3.3 AUDIT AND ACCOUNTABILITY

Quick link to Audit and Accountability Summary Table

AU-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] audit and accountability policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Audit and accountability policy and procedures address the controls in the AU family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of audit and accountability policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to audit and accountability policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

AU-2 EVENT LOGGING

Control:

a. Identify the types of events that the system is capable of logging in support of the audit function: [*Assignment: organization-defined event types that the system is capable of logging*];

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: [*Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type*];

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

Discussion: An event is an observable occurrence in a system. The types of events that require logging are those events that are significant and relevant to the security of systems and the privacy of individuals. Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage. In determining the set of event types that require logging, organizations consider the monitoring and auditing appropriate for each of the controls to be implemented. For completeness, event logging includes all protocols that are operational and supported by the system.

To balance monitoring and auditing requirements with other system needs, event logging requires identifying the subset of event types that are logged at a given point in time. For example, organizations may determine that systems need the capability to log every file access successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. The types of events that organizations desire to be logged may change. Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization. Organizations consider how the types of logging events can reveal information about individuals that may give rise to privacy risk and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the logging event is based on patterns or time of usage.

Event logging requirements, including the need to log specific event types, may be referenced in other controls and control enhancements. These include AC-2(4), AC-3(10), AC-6(9), AC-17(1), CM-3f, CM-5(1), IA-3(3.b), MA-4(1), MP-4(2), PE-3, PM-21, PT-7, RA-8, SC-7(9), SC-7(15), SI-3(8), SI-4(22), SI-7(8), and SI-10(1). Organizations include event types that are required by applicable laws, executive orders, directives, policies, regulations, standards, and guidelines. Audit records can be generated at various levels, including at the packet level as information traverses the network. Selecting the appropriate level of event logging is an important part of a monitoring and auditing capability and can identify the root causes of problems. When defining event types, organizations consider the logging necessary to cover related event types, such as the steps in distributed, transaction-based processes and the actions that occur in service-oriented architectures.

Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Control Enhancements:

(1) EVENT LOGGING | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES

[Withdrawn: Incorporated into AU-12.]

(2) EVENT LOGGING | SELECTION OF AUDIT EVENTS BY COMPONENT

[Withdrawn: Incorporated into AU-12.]

(3) EVENT LOGGING | REVIEWS AND UPDATES

[Withdrawn: Incorporated into AU-2.]

(4) EVENT LOGGING | PRIVILEGED FUNCTIONS

[Withdrawn: Incorporated into AC-6(9).]

References: [OMB A-130], [SP 800-92].

AU-3 CONTENT OF AUDIT RECORDS

Control: Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Related Controls: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

Control Enhancements:

(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION

Generate audit records containing the following additional information: [*Assignment: organization-defined additional information*].

Discussion: The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records including, but not limited to, access control or flow control rules invoked and individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements. This facilitates the use of audit trails and audit logs by not including information in audit records that could potentially be misleading, make it more difficult to locate information of interest, or increase the risk to individuals' privacy.

Related Controls: None.

(2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

[Withdrawn: Incorporated into PL-9.]

(3) CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS

Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [*Assignment: organization-defined elements*].

Discussion: Limiting personally identifiable information in audit records when such information is not needed for operational purposes helps reduce the level of privacy risk created by a system.

Related Controls: RA-3.

References: [OMB A-130], [IR 8062].

AU-4 AUDIT LOG STORAGE CAPACITY

Control: Allocate audit log storage capacity to accommodate [*Assignment: organization-defined audit log retention requirements*].

Discussion: Organizations consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging capability.

Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Control Enhancements:

(1) AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE

Transfer audit logs [*Assignment: organization-defined frequency*] to a different system, system component, or media other than the system or system component conducting the logging.

Discussion: Audit log transfer, also known as off-loading, is a common process in systems with limited audit log storage capacity and thus supports availability of the audit logs. The initial audit log storage is only used in a transitory fashion until the system can communicate with the secondary or alternate system allocated to audit log storage, at which point the audit logs are transferred. Transferring audit logs to alternate storage is similar to AU-9(2) in that audit logs are transferred to a different entity. However, the purpose of selecting AU-9(2) is to protect the confidentiality and integrity of audit records. Organizations can select either control enhancement to obtain the benefit of increased audit log storage capacity and preserving the confidentiality, integrity, and availability of audit records and logs.

Related Controls: None.

References: None.

AU-5 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control:

a. Alert [*Assignment: organization-defined personnel or roles*] within [*Assignment: organization-defined time period*] in the event of an audit logging process failure; and

b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Organization-defined actions include overwriting oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

Related Controls: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Control Enhancements:

(1) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | STORAGE CAPACITY WARNING

Provide a warning to [*Assignment: organization-defined personnel, roles, and/or locations*] within [*Assignment: organization-defined time period*] when allocated audit log storage volume reaches [*Assignment: organization-defined percentage*] of repository maximum audit log storage capacity.

Discussion: Organizations may have multiple audit log storage repositories distributed across multiple system components with each repository having different storage volume capacities.

Related Controls: None.

(2) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS

Provide an alert within [*Assignment: organization-defined real-time period*] to [*Assignment: organization-defined personnel, roles, and/or locations*] when the following audit failure events occur: [*Assignment: organization-defined audit logging failure events requiring real-time alerts*].

Discussion: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

Related Controls: None.

(3) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS

Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [*Selection: reject; delay*] network traffic above those thresholds.

Discussion: Organizations have the capability to reject or delay the processing of network communications traffic if audit logging information about such traffic is determined to exceed the storage capacity of the system audit logging function. The rejection or delay response is triggered by the established organizational traffic volume thresholds that can be adjusted based on changes to audit log storage capacity.

Related Controls: None.

(4) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE

Invoke a [*Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available*] in the event of [*Assignment: organization-defined audit logging failures*], unless an alternate audit logging capability exists.

Discussion: Organizations determine the types of audit logging failures that can trigger automatic system shutdowns or degraded operations. Because of the importance of ensuring mission and business continuity, organizations may determine that the nature of the audit logging failure is not so severe that it warrants a complete shutdown of the system supporting the core organizational mission and business functions. In those instances, partial system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives.

Related Controls: AU-15.

(5) RESPONSE TO AUDIT LOGGING PROCESS FAILURES | ALTERNATE AUDIT LOGGING CAPABILITY

Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [*Assignment: organization-defined alternate audit logging functionality*].

Discussion: Since an alternate audit logging capability may be a short-term protection solution employed until the failure in the primary audit logging capability is corrected, organizations may determine that the alternate audit logging capability need only provide a subset of the primary audit logging functionality that is impacted by the failure.

Related Controls: AU-9.

References: None.

AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control:

a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications of [*Assignment: organization-defined inappropriate or unusual activity*] and the potential impact of the inappropriate or unusual activity;

b. Report findings to [*Assignment: organization-defined personnel or roles*]; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Discussion: Audit record review, analysis, and reporting covers information security- and privacy-related logging performed by organizations, including logging that results from the monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and non-local maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at system interfaces, and use of mobile code or Voice over Internet Protocol (VoIP). Findings can be reported to organizational entities that include the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The frequency, scope, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received.

Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION

Integrate audit record review, analysis, and reporting processes using [*Assignment: organization-defined automated mechanisms*].

Discussion: Organizational processes that benefit from integrated audit record review, analysis, and reporting include incident response, continuous monitoring, contingency planning, investigation and response to suspicious activities, and Inspector General audits.

Related Controls: PM-7.

(2) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS

[Withdrawn: Incorporated into SI-4.]

(3) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES

Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

Discussion: Organization-wide situational awareness includes awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level) and supports cross-organization awareness.

Related Controls: AU-12, IR-4.

(4) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS

Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Discussion: Automated mechanisms for centralized reviews and analyses include Security Information and Event Management products.

Related Controls: AU-2, AU-12.

(5) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS

Integrate analysis of audit records with analysis of [*Selection (one or more): vulnerability scanning information; performance data; system monitoring information;* [*Assignment: organization-defined data/information collected from other sources*]] to further enhance the ability to identify inappropriate or unusual activity.

Discussion: Integrated analysis of audit records does not require vulnerability scanning, the generation of performance data, or system monitoring. Rather, integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans of the system and in correlating attack detection events with scanning results. Correlation with performance data can uncover denial-of-service attacks or other types of attacks that result in the unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations.

Related Controls: AU-12, IR-4.

(6) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING

Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Discussion: The correlation of physical audit record information and the audit records from systems may assist organizations in identifying suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain systems with the additional physical security information that the individual was present at the facility when the logical access occurred may be useful in investigations.

Related Controls: None.

(7) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS

Specify the permitted actions for each [*Selection (one or more): system process; role; user*] associated with the review, analysis, and reporting of audit record information.

Discussion: Organizations specify permitted actions for system processes, roles, and users associated with the review, analysis, and reporting of audit records through system account management activities. Specifying permitted actions on audit record information is a way to enforce the principle of least privilege. Permitted actions are enforced by the system and include read, write, execute, append, and delete.

Related Controls: None.

(8) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS

Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Discussion: Full text analysis of privileged commands requires a distinct environment for the analysis of audit record information related to privileged users without compromising such information on the system where the users have elevated privileges, including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and parameters) as opposed to analysis that considers only the name of the command. Full text analysis includes the use of pattern matching and heuristics.

Related Controls: AU-3, AU-9, AU-11, AU-12.

(9) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES

Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Discussion: Nontechnical sources include records that document organizational policy violations related to harassment incidents and the improper use of information assets. Such information can lead to a directed analytical effort to detect potential malicious insider activity. Organizations limit access to information that is available from nontechnical sources due to its sensitive nature. Limited access minimizes the potential for inadvertent release of privacy-related information to individuals who do not have a need to know. The correlation of information from nontechnical sources with audit record information generally occurs only when individuals are suspected of being involved in an incident. Organizations obtain legal advice prior to initiating such actions.

Related Controls: PM-12.

(10) AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT

[Withdrawn: Incorporated into AU-6.]

References: [SP 800-86], [SP 800-101].

AU-7 AUDIT RECORD REDUCTION AND REPORT GENERATION

Control: Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Discussion: Audit record reduction is a process that manipulates collected audit log information and organizes it into a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or from the same organizational entities that conduct audit logging activities. The audit record reduction capability includes modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be an issue if the granularity of the timestamp in the record is insufficient.

Related Controls: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.

Control Enhancements:

(1) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING

Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [*Assignment: organization-defined fields within audit records*].

Discussion: Events of interest can be identified by the content of audit records, including system resources involved, information objects accessed, identities of individuals, event types, event locations, event dates and times, Internet Protocol addresses involved, or event success or failure. Organizations may define event criteria to any degree of granularity required, such as locations selectable by a general networking location or by specific system component.

Related Controls: None.

(2) AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH

[Withdrawn: Incorporated into AU-7(1).]

References: None.

AU-8 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity of time measurement*] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Discussion: Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds of milliseconds or tens of milliseconds). Organizations may define different time granularities for different system components. Time service can be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Related Controls: AU-3, AU-12, AU-14, SC-45.

Control Enhancements:

(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

[Withdrawn: Moved to SC-45(1).]

(2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE

[Withdrawn: Moved to SC-45(2).]

References: None.

AU-9 PROTECTION OF AUDIT INFORMATION

Control:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and

b. Alert [*Assignment: organization-defined personnel or roles*] upon detection of unauthorized access, modification, or deletion of audit information.

Discussion: Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Related Controls: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Control Enhancements:

(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA

Write audit trails to hardware-enforced, write-once media.

Discussion: Writing audit trails to hardware-enforced, write-once media applies to the initial generation of audit trails (i.e., the collection of audit records that represents the information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. Writing audit trails to hardware-enforced, write-once media does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes Compact Disc-Recordable (CD-R), Blu-Ray Disc Recordable (BD-R), and Digital Versatile Disc-Recordable (DVD-R). In contrast, the use of switchable write-protection media, such as tape cartridges, Universal Serial Bus (USB) drives, Compact Disc Re-Writeable (CD-RW), and Digital Versatile Disc-Read Write (DVD-RW) results in write-protected but not write-once media.

Related Controls: AU-4, AU-5.

(2) PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS

Store audit records [*Assignment: organization-defined frequency*] in a repository that is part of a physically different system or system component than the system or component being audited.

Discussion: Storing audit records in a repository separate from the audited system or system component helps to ensure that a compromise of the system being audited does not also result in a compromise of the audit records. Storing audit records on separate physical systems or components also preserves the confidentiality and integrity of audit records and facilitates the management of audit records as an organization-wide activity. Storing audit records on separate systems or components applies to initial generation as well as backup or long-term storage of audit records.

Related Controls: AU-4, AU-5.

(3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Discussion: Cryptographic mechanisms used for protecting the integrity of audit information include signed hash functions using asymmetric cryptography. This enables the distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Related Controls: AU-10, SC-12, SC-13.

(4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

Authorize access to management of audit logging functionality to only [*Assignment: organization-defined subset of privileged users or roles*].

Discussion: Individuals or roles with privileged access to a system and who are also the subject of an audit by that system may affect the reliability of the audit information by inhibiting audit activities or modifying audit records. Requiring privileged access to be further defined between audit-related privileges and other privileges limits the number of users or roles with audit-related privileges.

Related Controls: AC-5.

(5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

Enforce dual authorization for [*Selection (one or more): movement; deletion*] of [*Assignment: organization-defined audit information*].

Discussion: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms (also known as two-person control) require the approval of two authorized individuals to execute audit functions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety.

Related Controls: AC-3.

(6) PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS

Authorize read-only access to audit information to [*Assignment: organization-defined subset of privileged users or roles*].

Discussion: Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.

Related Controls: None.

(7) PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM

Store audit information on a component running a different operating system than the system or component being audited.

Discussion: Storing auditing information on a system component running a different operating system reduces the risk of a vulnerability specific to the system, resulting in a compromise of the audit records.

Related controls: AU-4, AU-5, AU-11, SC-29.

References: [FIPS 140-3], [FIPS 180-4], [FIPS 202].

AU-10 NON-REPUDIATION

Control: Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [*Assignment: organization-defined actions to be covered by non-repudiation*].

Discussion: Types of individual actions covered by non-repudiation include creating information, sending and receiving messages, and approving information. Non-repudiation protects against claims by authors of not having authored certain documents, senders of not having transmitted messages, receivers of not having received messages, and signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from an individual or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request, or receiving specific information). Organizations obtain non-repudiation services by employing various techniques or mechanisms, including digital signatures and digital message receipts.

Related Controls: AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Control Enhancements:

(1) NON-REPUDIATION | ASSOCIATION OF IDENTITIES

(a) Bind the identity of the information producer with the information to [*Assignment: organization-defined strength of binding*]; and

(b) Provide the means for authorized individuals to determine the identity of the producer of the information.

Discussion: Binding identities to the information supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of attribute binding between the information producer and the information based on the security category of the information and other relevant risk factors.

Related Controls: AC-4, AC-16.

(2) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY

(a) Validate the binding of the information producer identity to the information at [*Assignment: organization-defined frequency*]; and

(b) Perform [*Assignment: organization-defined actions*] in the event of a validation error.

Discussion: Validating the binding of the information producer identity to the information prevents the modification of information between production and review. The validation of bindings can be achieved by, for example, using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls: AC-3, AC-4, AC-16.

(3) NON-REPUDIATION | CHAIN OF CUSTODY

Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.

Discussion: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each individual who handled the evidence, the date and time the evidence was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release or transfer function, the system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, maintaining the credentials of reviewers or releasers provides the organization with the means to identify who reviewed and released the information. In the case of automated reviews, it ensures that only approved review functions are used.

Related Controls: AC-4, AC-16.

(4) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY

(a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [*Assignment: organization-defined security domains*]; and

(b) Perform [*Assignment: organization-defined actions*] in the event of a validation error.

Discussion: Validating the binding of the information reviewer identity to the information at transfer or release points prevents the unauthorized modification of information between review and the transfer or release. The validation of bindings can be achieved by using cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically.

Related Controls: AC-4, AC-16.

(5) NON-REPUDIATION | DIGITAL SIGNATURES

[Withdrawn: Incorporated into SI-7.]

References: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-177].

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Discussion: Organizations retain audit records until it is determined that the records are no longer needed for administrative, legal, audit, or other operational purposes. This includes the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on records retention.

Related Controls: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Control Enhancements:

(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY

Employ [*Assignment: organization-defined measures*] to ensure that long-term audit records generated by the system can be retrieved.

Discussion: Organizations need to access and read audit records requiring long-term storage (on the order of years). Measures employed to help facilitate the retrieval of audit records include converting records to newer formats, retaining equipment capable of reading the records, and retaining the necessary documentation to help personnel understand how to interpret the records.

Related Controls: None.

References: [OMB A-130].

AU-12 AUDIT RECORD GENERATION

Control:

a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [*Assignment: organization-defined system components*];

b. Allow [*Assignment: organization-defined personnel or roles*] to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Discussion: Audit records can be generated from many different system components. The event types specified in AU-2d are the event types for which audit logs are to be generated and are a subset of all event types for which the system can generate audit records.

Related Controls: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

Control Enhancements:

(1) AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL

Compile audit records from [*Assignment: organization-defined system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail*].

Discussion: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances.

Related Controls: AU-8, SC-45.

(2) AUDIT RECORD GENERATION | STANDARDIZED FORMATS

Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Discussion: Audit records that follow common standards promote interoperability and information exchange between devices and systems. Promoting interoperability and information exchange facilitates the production of event information that can be readily analyzed and correlated. If logging mechanisms do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails.

Related Controls: None.

(3) AUDIT RECORD GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS

Provide and implement the capability for [*Assignment: organization-defined individuals or roles*] to change the logging to be performed on [*Assignment: organization-defined system components*] based on [*Assignment: organization-defined selectable event criteria*] within [*Assignment: organization-defined time thresholds*].

Discussion: Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed (e.g., near real-time, within minutes, or within hours).

Related Controls: AC-3.

(4) AUDIT RECORD GENERATION | QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION

Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.

Discussion: Query parameters are explicit criteria that an individual or automated system submits to a system to retrieve data. Auditing of query parameters for datasets that contain personally identifiable information augments the capability of an organization to track and understand the access, usage, or sharing of personally identifiable information by authorized personnel.

Related Controls: None.

References: None.

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control:

a. Monitor [*Assignment: organization-defined open-source information and/or information sites*] [*Assignment: organization-defined frequency*] for evidence of unauthorized disclosure of organizational information; and

b. If an information disclosure is discovered:

1. Notify [*Assignment: organization-defined personnel or roles*]; and
2. Take the following additional actions: [*Assignment: organization-defined additional actions*].

Discussion: Unauthorized disclosure of information is a form of data leakage. Open-source information includes social networking sites and code-sharing platforms and repositories. Examples of organizational information include personally identifiable information retained by the organization or proprietary information generated by the organization.

Related Controls: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Control Enhancements:

(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS

Monitor open-source information and information sites using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms include commercial services that provide notifications and alerts to organizations and automated scripts to monitor new posts on websites.

Related Controls: None.

(2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES

Review the list of open-source information sites being monitored [*Assignment: organization-defined frequency*].

Discussion: Reviewing the current list of open-source information sites being monitored on a regular basis helps to ensure that the selected sites remain relevant. The review also provides the opportunity to add new open-source information sites with the potential to provide evidence of unauthorized disclosure of organizational information. The list of sites monitored can be guided and informed by threat intelligence of other credible sources of information.

Related Controls: None.

(3) MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED REPLICATION OF INFORMATION

Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.

Discussion: The unauthorized use or replication of organizational information by external entities can cause adverse impacts on organizational operations and assets, including damage to reputation. Such activity can include the replication of an organizational website by an adversary or hostile threat actor who attempts to impersonate the web-hosting organization. Discovery tools, techniques, and processes used to determine if external entities are replicating organizational information in an unauthorized manner include scanning external websites, monitoring social media, and training staff to recognize the unauthorized use of organizational information.

Related Controls: None.

References: None.

AU-14 SESSION AUDIT

Control:

a. Provide and implement the capability for [*Assignment: organization-defined users or roles*] to [*Selection (one or more): record; view; hear; log*] the content of a user session under [*Assignment: organization-defined circumstances*]; and

b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Discussion: Session audits can include monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session audit capability is implemented in addition to event logging and may involve implementation of specialized session capture technology. Organizations consider how session auditing can reveal information about individuals that may give rise to privacy risk as well as how to mitigate those risks. Because session auditing can impact system and network performance, organizations activate the capability under well-defined situations (e.g., the organization is suspicious of a specific individual). Organizations consult with legal counsel, civil liberties officials, and privacy officials to ensure that any legal, privacy, civil rights, or civil liberties issues, including the use of personally identifiable information, are appropriately addressed.

Related Controls: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Control Enhancements:

(1) SESSION AUDIT | SYSTEM START-UP

Initiate session audits automatically at system start-up.

Discussion: The automatic initiation of session audits at startup helps to ensure that the information being captured on selected individuals is complete and not subject to compromise through tampering by malicious threat actors.

Related Controls: None.

(2) SESSION AUDIT | CAPTURE AND RECORD CONTENT

[Withdrawn: Incorporated into AU-14.]

(3) SESSION AUDIT | REMOTE VIEWING AND LISTENING

Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.

Discussion: None.

Related Controls: AC-17.

References: None.

AU-15 ALTERNATE AUDIT LOGGING CAPABILITY

[Withdrawn: Moved to AU-5(5).]

AU-16 CROSS-ORGANIZATIONAL AUDIT LOGGING

Control: Employ [*Assignment: organization-defined methods*] for coordinating [*Assignment: organization-defined audit information*] among external organizations when audit information is transmitted across organizational boundaries.

Discussion: When organizations use systems or services of external organizations, the audit logging capability necessitates a coordinated, cross-organization approach. For example, maintaining the identity of individuals who request specific services across organizational boundaries may often be difficult, and doing so may prove to have significant performance and privacy ramifications. Therefore, it is often the case that cross-organizational audit logging simply captures the identity of individuals who issue requests at the initial system, and subsequent systems record that the requests originated from authorized individuals. Organizations consider including processes for coordinating audit information requirements and protection of audit information in information exchange agreements.

Related Controls: AU-3, AU-6, AU-7, CA-3, PT-7.

Control Enhancements:

(1) CROSS-ORGANIZATIONAL AUDIT LOGGING | IDENTITY PRESERVATION

Preserve the identity of individuals in cross-organizational audit trails.

Discussion: Identity preservation is applied when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual.

Related Controls: IA-2, IA-4, IA-5, IA-8.

(2) CROSS-ORGANIZATIONAL AUDIT LOGGING | SHARING OF AUDIT INFORMATION

Provide cross-organizational audit information to [*Assignment: organization-defined organizations*] based on [*Assignment: organization-defined cross-organizational sharing agreements*].

Discussion: Due to the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only individuals' home organizations have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.

Related Controls: IR-4, SI-4.

(3) CROSS-ORGANIZATIONAL AUDITING | DISASSOCIABILITY

Implement [*Assignment: organization-defined measures*] to disassociate individuals from audit information transmitted across organizational boundaries.

Discussion: Preserving identities in audit trails could have privacy ramifications, such as enabling the tracking and profiling of individuals, but may not be operationally necessary. These risks could be further amplified when transmitting information across organizational boundaries. Implementing privacy-enhancing cryptographic techniques can disassociate individuals from audit information and reduce privacy risk while maintaining accountability.

Related Controls: None.

References: None.