Version 9.4 Summary of Changes

Incorporates changes stemming from the incorporation of the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC) Framework

June 2020

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

Fundamental to HITRUST's mission is the availability of a common security and privacy framework, the HITRUST CSF ("CSF"), which provides the needed structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their data protection compliance. The initial development of the CSF leveraged nationally and internationally accepted security and privacy related regulations, standards, and frameworks—including ISO, NIST, PCI, HIPAA, and COBIT—to ensure a comprehensive set of security and privacy controls. The CSF standardizes these requirements, providing clarity and consistency and reducing the burden of compliance.

HITRUST ensures the CSF stays relevant and current to the needs of organizations by regularly updating the CSF to integrate and normalize applicable requirements and best practices as authoritative sources.

In developing a framework that can meet the needs of organizations locally, nationally, and globally, HITRUST recognizes that various organizations may have requirements imposed as a result of being part of a smaller community—such as a subset of an industry group, a State Agency, or by a cooperative sharing agreement. In many cases, these may not be new security or privacy controls but more specific implementation requirements. HITRUST has established a mechanism in the HITRUST CSF, that is enabled through MyCSF for these requirements to be incorporated, harmonized, and selected for inclusion during the assessment process and then included in the HITRUST CSF Assessment Report. The intent is to reduce any additional assessments by enabling organizations to Assess Once, Report Many™. HITRUST CSF v9.4 includes such community standards and we are evaluating the inclusion of others based on market demand.

The HITRUST CSF v9.4 release includes changes based on feedback from the HITRUST community; miscellaneous corrections; clarification and enhancement of certain illustrative procedures to ensure alignment with the corresponding authoritative sources; incorporation of regulatory requirements from the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC), as well as the inclusion of a community-specific authoritative source, currently referred to as Supplemental Requirements or Community Supplemental Requirements (CSR). These updates reflect HITRUST's commitment to provide a framework fitting for any organization globally. Organizations required or choosing to include community supplemental requirements (CSR) can select them with other regulatory factors under the Admin & Scoping section of the MyCSF platform.

Minor administrative updates, such as the correction of grammar or formatting errors, are generally not reflected in the Summary of Changes. Simple mapping updates from one version of a source to a newer version, which do not impact existing content, are also generally not reflected.

The table below provides a summary of the changes to the CSF broken down by Control Specification and Implementation Requirement Level.

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

CSF Control	Control Level	BUID	Requirement Statements Added to HITRUST CSF v9.4
01.n	CMMC	08921.01nCMMCSystem.1	Added: The organization uses encrypted sessions for the management of network devices.
06.f	CMMC	19922.06fCMMCSystem.1	Added: The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards when used to protect the confidentiality of information.
09.m	CMMC	08920.09mCMMCOrganizational.1	Added: The organization establishes and maintains a security operations center capability that facilitates 24/7 incident detection and response.
09.m	CMMC	08923.09mCMMCOrganizational.2	Added: The organization employs advanced analytics to test untrusted code and/or programs traversing through the network or system boundaries, in order to detect and block malicious content.
01.d	Supplemental Requirements	10902.01dSRSystem.1	Added: Authentication credentials are provided using a secure method.
01.q	Supplemental Requirements	11903.01qSRSystem.1	Added: Maintain individual ownership and accountability for use of all service accounts.
01.t	Supplemental Requirements	11904.01tSRSystem.1	Added: A time-out mechanism (e.g., screensaver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed.

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

05.k	Supplemental Requirements	14908.05kSROrganizational.1	Added: Supplier complies to requirements under the supplier agreement, including maintaining and adhering to documented processes for (i) reviewing and scanning software developed or customized for the organization to find and remediate malicious code and/or security vulnerabilities prior to initial deployment, and making scan results and remediation plans available to the organization upon request; (ii) cooperating with the organization and taking all reasonable and necessary steps to isolate, mitigate, terminate, and/or remediate all known or suspected threats within 90 days of notification of a threat to the organization or its customers' nonpublic information resources originating from the supplier's network; and (iii) notifying and cooperating with the organization upon discovery of a supplier's noncompliance with the organization's security requirements, or of a known or suspected threat/vulnerability impacting the organization or its customers, and to take all reasonable and necessary steps to isolate, mitigate, and/or remediate such noncompliance or threat/vulnerability within 90 days.
05.k	Supplemental Requirements	14912.05kSROrganizational.2	Added: Supplier maintains and adheres to any business continuity plan and/or disaster recovery plan requirements under the agreement.
06.c	Supplemental Requirements	19906.06cSROrganizational.1	Added: Guidelines are issued by the organization on the ownership, classification, retention, storage, handling, return, and disposal of all records and information.
06.c	Supplemental Requirements	19907.06cSRSystem.4	Added: Separation between operational information and non-production (development, test/quality assurance) environments is maintained.
06.c	Supplemental Requirements	19910.06cSROrganizational.2	Added: The organization maintains controls to detect and terminate unauthorized attempts to access, modify, store, and/or handle in-scope information.

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

06.c	Supplemental Requirements	19911.06cSROrganizational.3	Added: The confidentiality and integrity of information is protected at rest and in transit in the following scenarios using a cryptographic algorithm with minimum key lengths of 256 bits for symmetric and 2048 bits for asymmetric, and proper key management practices including keys with a maximum lifetime of two years for: (i) all in-scope information (ISI) transmitted over untrusted networks; (ii) all ISI stored or transmitted using mobile and portable devices; (iii) all wireless networking technologies used to transmit ISI; (iv) all ISI stored within, or transmitted to, from, and within non-organizational cloud services; and (v) all sensitive personal information (SPI)/sensitive customer data (SCD) stored or transmitted over all networks, including trusted networks.
09.d	Supplemental Requirements	06900.09dSRSystem.1	Added: Separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.
09.f	Supplemental Requirements	14909.09fSROrganizational.1	Added: Supplier (i) ensures all supplier entities performing any in-scope work are contractually obligated to comply with the organization's security requirements, or requirements that are no less stringent; (ii) ensure the use of the organization's information resources and in-scope information by supplier entities will only be for the performance of in-scope work; (iii) maintain and adhere to a documented program by which supplier entity compliance to the organization's security requirements is evaluated by supplier and all corrective actions are documented and implemented; and (iv) upon the organization’s request, supplier will provide documentation and/or evidence to adequately substantiate such compliance.
09.h	Supplemental Requirements	16905.09hSRSystem.1	Added: The organization protects against or limits the effects of various types of denial-of-service attacks, including distributed denial-of-service attacks.

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST’s prior written permission.

10.m	Supplemental Requirements	07901.10mSROrganizational.1	Added: Maintain and adhere to a documented process to remediate all critical, high, and medium risk security vulnerabilities promptly.

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

CSF Control	Control Level	Summary of Changes	Remarks
01.b	1	Updated: Examine policies and/or standards related to user registration and de-registration and determine if requirements are defined for the following: i. Communicate password procedures and policies to all users who have system access (See 01b.1.9); ii. access to the information systems is granted based on minimum necessary for assigned official duties, intended system usage and personnel security criteria such that usage/access is granular enough to support an individual's consent that has been captured by the organization and limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function; iii. communicate password procedures and policies to all users who have system access; iv. check that the user has authorization from the system owner for the use of the information system or service; v. separate approval for access rights from management; vi. check that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy (e.g., it is consistent with sensitivity and risks associated with the information and/or information system, and it does not compromise segregation of duties); vii. give users a written statement of their access rights; viii. require users to sign statements indicating that they understand the conditions of access; ix. ensure service providers do not provide access until authorization procedures have been completed; x. ensure default accounts are removed and/or renamed; xi. maintain a formal record of all persons registered to use the service; xii. remove or block critical access rights of users who have changed roles or jobs or left the organization immediately and remove or block non-critical access within twenty-four (24) hours; and xiii. automatically remove or disable accounts within ninety (90) days that have been inactive for a period of sixty (60) days or more.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1109.01b1System.479)
01.d	2	Updated: Examine policies and/or standards related to password management and determine if persons who use electronic signatures based upon use of identification codes in combination with passwords	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s).

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		employ controls to ensure their security and integrity, which include the following: i. maintaining the uniqueness of each combined identification code and password, such that no two (2) individuals have the same combination of identification code and password. ii. ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging); iii. following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls; iv. use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report, in an immediate and urgent manner, any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and v. initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	(1010.01d2System.5)

01.d	CMS	Updated:
		
		Examine policies and/or standards related to password management and determine if the organization enforces the following minimum password requirements (User/Privileged):
		i. Minimum Password Age = 1/1;
		ii. Maximum Password Age = 60/60;
		iii. Minimum Password Length = 8/8;
		iv. Password Complexity = 1/1 (minimum one (1) character from the four (4) character categories (A-Z, a-z, 0-9, special characters); and
		v. Password History Size = 6.
			Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s).
			(1016.01dCMSSystem.1)

01.p	2	Updated: Examine policies and/or standards related to secure log-on procedures and determine if the procedure for logging into an operating system is designed to minimize the opportunity for unauthorized access. The log-on procedure will therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. The log-on procedures: i. limit the number of unsuccessful log-on attempts allowed to three attempts, and enforce: 1. disconnecting data link connections; 2. sending an alarm message to the system console if the maximum number of log-on attempts is reached;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (11103.01p2Organizational.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		and 3. setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected; 4. limit the maximum and minimum time allowed for the log-on procedure, if exceeded, the system terminates the log-on; 5. not transmit usernames and passwords in clear text over the network; 6. not display system or application identifiers until the log-on process has been successfully completed; 7. not provide help messages during the log-on procedure that would aid an unauthorized user; and 8. validate the log-on information only on completion of all input data. If an error condition arises, the system does not indicate which part of the data is correct or incorrect.	
01.v	1	Updated: Access rights to applications and application functions ~~are limited to the minimum necessary using menus.~~ should be restricted in accordance with the access control policy.	Requirement Statement updated to provide further clarity and alignment with the authoritative source(s). (1129.01v1System.12)
01.v	1	Updated: Examine policies and/or standards related to information access restriction and determine whether ~~business applications provide menus to control access to application system functions and controls access rights of users (e.g., read, write, delete, and execute).~~ the requirements for controlling access to applications and application functions are addressed, such as, but not exclusive to: (i) providing menus to control access to application system functions; (ii) controlling which data can be accessed by a particular user; (iii) controlling the access rights of users, e.g. read, write, delete and execute; (iv) controlling the access rights of other applications; (v) limiting the information contained in outputs; and (vi) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1129.01v1System.12)
01.v	1	Updated: For ~~application security,~~ controlling access to applications and application functions, validate written procedures exist and confirm each element of the policy/control requirements stipulated in the policy level are addressed. Interview responsible parties to confirm the procedures address all required elements of the policy/control requirements, irrespective of the existence of a written policy/procedure. Notate the responsible parties understanding of the procedures, as implemented, and compare against any existing written procedures to validate consistency.	Illustrative Procedure Process updated to provide further clarity and alignment with the authoritative source(s). (1129.01v1System.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

01.v	1	Updated: For ~~application security,~~ controlling access to applications and application functions, evidence policy/control requirements stipulated in the policy level have been implemented, e.g., examine relevant documentation, observe relevant processes, interview responsible parties. For example, select a sample of applications, and examine the access rights setting and determine whether ~~users access rights have been limited through the use of application menus. Further, observe the functionality of the application and confirm that application menus have been implemented to restrict access to information based on access privilege.~~ the system has restricted access rights to applications and application functions in accordance with the access control policy.	Illustrative Procedure Implemented updated to provide further clarity and alignment with the authoritative source(s). (1129.01v1System.12)
01.v	1	Updated: Examine measure(s) that evaluate the organization's compliance with the ~~information security~~ access control policies and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated in the policy level. For example, the measure(s) indicate % of the organization's business applications where access rights and application functions that have been configured to restrict access 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 confirm that the organization requires that access rights to applications and application functions are limited to the minimum necessary using menus.~~ system has restricted access rights to applications and application functions in accordance with the access control policy.	Illustrative Procedure Measured updated to provide further clarity and alignment with the authoritative source(s). (1129.01v1System.12)
01.x	1	Updated: Examine policies and/or standards related to mobile computing & communications and determine the following (i) The organization uses full-disk encryption to protect the confidentiality of information on laptops and other mobile devices that support full-disk encryption and is enforced through technical controls; (ii) A mobile computing policy is developed and includes the organizations definition of mobile devices, acceptable usage, and the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection; (iii) The organization installs personal firewall software or equivalent functionality on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network; (iv) Mobile computing devices are physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places (v) The organization only authorizes connections of mobile devices meeting organizational usage restrictions, configuration requirements, connection requirements, and implementation guidance; enforce requirements for the connection of mobile devices to sensitive information systems; and (vi) Information system functionality on mobile devices that provides the capability for automatic execution of code without user direction is disabled.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0401.01x1System.124579)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

01.x	FTI	Updated: Examine policies and/or standards related to mobile computing & communications and determine, if using FTI in a mobile device environment, including BYOD, the agency must meet the following mandatory requirements: i. Mobile device management controls must be in place that include security policies and procedures, inventory, and standardized security configurations for all devices; ii. An annual risk assessment must be conducted on the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI; iii. Protection mechanisms must be in place in case a mobile device is lost or stolen all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards; iv. All data communication with the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 compliant; v. The agency must control end-user ability to download only authorized applications to the device and must limit the accessibility to FTI by applications to only authorized applications; vi. All mobile device management servers that receive, process, store, or transmit FTI must be hardened; vii. A centralized mobile device management solution must be used to authenticate agency-issued and personally owned mobile devices prior to allowing access to the internal network; viii. Security events must be logged for all mobile devices and the mobile device management server; ix. The agency must disable wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage; x. Access to hardware, such as the digital camera, global positioning system (GPS), and universal serial bus (USB) interface, must be disabled to the extent possible; and xi. Disposal of all mobile device component hardware follows the same media sanitization and disposal procedures as other media.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0413.01xFTIOrganizational.2)
02.c	1	Updated: Examine policies and/or standards related to the terms and conditions of employment to determine if the terms and conditions of employment reflect the organization's security policy, while also clarifying and stating the following: i. that all employees, contractors and third-party users who are given access to covered information sign a confidentiality or non-disclosure agreement prior to being given access to information assets; ii. the employee's, contractor's and any other user's legal responsibilities and rights (e.g. regarding copyright laws or data protection legislation); iii. responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third-party user; iv. responsibilities of the employee, contractor or third-party user for the handling of information received	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0150.02c1Organizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		from other companies or external parties; v. responsibilities of the organization for the handling of covered information, including covered information created as a result of, or in the course of, employment with the organization; vi. responsibilities that are extended outside the organization's premises and outside normal working hours (e.g. in the case of home-working); vii. actions to be taken if the employee, contractor or third-party user disregards the organization's security requirements; and viii. ensure that conditions relating to security policy survive the completion of the employment in perpetuity.	
02.e	2	Updated: Examine policies and/or standards related to information security awareness, education, and training and determine whether the organization formally creates dedicated security awareness training as part of a resource on-boarding process to the organization, the training process is formally documented, and includes the recognition and reporting of potential indicators of an insider threat. The organizations awareness program: i. focuses on the methods commonly used in intrusions that can be blocked through individual action; ii. delivers content in short online modules convenient for employees; iii. receives frequent updates (at least annually) to address the latest attack techniques; and iv. includes the senior leadership teams personal messaging and involvement.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1302.02e2Organizational.134)
03.a	1	Updated: Examine policies and/or standards related to risk management to determine whether the organization has developed a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems, including physical and environmental hazards; implement the strategy consistently across the organization, and ensure that their information protection programs do not apply safeguards unnecessarily, e.g., to de-identified information. The elements of the risk management program include: (i) objectives of the risk management process; (ii) management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; (iii) the plan for managing operational risk communicated to stakeholders; (iv) the connection between the risk management policy and the organization's strategic planning processes; and documented risk assessment processes and procedures. (v) regular performance of risk assessments; (vi) mitigation of risks identified from risk assessments and threat monitoring procedures; (vii) risk tolerance thresholds are defined for each category of risk; (viii) reassessment of the risk management policy to ensure management's stated level of acceptable risk is	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1701.03a1Organizational.12345678)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; (ix) updating the risk management policy if any of these elements have changed; and (x) repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	
03.a	3	Updated: Examine policies and/or standards related to risk management to determine whether the organization develops and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account that involves or is designed to permit multiple payments or transactions. The organization defines and incorporates existing policies and implement procedures to: (i) identify relevant patterns, practices, or specific activities that indicate the possible existence of identity theft for the accounts, and incorporate those patterns, practices, and activities into its program; (ii) detect patterns, practices, and activities that have been incorporated into the program; (iii) respond appropriately to any patterns, practices, and activities that are detected to prevent and mitigate identity theft; and (vi) ensure the program and patterns, practices, and activities are updated at least annually, to reflect changes in risks to customers and to the safety and soundness of the organization.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1703.03a3Organizational.123)
03.a	3	Updated: Examine policies and/or standards related to risk management to determine whether the organization has identified that ~~personally identifiable information~~ 'Personal Identifying Information' (PII) [also Personally Identifiable Information] means information that alone, or in conjunction with other information, identifies an individual, including but not limited to an individual's: (i) Name, social security number, date of birth, or government-issued identification number; (ii) Mothers maiden name; (iii) Unique biometric data, including the individuals fingerprint, voice print, and retina or iris image; (iv) Unique electronic identification number, address, or routing code; and Telecommunication access device.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1711.03a3Organizational.4)
03.b	HIPAA	Updated: Examine policies and/or standards related to performing risk assessments to determine whether risk assessments (analysis) used to ~~validate~~ determine whether a breach of unsecured Protected Health Information (PHI) as these terms are defined by the Secretary of Health and Human Services is reportable to the Secretary must demonstrate there is a low probability of compromise (lo pro co) rather than a significant risk of harm. The methodology, at a minimum, address the following factors:	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1706.03bHIPAAOrganizational.3)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		(i) the nature of the PHI involved, including the types of identifiers involved and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; (iv) the extent to which the risk to the PHI has been mitigated; and (v) and other factors/guidance promulgated by the Secretary. With respect to risk assessments (analysis) used to determine whether a breach of unsecured protected health information (PHI)as these terms are defined by the Secretary of Health and Human Services is reportable to the Secretary must demonstrate there is a low probability of compromise (lo pro co) rather than a significant risk of harm. The methodology, at a minimum, addresses the following factors: (i) the nature of the PHI involved, including the types of identifiers involved and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; (iv) the extent to which the risk to the PHI has been mitigated; and (v) other factors/guidance promulgated by the Secretary.	
03.b	GDPR	Updated: ~~Examine policies and/or standards related to risk management where data processing is likely to result in a high risk to the rights and liberties (freedoms) of natural persons, and unless (i) processing has a legal basis in EU law, or the law of the member state to which the controller is subject; (ii) that law regulates the processing in question, (iii) a data impact assessment has already been carried out as part of a general impact assessment; or, (iv) the processing has been exempted by the Supervisory Authority the data controller, prior to processing, carries out an assessment of the impact of said processing on the protection of personal data, taking into account the nature, scope, context and purposes of the processing.~~ Examine policies and/or standards related to risk management and--unless (a) processing has a legal basis in EU law or the law of the Member State to which the controller is subject, (b) that law regulates the processing in question, and (c) a data impact assessment has already been carried out as part of a general impact assessment, OR (d) the processing has been exempted by the Supervisory Authority --then where data processing is likely to result in a high risk to the rights and liberties (freedoms) of natural persons, the controller prior to processing carries out an assessment of the impact of said processing on the protection of personal data, taking into account the nature, scope, context and purposes of the processing. Determine if a data protection impact assessment is required, unless exempted, in the case of (a) a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of personal data, or of personal data relating to criminal convictions and offences; or (c) a systematic monitoring of a publicly accessible area on a large scale. Note: A single assessment may address a set of similar processing	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (17132.03bGDPROrganizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		operations that present similar high risks. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	
03.b	GDPR	Updated: Examine policies and/or standards related to risk management and determine if the ~~data~~ controller consults the supervisory authority, prior to processing, where a data protection impact assessment indicates that the processing would result in a high risk, in the absence of measures taken by the ~~data~~ controller to mitigate the risk; AND, when consulting the supervisory authority, the controller provides the supervisory authority with (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings; (b) the purposes and means of the intended processing; (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the EU GDPR; (d) where applicable, the contact details of the data protection officer; (e) the data protection impact assessment; and (f) any other information requested by the supervisory authority. Note: processing operations which are likely to result in a high risk include those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (17136.03bGDPROrganizational.5)
04.a	1	Updated: Examine policies and/or standards related to information security to determine whether the organization Information security policy is developed, published, disseminated and implemented. The information security policy documents state the purpose and scope of the policy, communicate management's commitment, describe management and workforce member's roles and responsibilities, and establish the organization's approach to managing information security. As applicable to the focus of a particular document, policies contain: (i) the organization's mission, vision, values, objectives, activities, and purpose, including the organization's place in critical infrastructure; (ii) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; (iii) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; (iv) a framework for setting control objectives and controls, including the structure of risk assessment and risk management; (v) the need for information security;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0113.04a1Organizational.123)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		(vi) the goals of information security; (vii) compliance scope; (viii) legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; (ix) arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination. (x) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization , including but not limited to CSF control objectives such as: (1) compliance with legislative, regulatory, and contractual requirements; (2) security education, training, and awareness requirements for the workforce, including researchers and research participants; (3) incident response and business continuity management; (4) consequences of information security policy violations; (5) continuous monitoring; (6) designating and maintaining an appropriately resourced and technically experienced information security team; (7) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (8) coordination among organizational entities; (x) a definition of general and specific responsibilities for information security management, including reporting information security incidents; prescribes the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls; and references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with).	
04.b	2	Updated: Examine policies and/or standards related to the information security policy to determine whether the information security policy documents has an owner who has approved management responsibility for the development, review, and evaluation of the security policy. Policies are reviewed no less than every ~~365~~ three hundred sixty five (365) days or if significant changes occur in the operating or business environment, updated/improved based on specific feedback (e.g., prior reviews, incidents and preventative/corrective actions) and approved by an appropriate level of management. The input to the management review includes information on: i. feedback from interested parties; ii. results of independent reviews (see 5.h); iii. status of preventive and corrective actions (see 5.h and 6.g); iv. results of previous management reviews; v. process performance and information security policy compliance;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0115.04b2Organizational.123)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		vi. changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment; vii. trends related to threats and vulnerabilities; viii. reported information security incidents (see 11.a); and ix. recommendations provided by relevant authorities (see 5.f).	
05.b	2	Updated: Examine policies and/or standards related to information security coordination to determine if information security coordination involves the active cooperation and collaboration across the entire organization to include managers, users, administrators, application designers, auditors and security personnel. This activity: i. involves the active cooperation and collaboration across the entire organization to include managers, users, administrators, application designers, auditors and security personnel; ii. also includes specialist skills in areas such as insurance, legal issues, human resources, privacy, IT or risk management; iii. address deviations via a risk acceptance process; iv. approves methodologies and processes for information security management activities (e.g. risk acceptance, information classification, security incidents); v. identifies and promptly reports to senior management significant threat changes and exposure of information and information processing resources to threats; vi. evaluates information received from the monitoring and reviewing of information security activities to identify "lessons learned", and recommends to senior management appropriate actions in response to identified information security incidents; vii. creates an internal security information sharing mechanism, such as an email group, periodic conference call or standing meeting; and viii. establishes an internal reporting mechanism, such as a telephone hotline or dedicated email address, to allow security contacts to report information security incidents or obtain security policy clarifications on a timely basis. An internal security information sharing mechanism has been created to ensure security-related activities affecting the information system are planned and coordinated with appropriate stakeholders before conducting such activities in order to reduce the impact on other organizational entities. The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on other organizational entities.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0128.05b2Organizational.126)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

05.c	2	Updated: Examine policies and/or standards related to the allocation of information security responsibilities to determine if the organization identifies, by name or position, non-professional or professional security contacts in each major organizational area or business unit. The organization clearly defines the roles, responsibilities and authority of each security contact including the administration and implementation of the organization's security programs. Each security contact annually documents compliance related to identified legal requirements (see CSF 06.a), reports to the organization's single point of contact for security, and provides the following at a minimum: i. evaluations on the effectiveness of the policies and procedures implemented in addressing risk; ii. evaluations of service provider arrangements (see CSF 09.e, 09.f, 09.g); iii. significant incidents and the response; and iv. recommendations for material changes to the security programs for which they are responsible. The organization's single point of contact for security matters provides supplemental security awareness and training (see 02.e). Security contacts are responsible for reviewing reports related to the security organization, network, systems and programs implemented and formally approves any material changes to these items prior to implementation.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0174.05c2Organizational.12345)
05.e	1	Updated: Examine policies and/or standards related to confidentiality agreements to determine if confidentiality or non-disclosure agreements address the requirement to protect confidential information using legally enforceable terms. Confidentiality or nondisclosure agreements include, but are not limited to, the following: i. a definition of the information to be protected (e.g. confidential information); ii. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely; iii. required actions when an agreement is terminated; iv. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know'); v. disclosures required to be limited to the limited data set (see 07.d) or the minimum necessary to accomplish the intended purpose of such use, disclosure, or request; vi. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; vii. the permitted use of confidential information, and rights of the signatory to use information; viii. individuals' rights to obtain a copy of the individual's information in an electronic format; ix. individuals' rights to have the individual's information transmitted to another entity or person designated by the individual, provided the request is clear, conspicuous, and specific; x. the right to audit and monitor activities that involve confidential information; xi. the process for notification and reporting of unauthorized disclosure or confidential information breaches;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19130.05e1Organizational.123)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		xii. terms for information to be returned or destroyed at agreement cessation; and xiii. expected actions to be taken (i.e. penalties that are possible) in case of a breach of this agreement. The confidentiality agreements are applicable to all personnel accessing covered information.	
05.g	FedRAMP	Updated: The organization receives information system security alerts, advisories, and directives ~~from US-CERT~~ on an ongoing basis. Furthermore, the organization generates and disseminates security alerts, advisories, and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities; and implements security directives in accordance with established time frames or notifies the business owner of the degree of noncompliance.	Requirement Statement updated to provide further clarity and alignment with the authoritative source(s). (17129.05gFedRAMPOrganizational.1)
05.g	FedRAMP	Updated: Examine policies and/or standards related to the contact with special interest groups to determine if the organization receives information system security alerts, advisories, and directives ~~from US-CERT~~ on an ongoing basis. Further the organization generates and disseminates security alerts, advisories and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities, and implements security directives in accordance with established time frames, or notifies the business owner of the degree of noncompliance.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (17129.05gFedRAMPOrganizational.1)
05.g	FedRAMP	Updated: For contacting special interest groups, evidence policy/control requirements stipulated in the policy level have been implemented, e.g., examine relevant documentation, observe relevant processes, interview responsible parties. Examine evidence to confirm that the organization is ~~a member of, and~~ receiving ~~notifications from, US-CERT or from other sources to receive~~ security alerts, advisories, and directives. If security directives are not implemented, confirm that the organization appropriately notifies the business owner of noncompliance.	Illustrative Procedure Implemented updated to provide further clarity and alignment with the authoritative source(s). (17129.05gFedRAMPOrganizational.1)
05.g	FedRAMP	Updated: Examine measure(s) that evaluate the organization's compliance with the information security policy and determine if the measures address implementation of the policy/control requirements stipulated in the policy level. For example, measures indicate the percent of security directives not sent to appropriate personnel in the organization. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization receives information system security alerts, advisories, and directives ~~from US-CERT~~ on an ongoing basis. Further the organization generates and	Illustrative Procedure Measured updated to provide further clarity and alignment with the authoritative source(s). (17129.05gFedRAMPOrganizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		disseminates security alerts, advisories and directives to organization-defined personnel with roles in system administration, monitoring, and/or security responsibilities, and implements security directives in accordance with established time frames, or notifies the business owner of the degree of noncompliance.	
05.h	1	Updated: Examine policies and/or standards related to the independent review of information security and determine if an independent review of the organization's information security management program is initiated by management to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security and privacy. Independent security program reviews: i. include an assessment of the organizations adherence to its security plan and the tests and methods used are sufficient to validate the effectiveness of the security plan; ii. include notification requirements to confirm whom to inform within the organization about the timing and nature of the assessment; iii. address the need for changes to the approach to security in light of evolving circumstances, including the policy and control objectives and other opportunities for improvement, including those based on regular vulnerability assessments (e.g., network scans and penetration testing); iv. carefully control information security tests to limit the risks to confidentiality, integrity, and system availability; v. be carried out by individuals independent of the area under review (e.g., the internal audit function, an independent manager or a third-party organization specializing in such reviews); and vi. be carried out by individuals who have the appropriate skills and experience.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0177.05h1Organizational.12)
05.i	1	Updated: Examine policies and/or standards related to identification of risks related to external parties and determine the identification of risks related to external party access takes into account the following issues: i. the information asset(s) an external party is required to access; ii. the type of access the external party will have to the information and information asset(s), such as: 1. physical access (e.g. to offices, computer rooms, filing cabinets); 2. logical access (e.g. to an organization's databases, information systems); 3. network connectivity between the organization's and the external party's network(s) (e.g. permanent connection, remote access); 4. whether the access is taking place on-site or off-site; iii. the value and sensitivity of the information involved, and its criticality for business operations; iv. the controls necessary to protect information that is not intended to be accessible by external parties; v. the external party personnel involved in handling the organization's information; vi. how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1418.05i1Organizational.8)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		vii. the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information; viii. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information; ix. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident; x. legal and regulatory requirements and other contractual obligations relevant to the external party are taken into account; xi. how the interests of any other stakeholders may be affected by the arrangements.	
05.j	2	Updated: Examine policies and/or standards related to addressing security when dealing with customers to determine if certain the following security terms are addressed prior to giving customers access to any of the organization's assets: i. asset protection, including: 1. procedures to protect the organization's assets, including information and software, and management of known vulnerabilities; 2. procedures to determine whether any compromise of the assets (e.g. loss or modification of data) has occurred; 3. integrity; and 4. restrictions on copying and disclosing information; ii. access control policy, covering: 1. permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; 2. an authorization process for user access and privileges; 3. a statement that all access that is not explicitly authorized is forbidden; 4. a process for revoking access rights or interrupting the connection between systems; iii. arrangements for reporting, notification, and investigation of information inaccuracies (e.g. of personal details), information security incidents and security breaches; iv. a description of each service to be made available; v. the target level of service and unacceptable levels of service; vi. the different reasons, requirements, and benefits for customer access; vii. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g. data protection legislation), especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries (see 06.i); and viii. intellectual property rights (IPRs) and copyright assignment (see 06.b) and protection of any collaborative work (see 05.e). Access by customers to the organization's information is provided until the appropriate controls have been	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1421.05j2Organizational.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.	
05.j	FFIE	Updated: Examine policies and/or standards related to addressing security to determine if the organization implements a customer awareness and education program that addresses both retail (consumer) and commercial account holders that addresses the following elements: 1. An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online. 2. An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution never asks the customer to provide his or her log-in credentials over the phone or via e-mail. 3. A list of recommended controls and prudent practices that the customer implements when using the institutions remote financial services. 4. A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically 5. Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise. 6. A method to contact the institution if customers notice suspicious account activity.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1463.05jFFIECISOrganizational.2)
05.k	1	Updated: Examine policies and/or standards related to addressing security in third-party agreements and determine if ~~certain~~ the following terms are implemented for inclusion in the agreement in order to satisfy the identified security requirements (see 5.i): i. the information security policy; ii. controls to ensure asset protection, including: 1. procedures to protect organizational assets, including information, software and hardware; 2. any required physical protection controls and mechanisms; 3. controls to ensure protection against malicious software (see 9.j); 4. procedures to determine whether any compromise of the assets (e.g. loss or modification of information, software and hardware) has occurred; 5. controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement; 6. confidentiality, integrity, availability, and any other relevant property of the assets; and 7. restrictions on copying and disclosing information, and using confidentiality agreements (see 05.b); iii. user and administrator training in methods, procedures, and security;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1406.05k1Organizational.110)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		iv. ensuring user awareness for information security responsibilities and issues; v. provision for the transfer of personnel, where appropriate; vi. responsibilities regarding hardware and software installation and maintenance; vii. a clear reporting structure and agreed reporting formats; viii. a clear and specified process of change management; ix. access-control policy, covering: 1. the different reasons, requirements, and benefits that make the access by the third party necessary; 2. permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; 3. an authorization process for user access and privileges; 4. a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use; 5. a statement that all access that is not explicitly authorized is forbidden; and 6. a process for revoking access rights or interrupting the connection between systems; x. arrangements for reporting, notification (e.g., how when and to whom), and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement, stating: 1. the third party, following the discovery of a breach of unsecured covered information, notifies the organization of such breach, including the identification of each individual whose unsecured PII has been, or is reasonably believed by the third party to have been, accessed, acquired, or disclosed during such breach; 2. all notifications are made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a breach if the third party is an agent of the organization, otherwise the timing of the notification is explicitly addressed in the contract if the third party is not an agent of the organization; 3. evidence is maintained demonstrating that all notifications were made without unreasonable delay; and 4. any other information that may be needed in the notification to individuals, either at the time notice of the breach is provided or promptly thereafter as information becomes available. xi. a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see CSF 07.d); xii. the target level of service and unacceptable levels of service; xiii. the definition of verifiable performance criteria, their monitoring and reporting; xiv. the right to monitor, and revoke, any activity related to the organization's assets; xv. the right to audit responsibilities, defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors; xvi. the penalties exacted in the event of any failure in respect of the above; xvii. the establishment of an escalation process for problem resolution; xviii. service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities; xix. the respective liabilities of the parties to the agreement; xx. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g. data protection legislation) especially taking into account different national legal systems if the	

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		agreement involves co-operation with organizations in other countries (see 6.1); xxi. intellectual property rights (IPRs) and copyright assignment (see 6. b) and protection of any collaborative work (see 5.e); and xxii. conditions for renegotiation/termination of agreements: 1. a contingency plan is in place in case either party wishes to terminate the relation before the end of the agreements; 2. renegotiation of agreements if the security requirements of the organization change; and 3. current documentation of asset lists, licenses, agreements or rights relating to them. The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.	
05.k	CSP	Updated: Examine policies and/or standards related to identification or risks related to external parties to determine if supply chain agreements (e.g., SLAs) between cloud service providers and customers (tenants) incorporate ~~certain~~ at least the following mutually-agreed-upon provisions and/or terms: i. Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations): ii. Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships: iii. Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts: iv. Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain): v. Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed: vi. Expiration of the business relationship and treatment of customer (tenant) data impacted; and vii. Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1453.05kCSPOrganizational.2)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

05.k	GDPR	Updated: Examine policies and/or standards related to third-party assurance and determine if the data controller jointly determines the purposes and means of processing with one or more other controllers, that they determine their respective responsibilities for compliance with their obligations under GDPR in a transparent manner, in particular as regards the exercising of the rights of the data subject and their respective duties to provide information regarding access to personal data, whether obtained by the controller from the subject or from another source, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by EU or Member State law to which the controllers are subject. This arrangement duly reflects the respective roles and relationships of the joint controllers vis-à-vis the data subjects, and the essence of the arrangement is made available to the data subject. In addition, each data controller involved in the arrangement specifically allows a data subject to exercise the subjects rights under the GDPR in respect of and against each of the controllers. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1464.05kGDPROrganizational.1)
05.k	GDPR	Updated: Examine policies and/or standards related to third-party assurance and determine if processing by the ~~data~~ processor is governed by a written contract or other legal act (instrument) under Union or member state law, which may be one in electronic form, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The contract or other legal act (instrument) must also stipulate that the processor (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant by the EU GDPR for the security of processing personal data; (d) respects the conditions for obtaining consent from the controller and stipulating data protection requirements in a contract or other legal act when engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in the EU GDPR; (f) assists the controller in ensuring compliance with the obligations for the security of personal data, including the security of processing and data breach notification to the supervisory authority and data subject, data protection impact assessments and prior consultation with a supervisory authority, taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller,	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1466.05kGDPROrganizational.3)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; and (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the contract or other legal act (instrument) and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if, in the processors opinion, an instruction infringes the EU GDPR or other EU or Member State data protection provision. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	
05.k	GDPR	Updated: Examine policies and/or standards related to third-party assurance and determine if the data processor requires the same data protection obligations in a written contract or other legal act (instrument) under EU or member state law, which may be in electronic form, where it engages another processor for carrying out specific processing activities on behalf of the controller, and in particular provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the EU GDPR. As with the controller-to-processor, the processor-to-processor contract or legal act (instrument) also sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the each processor. The contract or other legal act (instrument) must also stipulate that the processor (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required pursuant by the EU GDPR for the security of processing personal data; (d) respects the conditions for obtaining consent from the controller and stipulating data protection requirements in a contract or other legal act when engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in the EU GDPR; (f) assists the controller in ensuring compliance with the obligations for the security of personal data, including the security of processing and data breach notification to the supervisory authority and data subject, data protection impact assessments and prior consultation with a supervisory authority, taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; and (h) makes available to the controller all	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1467.05kGDPROrganizational.4)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		information necessary to demonstrate compliance with the obligations laid down in the contract or other legal act (instrument) and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, and immediately inform the controller if, in the processors opinion, an instruction infringes the EU GDPR or other EU or Member State data protection provision. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	
06.a	2	Updated: The organization joins industry trade associations, subscribes to thought leadership and market/security research organizations, or establishes some other reliable process to stay abreast of business sector, industry, technology, infrastructure, and legal and regulatory environment trends that may impact the organization's security policies; and the consequences of these impacts are incorporated into the development or update of the organization's policies and procedures.	Requirement Statement updated to provide further clarity and alignment with the authoritative source(s). (0182.06a2Organizational.12)
06.a	2	Updated: Examine policies and/or standards related to the identification of applicable legislation to determine if the organization joins industry trade associations, subscribe to thought leadership and market/security research organizations, or establish some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal and regulatory environment trends that may impact the organization's security policies. Consequences of business sector, industry, technology, infrastructure, legal and regulatory environment trends impacting the organizations security policies are incorporated into the development or update of IT policies and procedures.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0182.06a2Organizational.12)
06.a	2	Updated: For the identification of applicable legislation, evidence policy/control requirements stipulated in the policy level have been implemented, e.g., examine relevant documentation, observe relevant processes, interview responsible parties. For example, examine evidence (e.g., meeting minutes, newsletters) to confirm that the organization has joined industry trade associations, subscribed to thought leadership and market/security research organizations. Confirm that any information gained on trends within the business sector, industry, technology, infrastructure, legal and regulatory environment trends are then incorporated into the organization's policies and procedures.	Illustrative Procedure Implemented updated to provide further clarity and alignment with the authoritative source(s). (0182.06a2Organizational.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

06.a	2	Updated: Examine measure(s) that evaluate(s) the organization's compliance with applicable legislation and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated in the policy level. For example, the measure(s) could indicate the number of industry trade associations, thought leadership and market/security research organizations the organization has joined, as a percent of such relevant organizations. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization joins industry trade associations, subscribes to thought leadership and market research organizations, or establishes some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal and regulatory environment trends that may impact the organization's security policies; and that the consequences of these impacts are incorporated into the development or update of the organization's policies and procedures.	Illustrative Procedure Measured updated to provide further clarity and alignment with the authoritative source(s). (0182.06a2Organizational.12)
06.b	1	Updated: Examine policies and/or standards related to the identification of applicable legislation to determine if the organization ensures compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks by: i. acquiring software only through known and reputable sources, to ensure that copyright is not violated; ii. maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.; iii. implementing controls to ensure that any maximum number of users permitted is not exceeded; iv. carrying out annual checks that only authorized software and licensed products are installed; v. developing and providing a policy for maintaining agreed upon license conditions; vi. using manual audit tools; vii. complying with terms and conditions for software and information obtained from public networks; and viii. use of proprietary software must also be in compliance with encryption, export and local data privacy regulations.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19135.06b1Organizational.1)
06.b	2	Updated: Examine policies and/or standards related to the identification of applicable legislation to determine if the organization ensures compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks by also: i. publishing an intellectual property rights compliance policy which defines the legal use of software and information products; ii. maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them; iii. maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19136.06b2Organizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		iv. developing and providing a policy for disposing or transferring software to others; v. not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and vi. not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.	
06.d	1	Updated: Examine policies and/or standards related to the protection and privacy of covered information to determine if there is an appointment of a person responsible, such as a data protection officer or privacy officer, who reports directly to the highest level of management in the organization (e.g., a CEO), and is responsible for the organization's individual privacy protection program, and such appointment is based professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks. Responsibilities include the development and implementation of privacy policies and procedures, serving as the point of contact for all privacy-related issues, including the receipt of privacy-related complaints, and providing privacy-related guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that are followed. The data protection officer will, in the performance of those tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing. The data protection officer may fulfill other tasks and duties; however, the organization ensures that any such tasks and duties do not result in a conflict of interests. The organization supports the data protection officer in performing the tasks required by law or regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the data protection officers expert knowledge. The organization ensures that the data protection or privacy officer does not receive any instructions regarding the exercise of those tasks, and the officer is bound by secrecy or confidentiality concerning the performance of the of those tasks, in accordance with applicable law or regulation. The officer is not to be dismissed or penalized by the organization for performing those tasks.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1901.06d1Organizational.1)
06.d	GDPR	Updated: Examine policies and/or standards related to data protection and privacy and determine if a data protection officer is designated for a (i) controller, (ii) processor, (iii) group of undertakings, provided the officer is accessible from each establishment, or (iv) group of multiple public authorities or bodies, taking account of their organizational structure and size, in any case where (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes,	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19258.06dGDPROrganizational.2)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		require regular and systematic monitoring of data subjects on a large scale; OR (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences. The controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law, also designates a data protection officer, who may act for such associations and other bodies representing controllers or processors. Also determine if the controller or the processor requires publication of the contact details and communication of those details to the supervisory authority. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	
06.h	CIS	Updated: Examine policies and/or standards related to technical compliance checking to determine whether the organization uses file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The file integrity checking tools reporting system: i. has the ability to account for routine and expected changes ii. highlights and alerts on unusual or unexpected changes; iii. shows the history of configuration changes over time and identifies who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks also identify suspicious system alterations such as: i. owner and permissions changes to files or directories; ii. the use of alternate data streams which could be used to hide malicious activities; iii. and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0661.06hCISOrganizational.6)
07.a	3	Updated: Examine policies and/or standards related to asset management to determine whether the organization creates, documents, and maintains a process and procedure to physically inventory and reconcile IT asset inventory information on hand for capital assets (Inventory must be conducted at least annually) and non-capital assets. The asset inventory includes: i. unique identifier and/or serial number; ii. information system of which the component is a part; iii. type of information system component (e.g., server, desktop, application); iv. manufacturer/model information; v. operating system type and version/service pack level;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0704.07a3Organizational.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		vi. presence of virtual machines; vii. application software version/license information; viii. physical location (e.g., building/room number); ix. logical location (e.g., IP address, position with the IS architecture); x. Media access control (MAC) address; xi. data ownership and custodian by position and role; xii. operational status; xiii. primary and secondary administrators; and xiv. primary user.	
08.a	FTI	Updated: Examine policies and/or standards related to perimeter security to determine if minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. i. secured perimeter ii. security room iii. badged employee iv. security container	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1839.08aFTIOrganizational.16789)
08.a	FTI	Updated: Examine policies and/or standards related to perimeter security to determine if all doors entering the space must be locked in accordance with Locking Systems for Secured Areas. The number of keys or persons with knowledge of the combination to a secured area will be kept to a minimum. Keys and combinations will be given only to those individuals who have a frequent need to access the area. Access control systems (e.g., badge readers, smart cards, biometrics) that provide the capability to audit access control attempts must maintain audit records with successful and failed access attempts to secure areas containing FTI or systems that process FTI. Agency personnel must review access control logs on a monthly basis. The access control log must contain the following elements: i. Owner of the access control device requesting access ii. Success/failure of the request iii. Date and time of the request	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1842.08aFTIOrganizational.3)
08.g	1	Updated: Examine policies and/or standards related to equipment siting and protection to determine if controls are implemented to minimize the risk of potential physical threats including theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1881.08g1Organizational.789)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		interference, electromagnetic radiation, and vandalism. The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The following controls are implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster: i. Hazardous or combustible materials are stored at a safe distance from a secure area; ii. bulk supplies such as stationery are not stored within a secure area; and iii. fallback equipment and back-up media are stored at a safe distance to avoid damage from disaster affecting the main site.	
08.j	1	Updated: Examine policies and/or standards related to the equipment maintenance to determine if the organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization: i. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; ii. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions; iii. Maintains records for nonlocal maintenance and diagnostic activities; and iv. Terminates all sessions and network connections when nonlocal maintenance is completed.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (18110.08j1Organizational.5)
08.j	CMS	Updated: Examine policies and/or standards related to the equipment maintenance to determine if the organization implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: i. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; ii. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (18113.08jCMSOrganizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

09.d	2	Updated: Examine policies and/or standards related to the separation of development, test, and operational environments, and determine if the level of separation between development, test, and operational environments is identified and controls are implemented to prevent operational issues~~.~~, including: i. along with removing accounts, a review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability, to include at least the following: 1. code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices; 2. code reviews ensure code is developed according to secure coding guidelines; 3. appropriate corrections are implemented prior to release; and 4. code-review results are reviewed and approved by management prior to release; ii. test data and accounts is removed completely before the application is placed into a production state. iii. organizations remove all custom application accounts, user IDs, and passwords before applications go from development to production or are released to customers iv. rules for the transfer of software from development to operational status are defined and documented; v. development and operational software run on different systems or computer processors and in different domains or directories; vi. compilers, editors, and other development tools or system utilities are not accessible from operational systems when not required; vii. the test system environment emulates the operational system environment as closely as possible; viii. users use different user profiles for operational and test systems, and menus display appropriate identification messages to reduce the risk of error; and ix. covered information is not copied into the test system environment.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0622.09d2System.1)
09.g	2	Updated: Examine policies and/or standards related to the monitoring and review of third-party services to determine if the change management on a third-party service includes an assessment and explicit recording of the potential impacts, including security impacts, of such change. Further, third-party changes are evaluated prior to implementation, including: i. evaluating and implementing changes made by the organization for: 1. enhancements to the current services offered; 2. development of any new applications and systems; 3. modifications or updates of the organization's policies and procedures; and 4. new controls to resolve information security incidents and to improve security; ii. evaluating and implementing changes in third-party services for: 1. changes and enhancement to networks;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1415.09g2System.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		2. use of new technologies; 3. adoption of new products or newer versions/releases; 4. new development tools and environments; 5. changes to physical location	
09.h	2	Updated: Examine policies and/or standards ~~related to the protection of denial-of-service attacks (DOS) and determine if the organization protects against or limit the effects of the types of denial of service attacks defined in NIST SP 800-63 R1, Computer Security Incident Handling Guide, and the following websites: (i) SANS Organization www.sans.org/dosstep; (ii) SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and, (iii) NIST CVE List National Vulnerability Database: http://nvd.nist.gov/home.cfm.~~ relating to network security, and determine if the organization protects against or limits the effects of the different types of denial of service attacks.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1614.09h2System.3)
09.j	1	Updated: Examine policies and/or standards related to the protection against malicious code and determine if formal policies are required and technologies implemented for the timely installation and upgrade of the protective measures, including the installation of anti-virus or anti-spyware software, also known as anti-malware, and for the regular updating of it, including virus definitions, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include: i. checking any files on electronic or optical media, and files received over networks, for malicious code before use; ii. checking electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; this check is carried out at different places (e.g., at electronic mail servers, desk top computers and when entering the network of the organization); iii. checking Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; and iv. checking removable media (e.g., USB tokens and hard drives, CDs/DVDs, FireWire devices, and external serial advanced technology attachment devices) when inserted. Bring your own device (BYOD) users are required to use anti-malware software (where supported).	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0201.09j1Organizational.124)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

09.m	1	Updated: Examine policies and/or standards related to network security and determine if network managers implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access. Controls are implemented to ensure the availability of network services (e.g., network connections) and information services using the network. (i) responsibilities and procedures for the management of networking equipment are established; (ii) operational responsibility for networks are separated from computer operations where appropriate; (iii) special controls are established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications; special controls may also be required to maintain the availability of the network services and computers connected.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0859.09m1Organizational.78)
09.m	2	Updated: Examine policies and/or standards related to network segregation and determine if ~~the organization's network is logically and physically segmented with a defined security perimeter and a graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network, based on organizational requirements; traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements.~~ networks are divided into separate logical network domains (e.g., an organization's internal network domains and external network domains) each protected by a defined security perimeter. Separate domains are implanted by controlling the network data flows using routing/switching capabilities, including access control lists, according to applicable flow control policies. The domains are defined based on a risk assessment and the different security requirements within each of the domains. A graduated set of controls is applied in different logical network domains to further segregate the network security environments (e.g., publicly accessible systems, internal networks; critical assets; and key information security tools, mechanisms, and support components associated with system and security administration). The organization implements subnetworks for publicly accessible system components that are logically separated from internal organizational networks. To ensure proper separation, the organization verifies any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, moves it to an internal VLAN and gives it a private address. The criteria for segregation of networks into domains is based on the access control policy and access requirements, and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. In addition, segregation of networks is based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0806.01m2Organizational.12356)
09.n	2	Updated: Examine policies and/or standards related to the management of network services and determine if the	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		organization authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreements that: i. require providers to comply with organizational information security requirements; ii. employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance; iii. define and document organizational oversight and user roles and responsibilities with regard to external information system services; iv. provide for organizational monitoring of security control compliance by external service providers; v. require the use of FIPS-validated cryptographic mechanisms during transmission to protect the confidentiality and integrity of information unless otherwise protected by alternative physical measures; and vi. state the provider is responsible for the protection of covered information.	source(s). (0837.09n2Organizational.2)
09.0	CMS	Updated: Examine policies and/or standards related to the security of magnetic media and determine if the organization evaluates employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance and ,if PII is recorded on magnetic media with other data, it is protected as if it were entirely personally identifiable information.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19177.09oCMSOrganizational.4)
09.q	3	Updated: Examine policies and/or standards related to information handling to determine if inventory and disposition records for information system media is maintained to ensure control and accountability of the organization's information. Further, ensure that inventory and disposition of media-related records contain sufficient information to reconstruct the data in the event of a breach. The media records, at a minimum, will contain: (i) the name of media recipient; (ii) the signature of media recipient; (iii) the date/time media received; (iv) the media control number and contents; (v) the movement or routing information; and (vi) if disposed of, the date, time, and method of destruction.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0308.09q3Organizational.1}
09.r	1	Updated: Examine policies and/or standards related to the security of system documentation and determine if the organization obtains administrator ~~and user documentation for the information system, system component, or information system service. Organizations document attempts to obtain information system documentation when such documentation is either unavailable or non-existent.~~ documentation for the	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0730.09r1Organizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		information system, system component, or information system service that describes: (i) secure configuration, installation, and operation of the system, component, or service; (ii) effective use and maintenance of security functions/mechanisms; and (iii) known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. Obtains user documentation for the information system, system component, or information system service that describes: (i) user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (ii) methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (iii) user responsibilities in maintaining the security of the system, component, or service. Organizations document attempts to obtain information system documentation when such documentation is either unavailable or non-existent.	
09.s	1	Updated: Examine policies and/or standards related to information exchange to determine if, when using electronic communication applications or systems for information exchange, ~~certain criteria are addressed.~~ the following items are addressed: (i) requirements (e.g., policies, standards) or guidelines are defined outlining acceptable use of electronic communication applications or systems; (ii) the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications; (iii) procedures are implemented for the use of wireless communications including an appropriate level of encryption (see 09.m); (iv) employee, contractor and any other user's responsibilities are defined to not compromise the organization (e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.); (v) the required use of cryptographic techniques to protect the confidentiality, integrity and authenticity of covered information; (vi) the retention and disposal guidelines are defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and (vii) controls and restrictions are implemented associated with the forwarding of communications (e.g. automatic forwarding of electronic mail to external mail addresses).	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0901.09s1Organizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

09.s	1	Updated: Examine policies and/or standards related to information exchange to determine if personnel are appropriately educated and periodically reminded of ~~certain criteria.~~ the following: a. not discussing or leaving critical information on printing systems (e.g., copiers, printers, and facsimile machines) as these may be accessed by unauthorized personnel; b. taking the necessary precautions, including not to reveal covered information, to avoid being overheard or intercepted when making a phone call by: 1. people in their immediate vicinity, particularly when using mobile phones; 2. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; or 3. people at the recipient's end; c. not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing; and d. addressing the problems with printers, facsimile and copy machines, such as: 1. unauthorized access to built-in message stores to retrieve messages; 2. deliberate or accidental programming of machines to send messages to specific numbers; and 3. sending documents and messages to the wrong number either by misdialing or using the wrong stored number; 4. registering demographic data, e.g., email address or other personal information, in any software to avoid collection for unauthorized use; and 5. page caches and store page functionality that modern facsimile machines and photocopiers have in case of a paper or transmission fault, which will be printed once the fault is cleared.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1325.09s1Organizational.3)
09.s	GDPR	Updated: Examine policies and/or standards related to transmission protection and determine if the organization maintains records of the basis used to authorize cross-border flows of personal data to a third-country or international organization which include but are not limited to (a) an adequacy decision by the EU Commission; (b) the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available; (c) binding corporate rules approved by the relevant supervisory authority; (d) A court judgement or administrative decision of a third country if based on an international agreement between the third country and the EU; OR (e) If one of the following conditions are met, (i) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards, (ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person, (iv) the transfer is necessary for important reasons of public interest, (v) the transfer is necessary for the establishment, exercise or defense of legal claims, (vi) the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent, (vii) the transfer is made from a register which according to EU or Member State	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0965.09sGDPROrganizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in EU or Member State law for consultation are fulfilled in the particular case. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	
09.s	GDPR	Updated: Examine policies and/or standards related to transmission protection and determine if appropriate safeguards for cross-border flows of personal data ~~are included~~ include (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules; (c) standard data protection clauses adopted by the Commission; (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission; (e) an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. IF AUTHORIZED by the relevant supervisory authority, appropriate safeguards may also include (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organization; OR (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0966.09sGDPROrganizational.2)
09.t	1	Updated: Examine policies and/or standards related to exchange agreements and determine if exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards and solutions. The exchange and data sharing agreements also specify organization policies including: i. classification policy for the sensitivity of the business information; ii. management responsibilities for controlling and notifying transmission, dispatch, and receipt; iii. procedures for notifying sender of transmission, dispatch, and receipt; iv. procedures to ensure traceability and non-repudiation; v. minimum technical standards for packaging and transmission; vi. courier identification standards; vii. responsibilities and liabilities in the event of information security incidents, such as loss of data; viii. use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ix. ownership and responsibilities for data protection, copyright, software license compliance and similar	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1444.09t1Organizational.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		considerations; x. technical standards for recording and reading information and software; xi. any special controls that may be required to protect covered items, including cryptographic keys; and xii. escrow agreements.	
09.w	1	Updated: Examine policies and/or standards related to interconnecting business information systems and determine if security and business implications are addressed for interconnecting business information assets including: i. policy and appropriate controls to manage information sharing; ii. excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection; iii. categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed; iv. restricting selected systems and facilities to specific categories of user; and v. identifying the status of users (e.g. employees of the organization or contractors in directories for the benefit of other users).	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0933.09w1Organizational.1)
09.x	1	Updated: Examine policies and/or standards related to electronic commerce and determine if the confidentiality and integrity for electronic commerce is maintained by ensuring the following: i. the level of confidence each party requires in each other's claimed identity (e.g. through authentication); ii. authorization processes associated with who may set prices, issue or sign key trading documents; iii. ensuring that trading partners are fully informed of their authorizations; iv. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts (e.g. associated with tendering and contract processes); v. the level of trust required in the integrity of advertised price lists; vi. the confidentiality of any covered data or information; vii. the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts; viii. the degree of verification appropriate to check payment information supplied by a customer; ix. selecting the most appropriate settlement form of payment to guard against fraud; x. the level of protection required to maintain the confidentiality and integrity of order information; xi. avoidance of loss or duplication of transaction information; xii. liability associated with any fraudulent transactions; and xiii. insurance requirements.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0938.09x1Organizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

10.a	CMS	Updated: Examine policies and/or standards related to system and information integrity policy to determine if the organization manages the information system using ~~a formally defined and documented system development lifecycle process that incorporates information security control considerations.~~ the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS eXpedited Life Cycle (XLC) that incorporates information security control considerations	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (17102.10aCMSOrganizational.1)
10.a	CMS	Updated: Examine policies and/or standards related to system and information integrity policy to determine if the organization requires the developer of the information system, system component, or information system service to follow a documented development process that: i. Explicitly addresses security requirements; 1. Identifies the standards and tools used in the development process; 2. Documents the specific tool options and tool configurations used in the development process; and 3. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development. ii. Identifies the standards and tools used in the development process; iii. Documents the specific tool options and tool configurations used in the development process; and iv. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (17104.10aCMSOrganizational.3)
10.b	1	Updated: Examine policies and/or standards related to input validation in applications to determine if the organization developed applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including but not limited to: i. injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); ii. buffer overflow (Validate buffer boundaries and truncate input strings) iii. insecure cryptographic storage (Prevent cryptographic flaws) iv. insecure communications (Properly encrypt all authenticated and sensitive communications); v. improper error handling (Do not leak information via error messages); vi. broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user); vii. cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.);	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0706.10b1System.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		viii. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); ix. cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and x. any other input-validation vulnerability listed in the OWASP top 10. Applications that are not developed using secure coding guidelines undergo automatic or manual input validation checks during testing and annually thereafter, and such checks include: i. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors: 1. out-of-range values 2. invalid characters in data fields 3. missing or incomplete data 4. exceeding upper and lower data volume limits 5. unauthorized or inconsistent control data ii. periodic review of the content of key fields or data files to confirm their validity and integrity; iii. procedures for responding to validation errors; iv. procedures for testing the plausibility of the input data; v. verifying the identity of an individual opening or updating an account; vi. defining the responsibilities of all personnel involved in the data input process; and vii. creating a log of the activities involved in the data input process (see 9.aa)	
09.aa	FTI	Updated: Examine policies and/or standards related to audit logging and determine if the organization provides an audit record generation capability and audits ~~events.~~ the following events, at a minimum: i. Log onto system; ii. Log off of system; iii. Change of password; iv. All system administrator commands, while logged on as system administrator; v. Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS); vi. Creation or modification of super-user groups; vii. Subset of security administrator commands, while logged on in the security viii. administrator role; ix. Subset of system administrator commands, while logged on in the user role; x. Clearing of the audit log file;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1250.09aaFTISystem.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		xi. Startup and shutdown of audit functions; xii. Use of identification and authentication mechanisms (e.g., user ID and password); xiii. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su); xiv. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system; xv. Changes made to an application or database by a batch file; xvi. Application-critical record changes; xvii. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility); xxiii. All system and data interactions concerning FTI; and xxiv. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards Website. The organization audits records for the following events in addition to those specified in other controls: i. all successful and unsuccessful authorization attempts; ii. all changes to logical access control authorities (e.g., rights, permissions); iii. all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services; iv. the audit trail captures the enabling or disabling of audit report generation services; and v. the audit trail captures command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).	
09.ac	CMS	Updated: Examine policies and/or standards related to the protection of log information and determine if the information system provides a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity. The information system provides an alert in real time to defined personnel, roles, and/or locations (defined in the applicable security plan) when the following audit failure events occur: - Record log is full; - Authentication logging failure; and - Encryption logging failure.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1264.09acCMSSystem.12)
10.g	2	Updated: Examine policies and/or standards related to encryption key management to determine if the organization has a formal key management system (KMS), which is consistent with federal or industry-recognized guidelines and best practices, including: i. verifying user identity prior to generating new certificates or keys;	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0906.10g2Organizational.13)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		ii. generating keys for different cryptographic systems and different applications; iii. generating and obtaining public key certificates; iv. distributing keys to intended users, including how keys are activated when received; v. storing keys in the fewest possible locations, including how authorized users obtain access to keys; vi. changing or updating keys including rules on when keys are changed and how this will be done: 1. as deemed necessary and recommended by the associated application; and 2. at least annually; vii. revoking keys including how keys are withdrawn or deactivated (e.g. when keys have been compromised or suspected to have been compromised or when a user leaves an organization, in which case keys are also archived); viii. recovering keys that are lost or corrupted as part of business continuity management (e.g. for recovery of encrypted information); ix. archiving keys (e.g. for information archived or backed up); x. destroying keys; and xi. logging and auditing of key management related activities. The organization securely manages secret and private keys, including the authenticity of public keys using public key certificates issued by a trusted Certification Authority (CA) that is a recognized organization with suitable controls and procedures in place to provide the required degree of trust.	
10.j	2	Updated: Examine policies and/or standards related to the protection of program source code to determine if program source code is stored in a central location, specifically in program source libraries. The following requirements are implemented (see 1.0) to control access to such program source libraries in order to reduce the potential for corruption of computer programs: i. program source libraries are not held in operational systems; ii. the program source code and the program source libraries are managed according to established procedures; iii. access to program source libraries is strictly limited to that which is needed to perform a job function; iv. the updating of program source libraries and associated items, and the issuing of program sources to programmers is only performed after appropriate authorization has been received; v. program listings are held in a secure environment (see 9.r); vi. an audit log is maintained of all accesses to program source libraries; and vii. maintenance and copying of program source libraries is subject to strict change control procedures (see 10.k).	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0634.10j2System.12)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

10.k	2	Updated: Examine policies and/or standards related to change management to determine if the organization develops, documents, and implements a configuration management plan for the information system that: i. addresses roles, responsibilities, and configuration management processes and procedures; ii. defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; iii. establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; and iv. protects the configuration management plan from unauthorized disclosure and modification.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0637.10k2Organizational.2
10.k	2	Updated: Examine policies and/or standards related to change management to determine if changes are formally controlled, documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems are formally documented, specified, tested, quality controlled, and the implementation managed. The organization ensures change control includes a risk assessment, analysis of the security and privacy impacts of changes, and specification of security controls needed. The organization ensures changes do not compromise existing security requirements/controls that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Change control minimally includes: i. ensuring changes are submitted by authorized users; ii. maintaining a record of agreed authorization levels; iii. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; iv. identifying all software, information, database entities, and hardware that require amendment; v. obtaining formal approval for detailed proposals requesting changes before work commences; vi. documenting unit, system, and user acceptance testing procedures in an environment segregated from development and production; vii. ensuring all system components are tested and approved (operating system, utility, applications) prior to promotion to production; viii. documenting rollback procedures for failed changes; ix. ensuring authorized users accept changes prior to implementation based on the results on the completion of each change of testing the changes; x. ensuring that the system documentation set is updated and that old documentation is archived or disposed of; xi. maintaining a version control for all software updates; xii. maintaining an audit trail of all change requests and approvals; xiii. testing for mobile device, operating system, and application compatibility issues via a documented	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0638.10k2Organizational.34569)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		application validation process; and xiv. ensuring that operating documentation (see 9.a) and user procedures are changed as necessary to remain appropriate. If a change that is not listed on the organizations approved baseline is discovered, an alert is generated and reviewed by the organization.	
10.k	CMS	Updated: ~~Examine policies and/or standards related to change control procedures to determine if –for the following OS and applications: HHS approved USGCB Windows Standards (e.g., Microsoft supported versions only), Blackberry Server-Websense, and for all other operating systems and applications–to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is used.~~ Examine policies and/or standards related to change management to determine if HHS-specific minimum security configurations are used for the following Operating System (OS) and Applications: HHS FDCC Windows XP Standard, HHS FDCC Windows Vista Standard, Blackberry Server, Websense. For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines as follows: (1) USGCB (2) NIST National Checklist Program (NCP); Tier IV, then Tier III, Tier II, and Tier I, in descending order. (3) Defense Information Systems Agency (DISA) STIGs (4) National Security Agency (NSA) STIGs (5) If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists. (6) In situations where no guidance exists, coordinate with CMS for guidance. CMS collaborates within CMS and the HHS Cybersecurity Program, and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor best practices. (7) All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented in an approved HHS waiver (available at http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy%20and%20Standard%20Waiver), with copies submitted to the Department.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (0645.10kCMSOrganizational.12)
11.a	Texas	Updated: Examine policies and/or standards related to the disclosure of breaches to determine if breach disclosures are made as quickly as possible, except at the request of a law enforcement agency that determines notification will impede a criminal investigation, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. THSC § 195.002 (b) allows the state registrar or the state registrar's	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1527.11aTexasOrganizational.2)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		representative may investigate cases of irregularity or violations of law. On request, any other registrar shall aid in the investigation. THSC § 195.003: False Records: 1) A person commits an offense if the person intentionally or knowingly makes a false statement or directs another person to make a false statement in: a) a certificate, record, or report required under this title; b) an application for an amendment of a certificate, record, or report required under this title; c) an application for a delayed birth certificate or delayed death certificate; or d) an application for a certified copy of a vital record. 2) A person commits an offense if the person intentionally or knowingly supplies false information, or intentionally or knowingly creates a false record, or directs another person to supply false information or create a false record, for use in the preparation of a certificate, record, report, or amendment under this title. 3) A person commits an offense if the person, without lawful authority and with intent to deceive, makes, counterfeits, alters, amends, or mutilates, or directs another person to make, counterfeit, alter, amend, or mutilate: a) a certificate, record, or report required under this title; or b) a certified copy of a certificate, record, or report required under this title. 4) A person commits an offense if the person, for purposes of deception, intentionally or knowingly obtains, possesses, uses, sells, or furnishes, or attempts or directs another person to attempt to obtain, possess, use, sell, or furnish a certificate, record, or report required under this title, or a certified copy of a certificate, record, or report required under this title, if the document: a) is made, counterfeited, altered, amended, or mutilated without lawful authority and with intent to deceive; b) is false in whole or in part; or c) relates to the birth of another individual. 5) A person commits an offense if the person intentionally or knowingly fraudulently identifies himself or herself to obtain or return registration forms, certificates, or any other forms required under this title. 6) An offense under this section is a felony of the third degree. 7) In this section, "person" means an individual, corporation, or association. 8) If a person is convicted of an offense under this section, the court shall order as a condition of probation that the person cannot obtain a certificate, record, or report to which this section applies or practice midwifery, and the Texas Department of Criminal Justice shall require as a condition of parole that the person cannot obtain a certificate, record, or report to which this section applies or practice midwifery. THSC § 195.004: Failure to Perform Duty. 1) A person commits an offense if the person refuses or fails to furnish correctly any information in the person's possession affecting a certificate or record required under this title. 2) A person commits an offense if the person fails, neglects, or refuses to fill out a birth or death certificate and file the certificate with the local registrar or deliver it on request to the person with the duty to file it, as	

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		required by this title. 3) A local registrar, deputy registrar, or sub registrar commits an offense if that person fails, neglects, or refuses to perform a duty under this title or under instructions and directions of the state registrar given under this title. 4) Except as provided by Subsection (d-1), an offense under this section is a Class C misdemeanor. 5) (d-1) An offense under this section for failure to perform a duty required by Section 192.003 is a Class A misdemeanor. 6) In this section, "person" means an individual, corporation, or association. THSC § 195.005: Disclosure of Confidential Information 1) A person commits an offense if the person knowingly violates Section 192.002(b), knowingly induces or causes another to violate that section, or knowingly fails to comply with a rule adopted under that section. 2) An offense under this section is a Class A misdemeanor.	
11.a	FTI	Updated: Examine policies and/or standards related to the reporting of information security events to determine if any data incident potentially involving FTI must immediately be reported to the appropriate Treasury Inspector General for the Tax Administration (TIGTA) field office and the IRS Office of Safeguards immediately, but no later than ~~24~~ twenty-four (24) hours after identification of a possible issue involving FTI. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time in a data incident report, as follows: i. Name of agency and agency Point of Contact for resolving data incident with contact information; ii. Date and time of the incident; iii. Date and time the incident was discovered; iv. How the incident was discovered; v. Description of the incident and the data involved, including specific data elements, if known; vi. Potential number of FTI records involved; if unknown, provide a range if possible; vii. Address where the incident occurred; viii. IT involved (e.g., laptop, server, mainframe); ix. Do not include any FTI in the data Incident report; and x. Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1532.11aFTIOrganizational.12)
11.a	GDPR	Updated: Examine policies and/or standards related to incident management and determine if, in the case of a personal data breach, the ~~data~~ controller notifies the appropriate supervisory authority without undue delay	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s).

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and liberties (freedoms) of natural persons, such notification is provided all at once or, if in phases, without further undue delay; and such notification at least (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; and (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Where the notification to the supervisory authority is not made within 72 hours, it is accompanied by reasons for the delay. Note: In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration is given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	(1589.11aGDPROrganizational.1)
11.c	2	Updated: Examine policies and/or standards related to the reporting and management of information security events to determine if, following an incident, audit trails and evidence are collected and secured, as appropriate for: (i) internal problem analysis; (ii) 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, (iii) negotiating for compensation from software and service suppliers. Action to recover from security breaches and correct system failures are carefully and formally controlled. The procedures ensure that: i. only clearly identified and authorized personnel are allowed access to live systems and data; ii. all emergency actions taken are documented in detail; iii. damage is minimized through the containment of the incident, restoration of systems, and preservation of data and evidence; iv. emergency action is reported to management and reviewed in an orderly manner; v. the integrity of business systems and controls is confirmed with minimal delay; and vi. stakeholders are notified immediately when a safe and secure environment has been restored.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1518.11c2Organizational.13)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

12.a	2	Updated: Examine policies and/or standards related to the business continuity management process to determine if the organization brings together the following key information security elements of business continuity management: i. identifying critical information system assets supporting organizational missions and functions; ii. understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes; iii. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information assets; iv. implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible; v. identifying financial, organizational, technical, and environmental resources to address the identified information security requirements; vi. testing and updating, at a minimum, a section of the plans and processes put in place at least annually; vii. ensuring that the management of business continuity is incorporated in the organization's processes and structure; and viii. assigning responsibility for the business continuity management process at an appropriate level within the organization.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1633.12a2Organizational.1)
12.c	1	Updated: Examine policies and/or standards related to business continuity to determine if the business continuity planning process includes the following: i. recovery and restoration of business operations and establish an availability of information in a time-frame specified by the organization; ii. particular attention is given to the assessment of internal and external business dependencies and the contracts in place; iii. documentation of agreed procedures and processes; and iv. testing and updating of at least a section of the plans. The planning process focuses on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered information during an emergency is defined. The services and resources facilitating this is identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. Following an interruption to business operations,	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1601.12c1Organizational.1238)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		full information system restoration without deterioration of the security measures originally planned and implemented can be achieved.	
12.c	CMS	Updated: Examine policies and/or standards related to business continuity to determine if the organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. (see 12.e, Level 2). The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (1656.12cCMSOrganizational.810)
13.a	Texas	Updated: Examine the policies and/or standards related to patient rights at a nursing or other facility in which the patient is resident including the organization's formal statement of patient rights and determine if they ensure the rights of the patient, within the limits of federal and state law, to personal privacy and confidentiality of personal information and clinical records. Personal privacy includes accommodations, medical treatment, written and telephone communications, personal care, visits, and meetings of family and resident groups, but this does not require the facility to provide a private room for each resident. 40 TAC §19.407 goes on to state: 1) The facility must ensure the resident's right to privacy in the following areas: a) accommodations as described in §19.1701 of this title (relating to General Requirements); b) medical treatment. The facility must provide privacy to each resident during examinations, treatment, case discussions, and consultations. Staff must treat these matters confidentially; c) personal care; d) access and visitation as described in §19.413 of this title (relating to Access and Visitation Rights); e) governmental searches are permitted only if there exists probable cause to believe an illegal substance or activity is being concealed. Administrative searches by the appropriate entity, such as the fire inspector, are allowed only for limited purposes, but such searches would not ordinarily extend to the resident's personal belongings. The Texas Department of Aging and Disability Services (DADS) and the nursing facility must provide for and allow residents their individual freedoms. State statutes authorize inspections of the nursing facility but do not authorize inspection of those areas in which an individual has a reasonable expectation of privacy. Any direct participation by DADS personnel in an inspection of "the contents of residents' personal drawers and possessions," is in violation of federal and state law; and f) the resident has the right to privacy for meetings with family and resident groups. 2) All information that contains personal identification or descriptions which would uniquely identify an individual resident or a provider of health care is considered to be personal and private and will be kept confidential. Personal identifying information (except for PCN numbers) will be deleted from all records, reports, and/or minutes from formal studies which are forwarded to DADS, or anyone else. These records, reports, and/or minutes, which have been de-identified, will still be treated as confidential. All such material	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19304.13aTexasOrganizational.2)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		mailed to DADS or anyone else must be in a sealed envelope marked "Confidential."	
13.e	GDPR	Updated: Examine policies and/or standards related to choice and determine if a data subject may obtain a restriction from a ~~data~~ controller where one of the following applies: (i) the accuracy of the PII is contested by the data subject, for a period enabling the controller to verify the accuracy of the PII; (ii) the processing is unlawful and the data subject opposes the erasure of the PII and requests the restriction of their use instead; (iii) the controller no longer needs the PII for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims; or, (iv) the data subject has objected to processing necessary for the performance of a task carried out in the public interest, in the exercise of official authority vested in the controller, or for the legitimate interests pursued by the controller or by a ~~third-party~~ third party pending the verification whether the legitimate grounds of the controller override those of the data subject. The data controller ensures that, when processing has been restricted, that further processing other than for storage will only be performed with the data subjects consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State; and informs the data subject prior to lifting such a restriction. (The assessor is strongly encouraged to examine the GDPR Articles in detail and refer to the Recitals supporting the Articles prior to assessing the organization's compliance at any level for this requirement statement.)	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19362.13eGDPROrganizational.2)
13.f	EHNAC	Updated: ~~Examine policies and/or standards related to access to individual information and ensure they identify the following levels at which PHI is handled within the organization: (i) Level 1: PHI is never directly accessed by any workforce member; (ii) Level 2: PHI is sometimes accessible to workforce members; and, (iii) Level 3: PHI is created when workforce members communicate directly with members or patients. Creation of PHI means a designated record check is created.~~ Examine policies and/or standards related to access to individual information and ensure they identify the following levels at which PHI is handled within the organization: Level 1: PHI is NEVER directly accessed by any workforce member. Level 2: PHI is sometimes accessible to workforce members. Level 3: PHI is created when workforce members communicate directly with members or patients. Creation of PHI means a designated record check is created. Then ensure the policies and/or standards require access to personal information based on the	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19562.13fEHNACOrganizational.1)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		aforementioned levels, as follows: Level 1: None Level 2: 1. Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. 2. Review the HIPAA Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. 3. Provide a general statement as to the determination if it is deemed that NO Uses or Disclosures or Individual Rights are deemed applicable. Level 3: 1. Review the HIPAA Privacy Rule Uses and Disclosures regulations and document which requirements apply to your business model and the way in which ePHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. 2. Review the Privacy Rule Individual Rights regulations and document which requirements apply to your business model and the way in which PHI is handled. Provide evidence of this review along with policy and procedure documents in the respective sections within this self-assessment. 3. Provide a general statement as to the determination if it is deemed that CERTAIN Uses or Disclosures or Individual Rights are deemed applicable.	
13.k	HIPAA	Updated: Examine policies and/or standards related to use and disclosure and ensure that uses and disclosures of PII for research is only allowed if approved by a valid institutional review board (IRB) or privacy board and the entity receives appropriate representation from the researcher regarding the appropriate uses and disclosures necessary for research purposes. Based on the complexity of the entity, policy elements to consider include, but are not limited to, whether the entity obtains documentation that an alteration to a required authorization, or waiver of the authorization, has been approved by an IRB or privacy board and/or obtains from the researchers the required representations regarding reviews preparatory to research on decedents. Documentation of an approved alteration or waiver for a permitted use or disclosure for research must contain a signed, dated statement from the IRB or privacy board that confirms the necessary conditions for use or disclosure, as required by applicable law, regulation, policy, contract or similar obligation. Based on the complexity of the entity, policy elements to consider include, but are not limited to, whether the documentation includes identification and date of action, includes waiver criteria, and includes the PII needed, requires review and approval procedures, and requires signature.(The assessor is strongly encouraged to examine relevant legal, regulatory, policy, contractual and other applicable requirements in detail prior to assessing the organization's compliance at any level for this requirement statement.)	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19436.13kHIPAAOrganizational.8)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

13.k	Texas	Updated: Examine policies and/or standards related to the confidentiality and disclosure of sensitive information to ensure that government benefits / federal assistance information (records) is confidential and may not be disclosed except as provided by relevant legislation and regulations. For example, 42 CFR § 431.300 states that (i) a State plan must provide safeguards that restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan. The CFR also states that information exchanged by State agencies is made available only to the extent necessary to assist in the valid administrative needs of the program receiving the information, and information received under section 6103(l) of the Internal Revenue Code of 1954 is exchanged only with agencies authorized to receive that information under that section of the Code; and, (ii) The information is adequately stored and processed so that it is protected against unauthorized disclosure for other purposes. Assessors must determine if the assessed entity receives any information related to government benefits / federal assistance, such as those relating to 7 CFR § 272 (SNAP), 45 CFR § 205.50 (TANF) and 42 CFR § 431.300 (Medicaid), identify the programs and the confidentiality and disclosure requirements specific to those programs, and include the criteria in the assessment of the entity's compliance.	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (19481.13kTexasOrganizational.24)
13.k	EHNAC	Updated: Examine policies and/or standards related to permitted uses and disclosures of PHI and ensure they address the implementation specifications listed in the HIPAA Privacy Rule. If a covered entity, ensure the policies and/or standards address the handling of the following requirements: 1. Minimum Necessary (required) 2. Use & Disclosure Policies (required to the degree the candidate handles PHI in support of such as determined in control reference 13.f): a. Extension of Privacy Protection to Deceased Individuals b. Authorization to Use or Disclose PHI c. De-Identified Information d. Limited Data Set e. Use and Disclosure of PHI for Purposes of Research f. Use or Disclosure of Psychotherapy Notes g. Use and Disclosure of PHI for Marketing Purposes h. Use and Disclosure of PHI for Fundraising i. Use and Disclosure of Genetic Information for Underwriting Purposes j. Uses and Disclosures for Facility Records 3. Disclosure of PHI Policies (required to the degree the candidate handles PHI in support of such as determined in control reference 13.f): a. Verification of the Identity and Authority of a Person Requesting Disclosure of PHI	Illustrative Procedure Policy updated to provide further clarity and alignment with the authoritative source(s). (195634.13kEHNACOrganizational.2)

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.

		b. Providing Medical Information to Family, Friends, Or Others Directly Involved in the Patients Care c. Disclosures of PHI Required by Law d. Disclosures of PHI for Public Health Purposes e. Disclosures of PHI to Report Child Abuse, or Other Abuse, Neglect, or Domestic Violence f. Reporting PHI to Employers under OSHA and Other Similar Laws g. Disclosures of PHI to Regulators h. Subpoenas, Court Orders, Discovery Requests, and other Legal Processes and the Disclosure of PHI i. Disclosures of PHI for Law Enforcement Purposes j. Disclosures of PHI in Disaster Situations k. Disclosures of PHI without Authorization to Avert a Serious Threat to Health or Safety l. Disclosures of PHI for Certain Government Functions m. Disclosure of PHI Pertaining to Inmates n. Disclosure of PHI to Workers Compensation Programs Business Associates handling PHI on behalf of one or more Covered Entities must address each of the foregoing elements, as required, based on completion of the PHI Level information described in the EHNAC Industry Segment for CSF Control 13.f.	

© 2020 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronical or mechanical, without HITRUST's prior written permission.