HITRUST CSF v11.9 e1 and i1 Baseline Change FAQ

Changes to the e1 and i1 baselines in v11.9

With the release of v11.9.0, HITRUST is making several updates to the CSF library. These updates are intended to improve clarity and address emerging technologies and risks.

What baselines are changing?

The e1 baseline has nine requirement-statement changes and one requirement addition. The i1 baseline has 24 requirement-statement changes.

Modifications to requirements in the current e1 baseline

0226.09k1Organizational.2

Current [0896.0]: The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.

Updated [0896.0]: The organization implements and regularly updates mobile code protection, including anti-malware.

Change: Specific references to anti-virus and anti-spyware were replaced with the broader term anti-malware.

10.01d1System.10

Current [2361.0]: Password policies applicable to the organization’s information systems are documented and enforced through technical controls.

Updated [2361.0]: Policies governing the authentication mechanisms used by the organization’s information systems (e.g., passwords or passwordless mechanisms such as passkeys) are documented and enforced through technical controls.

Change: Password policy requirements were broadened to clarify coverage of all authentication mechanisms, including passwordless methods.

0903.10f1Organizational.1

Current [1289.0]: Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).

Updated [1289.0]: Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required, including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).

Change: This requirement was added to the e1 baseline to increase the depth of coverage against relevant cyber threats. The requirement was also expanded to require documented consideration of cryptographic algorithm lifecycle status and the need to consider quantum-resistant cryptographic mechanisms.

19180.09z1Organizational.2

Current [1103.1]: The organization trains individuals to ensure that publicly posted information does not contain nonpublic information. If the organization permits the posting of information onto a publicly accessible information system, it designates individuals authorized to post the information.

Updated [1103.1]: The organization trains individuals to ensure that publicly posted information does not contain nonpublic information. If the organization permits the posting of nonpublic information onto a publicly accessible information system (e.g., online forum, social media platform, public repository, or AI service where the organization cannot control downstream access, use, retention, or disclosure), it designates individuals authorized to post the information.

Change: The requirement was updated to provide examples of publicly accessible information systems.

0701.07a1Organizational.7

Current [0626.1]: The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; and approved bring your own device (BYOD) equipment.

Updated [0626.3]: The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; approved bring your own device (BYOD) equipment; and cryptographic asset inventory components (e.g., algorithms, protocols, certificates, keys, and cryptographic libraries).

Change: Documentation of cryptographic assets, such as algorithms, protocols, certificates, keys, and libraries, were added to the required asset inventory.

06.09b1System.2

Current [2368.0]: Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.

Updated [2368.1]: Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, risk-assessed, security-tested, and approved.

Change: Change-management requirements were clarified to specifically require risk assessment and security testing, in addition to documentation and approval.

07.10m1Organizational.2

Current [2317.1]: The organization deploys automated software update tools in order to ensure that systems are running the most recent security updates provided by the software vendor, and installs software updates manually for systems that do not support automated software updates.

Updated [2317.2]: The organization deploys automated software update tools to apply vendor security updates, installs software updates manually for systems that do not support automated software updates, and installs vendor security updates within formally documented, risk-tiered remediation timeframes.

Change: The revision updates the requirement to focus on applying vendor security updates within timeframes based on risk, rather than only requiring the most recent updates through automated tools.

07.10m1Organizational.3

Current [2367.0]: Information systems are periodically scanned to proactively (annually at minimum) identify technical vulnerabilities.

Updated [2367.0]: Information systems are scanned to proactively identify technical vulnerabilities at a frequency based on the organization's formally documented assessment of risk (annually at minimum).

Change: Vulnerability scanning frequency was changed from periodic to risk-based, while maintaining the annual minimum.

1561.11c1Organizational.4

Current [1488.0]: The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).

Updated [1488.1]: The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); defined roles and responsibilities; incident handling procedures (business and technical); communication and escalation procedures; reporting and retention requirements; and coordination with the organization's vulnerability management, security monitoring, and forensic capabilities.

Change: The revision updates the requirement so that incident handling is more clearly integrated with the organization's vulnerability management, security monitoring, and forensic capabilities, and supported by defined roles, communication and escalation procedures, and reporting and retention requirements.

1704.03b1Organizational.12

Current [0394.0]: The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and the results reviewed annually.

Updated [0394.1]: The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization, including risks arising from changes in vulnerability exploitability and threat conditions, and are to be performed at planned intervals, when major changes occur in the environment, and when changes in exploitability or threat conditions materially affect risk. Risk assessment results are reviewed annually.

Change: The revision updates the requirement so that risk assessments explicitly account for risks arising from changes in vulnerability exploitability and threat conditions, and are revisited not only at planned intervals and after major environmental changes, but also when those changes materially affect risk

Modifications to requirements in the current i1 baseline

0201.09j1Organizational.124

Current [0873.0]: Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.

Updated [0873.0]: Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-malware are addressed via a network-based malware detection (NBMD) solution.

Change: References to host-based anti-virus and anti-spyware software were replaced with the broader term host-based anti-malware.

1003.01d1System.3

Current [0069.0]: User identities are verified prior to performing password resets.

Updated [0069.0]: User identities are verified prior to performing password resets or binding passwordless authenticators (e.g., passkeys) to user accounts.

Change: Identity verification requirements were revised to clarify the inclusion of passwordless authenticators.

1114.01h1Organizational.123

Current [0114.0]: Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately. When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).

Updated [0114.0]: Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are immediately removed from document processing devices (e.g., printers, copiers, scanners, or multifunction devices). When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).

Change: References to printers, copiers, and facsimile machines were revised to clarify inclusion of all document processing devices, including printers, copiers, scanners, and multifunction devices.

0704.07a1Organizational.9

Current [0633.2]: The asset inventory includes the: unique identifier and/or serial number of the IT asset; information system of which the component is a part; type of information system component (e.g., server, desktop, application); manufacturer/model information of the IT asset; operating system type and version/service pack level of the IT asset; presence of virtual machines; application software version/license information; physical location (e.g., building/room number) of the IT asset; logical location (e.g., IP address, position with the IS architecture) of the IT asset; Media access control (MAC) address of the IT asset; data ownership and custodian by position and role; operational status of the IT asset; primary and secondary administrators of the IT asset; and primary user of the IT asset.

Updated [0633.2]: The asset inventory includes the: unique identifier and/or serial number of the IT asset; information system of which the component is a part; type of information system component (e.g., server, desktop, application); manufacturer/model information of the IT asset; operating system type, version, build/release, and patch level of the IT asset; presence of virtual machines; application software version/license information; physical location (e.g., building/room number) of the IT asset; logical location (e.g., IP address, position with the IS architecture) of the IT asset; Media access control (MAC) address of the IT asset; data ownership and custodian by position and role; operational status of the IT asset; primary and secondary administrators of the IT asset; and primary user of the IT asset.

Change: Asset inventory details were updated to capture operating system type, version, build or release, and patch level instead of version and service-pack level.

0715.10m1Organizational.4

Current [1375.0]: Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

Updated [1375.1]: Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.3 or later or TLS v1.2 with approved cipher suites, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).

Change: TLS examples were updated to align with NIST recommendations.

1903.06d1Organizational.3456711

Current [0569.0]: Covered and/or confidential information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs. Exceptions to encryption requirements are authorized by management and documented. Encryption is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures. For full-disk encryption, logical access is independent of O/S access. Decryption keys are not tied to user accounts. If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.

Updated [0569.0]: Covered and/or confidential information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs. Exceptions to encryption requirements are authorized by management and documented. Data protection is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures that account for cryptographic algorithm strength and lifecycle status. For full-disk encryption, logical access is independent of O/S access. Decryption keys are not tied to user accounts. If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.

Change: The requirement was revised require consideration of algorithm strength and lifecycle status.

1444.09t1Organizational.12

Current [1072.0]: Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions. The exchange and data sharing agreements also specify organization policies including: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys; and escrow agreements.

Updated [1072.0]: Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions. The exchange and data sharing agreements also specify organization policies including: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for

notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys or quantum-resistant cryptographic mechanisms; and escrow agreements.

Change: Quantum-resistant cryptographic mechanisms were added to the protections that exchange and data-sharing agreements may require.

0913.09s1Organizational.5

Current [1055.0]: Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security (TLS) 1.2 or later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TLS VPNs: SSL Portal VPN; SSL Tunnel VPN.

Updated [1055.1]: Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security configured with NIST-approved algorithms, such as TLS v1.3 or TLS v1.2 with approved cipher suites; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TLS VPNs: SSL Portal VPN; SSL Tunnel VPN.

Change: TLS examples were updated to align with NIST recommendations.

19922.06f1Organizational.2

Current [1954.0]: The encryption policy addresses the type and strength of the encryption algorithm and when used to protect the confidentiality of information. The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards.

Updated [1954.1]: The encryption policy addresses the type and strength of the encryption algorithm, including documented consideration of cryptographic algorithm lifecycle status and the need for quantum-resistant cryptographic mechanisms, and when encryption should be used to protect the confidentiality of information. The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards.

Change: Encryption-policy considerations were expanded to include documented consideration of cryptographic algorithm lifecycle status, the need for quantum-resistant mechanisms, and clarification of when encryption should protect information confidentiality.

02962.09j1Organizational.5

Current [1989.0]: The organization augments endpoint protection strategies with additional solutions—including those built into the operating system if available—to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).

Updated [1989.1]: The organization, based on a formally documented assessment of risk, augments endpoint protection strategies with additional risk-appropriate solutions—including those built into the operating system if available—to mitigate exploitation of unknown and context-dependent vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).

Change: Supplemental endpoint-protection measures were revised to be based on a documented assessment of risk and address context-dependent vulnerabilities.

0633.10j1System.1

Current [1329.0]: Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) are strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Updated [1329.0]: Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) are strictly controlled, in order to prevent the introduction of unauthorized functionality, security-impacting changes, and unintentional changes.

Change: Source-code access controls were expanded to prevent security-impacting changes, in addition to unauthorized functionality and unintentional changes.

0706.10b1System.2

Current [1263.1]: The organization develops applications based on secure coding guidelines to prevent: common coding vulnerabilities in software development processes; injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); buffer overflow (Validate buffer boundaries and truncate input strings); insecure cryptographic storage (Prevent cryptographic flaws); insecure communications (Properly encrypt all authenticated and sensitive communications); improper error handling (Do not leak information via error messages); broken 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); cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and any other input-validation vulnerability listed in the OWASP Top 10.

Updated [1263.3]: The organization develops applications in accordance with secure coding guidelines to prevent common, complex, and context-dependent coding vulnerabilities, including those associated with injection flaws, buffer overflow, insecure cryptographic storage, insecure communications, improper error handling, authentication and session management weaknesses, cross-site scripting (XSS), access control, and any other weakness addressed by OWASP.

Change: The secure coding requirement was substantially rewritten to consolidate detailed vulnerability examples into broader common, complex, and context-dependent weakness categories while still aligning to OWASP.

0709.10m1Organizational.1

Current [1369.0]: Once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Further, the organization performs the necessary actions to correct identified technical vulnerabilities in a timely manner.

Updated [1369.1]: Once a potential technical vulnerability has been identified, the organization identifies the associated risks, determines the appropriate response based on exploitability and severity, and performs the necessary actions to remediate the vulnerability within formally documented, risk-tiered remediation timeframes.

Change: Vulnerability response decisions must consider exploitability and severity, with remediation required within formally documented, risk-tiered timeframes.

0778.10m1Organizational.5

Current [1398.0]: The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

Updated [1398.0]: The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been effectively remediated within formally documented, risk-tiered remediation timeframes.

Change: Consecutive vulnerability-scan results must confirm effective remediation within formally documented, risk-tiered timeframes.

12101.09ab1System.2

Current [1148.0]: The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.

Updated [1148.1]: The organization specifies, based on a formally documented assessment of risk, how often audit logs are reviewed, how the reviews are documented, the specific roles and responsibilities of the personnel conducting the reviews, and the professional certifications or other qualifications required.

Change: Audit-log review frequency was made dependent on a formally documented risk assessment, while documentation, role, responsibility, and qualification requirements were retained.

1270.09ad1System.12

Current [1216.0]: The organization ensures that proper logging is enabled in order to audit administrator activities. The organization ensures system administrator logs and operator logs are reviewed on a regular basis.

Updated [1216.1]: The organization ensures proper logging is enabled in order to audit operator and administrator activities and detect indicators of exploitation of technical vulnerabilities, system administrator logs are reviewed at a formally documented frequency based on an assessment of risk, and system operator logs are reviewed at a formally documented frequency based on an assessment of risk.

Change: Logging was expanded to audit operator as well as administrator activities and detect indicators of technical-vulnerability exploitation; administrator and operator log-review frequencies were made risk-based.

1272.09ae1System.13

Current [1218.0]: Faults reported by users or by system programs related to problems with information processing or communications systems are logged. Error logging is enabled if this system function is available.

Updated [1218.0]: Faults reported by users or by system programs related to problems with information processing or communications systems, including anomalous conditions that may indicate exploitation of technical vulnerabilities, are logged. Error logging is enabled if this system function is available.

Change: The types of faults required to be logged were expanded to include anomalous conditions that may indicate exploitation of technical vulnerabilities.

12148.06i1Organizational.1

Current [2121.0]: The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; and override of access control mechanisms.

Updated [2121.1]: The organization, based on a formally documented assessment of risk, determines which of the following auditable events require auditing on a continuous basis: user log-on and log-off (successful or unsuccessful); configuration changes; application alerts and error messages; all system administration activities; modification of privileges and access; account creation, modification, or deletion; concurrent log on from different workstations; override of access control mechanisms; and other auditable events indicative of exploitation of technical vulnerabilities (e.g., unexpected outbound connections, unexpected inter-process injection, suspicious scheduled execution).

Change: Continuous auditing decisions were made risk-based, and auditable events that may indicate technical-vulnerability exploitation were added.

1416.10l1Organizational.1

Current [1365.0]: Where software development is outsourced, formal contracts are in place to address: licensing arrangements; code ownership; intellectual property rights; certification of the quality and accuracy of the work; rights of access for the audit of the quality and accuracy of work; escrow arrangements; quality and security functionality requirements for the developed code; and security testing and evaluation prior to installation.

Updated [1365.0]: Where software development is outsourced, formal contracts are in place to address: licensing arrangements; code ownership; intellectual property rights; certification of the quality and accuracy of the work; rights of access for the audit of the quality and accuracy of work; escrow arrangements; quality and security functionality requirements for the developed code, including the identification and remediation of technical vulnerabilities; and security testing and evaluation prior to installation.

Change: Identification and remediation of technical vulnerabilities were added to security requirements for outsourced software development.

1535.11b1Organizational.12

Current [1457.0]: The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.

Updated [1457.0]: The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including suspicious or unusual system activity, violations of workforce rules of behavior, and acceptable use agreement violations, to their management and/or directly to their service provider as quickly as possible.

Change: Suspicious or unusual system activity was added to the reportable information and the acceptable-use-agreement language was clarified.

1589.11c1Organizational.5

Current [1462.0]: The organization tests and/or exercises its incident response capability regularly.

Updated [1462.1]: The organization tests and/or exercises its incident response capability at least annually, and more frequently based on a formally documented assessment of risk, for scenarios identified in the organization's documented risk assessment (e.g., the exploitation of technical vulnerabilities).

Change: The requirement was revised to require testing or exercising of the incident response capability at least annually and more frequently as needed based on a formally documented assessment of risk.

1560.11d1Organizational.1

Current [1487.0]: The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy.

Updated [1487.0]: The information gained from the evaluation of information security incidents is used to identify recurring, high-impact, or vulnerability-exploitation-related incidents, and update the incident response and recovery strategy.

Change: Incident evaluations were expanded to identify vulnerability-exploitation-related incidents, in addition to recurring or high-impact incidents.

1563.11d1Organizational.2

Current [1490.0]: The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.

Updated [1490.0]: The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises, including for incidents involving exploitation of technical vulnerabilities. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.

Change: Lessons learned from incidents involving exploitation of technical vulnerabilities must be incorporated into incident response procedures, training, and testing.

1781.10a1Organizational.23

Current [1227.0]: Specifications for the security control requirements include security controls to be incorporated in the information system, and supplemented by manual controls as needed. Further, security control requirements are considered when evaluating software packages, either developed or purchased.

Updated [1227.0]: Specifications for security control requirements include security controls to be incorporated in the information system to address common, complex, and context-dependent weaknesses, and supplemented by manual controls as needed. Security control requirements addressing such weaknesses are considered when evaluating software packages, whether developed or purchased.

Change: Security-control requirements were refocused on common, complex, and context-dependent weaknesses, which must also be considered when evaluating developed or purchased software.