security** or gradual changes in behavior affecting security.

Question Requirement Record: 07.10mAISecOrganizational.4 / 2913.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of text based model output that is encoded. Reviews, tests, or audits are completed by the **organization to measure the effectiveness of the implemented controls and to confirm the** organization to measure the effectiveness of the implemented controls and to confirm the information system applies output encoding to textual AI model output to prevent traditional injection attacks (e.g., remote code execution) which can create a vulnerability when processed.

Question Requirement Record: 17.03bGovRAMPOrganizational.2 / 2916.0

Change Count: 4

Field	Content
BaselineUniqueId	17.03b*State*State**Gov**GovRAMPOrganizational.*1*1**2**2
RequirementStatement	The organization accepts the results of an assessment of any *State*State**Gov**GovRAMP Accredited 3PAO performed by any *State*State**Gov**GovRAMP Accredited 3PAO when the assessment meets the conditions of the SAC/Sponsor in the *State*State**Gov**GovRAMP Repository.
IllustrativeProcedureImplemented	For example, select a sample of accepted assessments and obtain evidence to determine if they were performed by *State* State**Gov**GovRAMP Accredited 3PAO and met the conditions of the SAC/Sponsor in the *State*State**Gov**GovRAMP Repository.
IllustrativeProcedureMeasured	For example, measures indicate the number of accepted results from assessments performed by any *State*State**Gov** GovRAMP Accredited 3PAO when the assessment meets the conditions of the SAC/Sponsor in the *State*State**Gov**GovRAMP Repository. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization accepts the results of an assessment of any *State*State**Gov**GovRAMP Accredited 3PAO performed by any *State*State**Gov**GovRAMP Accredited 3PAO when the assessment meets the conditions of the SAC/Sponsor in the *State*State**Gov**GovRAMP Repository.

Question Requirement Record: 01.05dGovRAMPOrganizational.2 / 2915.0

Change Count: 1

Field	Content
BaselineUniqueId	01.05d*State*State**Gov**GovRAMPOrganizational.*1*1**2**2

Question Requirement Record: 08.09nGovRAMPOrganizational.2 / 2914.0

Change Count: 1

Field	Content
BaselineUniqueId	08.09n*State*State**Gov**GovRAMPOrganizational.*1*1**2**2

Question Requirement Record: 07.10bATLASSystem.1 / 2868.0

Change Count: 1

Field	Content
RequirementStatement	The information system detects and blocks the following types of inputs before they reach the production machine learning model: adversarial inputs; atypical inputs that deviate from known benign behavior; inputs that exhibit behavior patterns observed in previous attacks; inputs from potentially malicious IP addresses or domains, and unexpectedly large input.

Question Requirement Record: 01.00aPCIOrganizational.1 / 2855.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate whether the PCI DSS scope was reviewe**e**d by the organization within the last six months and upon significant change to the in-scope environment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization confirms PCI DSS scope annually and upon significant change to the in-scope environment.

Changes for Authoritative Source Document View D T O - v11.4.0 to v11.5.0

Authoritative Source Document View D T O: GovRAMP r5

Change Count: 3

Field	Content
Name	*State*State**Gov**GovRAMP r5
Description	*State*State**Gov**GovRAMP is built on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments.
ShortName	*State*State**Gov**GovRAMP r5

Authoritative Source Document View D T O: NY DoH Title 10 Section 405.46

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	NY DoH Title 10 Section 405.46

Authoritative Source Document View D T O: COBIT 2019

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	COBIT 2019

Authoritative Source Document View D T O: Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)

Change Count: 0

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

Authoritative Source Document View D T O: Strategies to Mitigate Cybersecurity Incidents (Australia)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Strategies to Mitigate Cybersecurity Incidents (Australia)

Authoritative Source Document View D T O: Network and Information Security (NIS) Directive

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Network and Information Security (NIS) Directive

Authoritative Source Document View D T O: Texas Business and Commerce Code Chapter 521

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Texas Business and Commerce Code Chapter 521

Authoritative Source Document View D T O: UK Guidelines for Secure AI System Development

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	UK Guidelines for Secure AI System Development

Authoritative Source Document View D T O: Singapore MAS Notice on Cyber Hygiene

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Singapore MAS Notice on Cyber Hygiene

Authoritative Source Document View D T O: Cybersecurity Act 2018 (Singapore)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Cybersecurity Act 2018 (Singapore)

Changes for Factor Type View D T O - v11.4.0 to v11.5.0

Factor Type View D T O: Compliance - GovRAMP r5

Change Count: 4

Field	Content
Name	*State*State**Gov**GovRAMP r5
Description	*State*State**Gov**GovRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments.
Tooltip	*State*State**Gov**GovRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments.
Order	10*15*15**07**07

Factor Type View D T O: Compliance - HHS Cybersecurity Performance Goals

Change Count: 1

Field	Content
Order	100*6*6**8**8

Factor Type View D T O: Compliance - FFIEC CAT

Change Count: 1

Field	Content
Order	100*4*4**5**5

Factor Type View D T O: Compliance - HIPAA

Change Count: 1

Field	Content
Order	10**1**10*8*8

Factor Type View D T O: Compliance - Cybersecurity Maturity Model Certification (CMMC)

Change Count: 1

Field	Content
Order	100*2*2**3**3

Factor Type View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1

Change Count: 1

Field	Content
Order	1001122

Factor Type View D T O: Compliance - CIS CSC v8.0

Change Count: 1

Field	Content
Order	1000011

Factor Type View D T O: Compliance - GDPR

Change Count: 1

Field	Content
Order	1005566

Factor Type View D T O: Compliance - FedRAMP r5

Change Count: 1

Field	Content
Order	1003344

Factor Type View D T O: Compliance - HICP 2023 Edition

Change Count: 1

Field	Content
Order	1007799

Factor Type View D T O: Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)

Factor Type View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia)

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia)

Changes for Factor View D T O - v11.4.0 to v11.5.0

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NY DOH System Security Plan v5 Critical Controls Attestation Overlay

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - NY DOH System Security Plan v5 Critical Controls Attestation Overlay

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Network and Information Security (NIS) Directive

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - Network and Information Security (NIS) Directive

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Texas Business and Commerce Code Chapter 521

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - Texas Business and Commerce Code Chapter 521

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - UK Guidelines for Secure AI System Development

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - UK Guidelines for Secure AI System Development

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Singapore MAS Notice on Cyber Hygiene

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - Singapore MAS Notice on Cyber Hygiene

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Cybersecurity Act 2018 (Singapore)

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - Cybersecurity Act 2018 (Singapore)

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NY DOH Title 10 Section 405.46

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - NY DOH Title 10 Section 405.46

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - COBIT 2019

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - COBIT 2019

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - VA Directive 6500

Change Count: 1

Field	Content
Order	*41*41**50**50

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - State of Nevada Security and Privacy of Personal Information

Change Count: 1

Field	Content
Order	**4**43*5*5

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - PDPA (Singapore)

Change Count: 1

Field	Content
Order	3*2*2**8**8

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Texas Medical Records Privacy Act

Change Count: 1

Field	Content
Order	*37*37**46**46

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Supplemental Requirements

Change Count: 1

Field	Content
Order	3636444

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - State of Massachusetts Data Protection Act (201 CMR 17.00)

Change Count: 1

Field	Content
Order	33422

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - SCIDSA

Change Count: 1

Field	Content
Order	33399

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - The Joint Commission v2016

Change Count: 1

Field	Content
Order	38384747

Factor View D T O: Compliance - GovRAMP r5 - Readiness

Change Count: 0

Field	Content
New Factor View D T O	Compliance - GovRAMP r5 - Readiness

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-171 r3

Change Count: 1

Field	Content
Order	26677

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - OWASP ML Top 10

Change Count: 1

Field	Content
Order	30066

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST Cybersecurity Framework 2.0

Change Count: 1

Field	Content
Order	25566

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-172

Change Count: 1

Field	Content
Order	27788

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - OWASP AI Exchange

Change Count: 1

Field	Content
Order	29293535

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - PCI DSS v4.0

Change Count: 1

Field	Content
Order	31177

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - TX-RAMP 2.0

Change Count: 1

Field	Content
Order	40088

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

Change Count: 1

Field	Content
Order	28283131

Factor View D T O: Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Service Provider

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Service Provider

Factor View D T O: Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Advanced

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Advanced

Factor View D T O: Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Transitional

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Transitional

Factor View D T O: Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Basic

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) - Basic

Factor View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Limited

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Limited

Factor View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Good

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Good

Factor View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Very Good

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Very Good

Factor View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Excellent

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Excellent

Factor View D T O: Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Essential

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Strategies to Mitigate Cybersecurity Incidents (Australia) - Essential