

Department of the Interior
Security Control Standard
Audit and Accountability

January 2012

Version: 1.2



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	December 8, 2010	Initial draft
Timothy Brown	0.2	December 10, 2010	Incorporated comments into text, removed non-mandated control enhancements
Timothy Brown	0.21	January 07, 2011	Added introductory paragraph
Timothy Brown	0.22	February 15, 2011	Checked/added moderate cloud to high
Chris Peterson	1.0	February 18, 2011	Final review of controls; removed margin notes
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1
Lawrence K. Ruffin	1.2	January 18, 2012	Revisions for closer alignment to FedRAMP Baseline Security Controls.v1.0 dated 1/6/2012

TABLE OF CONTENTS

REVISION HISTORY3

TABLE OF CONTENTS4

SECURITY CONTROL STANDARD: AUDIT AND ACCOUNTABILITY5

 AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES5

 AU-2 AUDITABLE EVENTS6

 AU-3 CONTENT OF AUDIT RECORDS7

 AU-4 AUDIT STORAGE CAPACITY8

 AU-5 RESPONSE TO AUDIT PROCESSING FAILURES8

 AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING9

 AU-7 AUDIT REDUCTION AND REPORT GENERATION9

 AU-8 TIME STAMPS10

 AU-9 PROTECTION OF AUDIT INFORMATION10

 AU-10 NON-REPUDIATION10

 AU-11 AUDIT RECORD RETENTION11

 AU-12 AUDIT GENERATION12

SECURITY CONTROL STANDARD: AUDIT AND ACCOUNTABILITY

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Audit and Accountability (AU) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

- a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the

organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AU-1	MOD AU-1	HIGH AU-1
----	----------	----------	-----------

AU-2 AUDITABLE EVENTS

Applicability: All Information Systems

Control: The organization:

- a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;
- b. Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
- c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
- d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: *[Assignment: organization defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event]*.

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are to be *audited* at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.

Control Enhancements:

3. The organization reviews and updates the list of auditable events annually or whenever there is a change in the threat environment.

Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.

4. The organization includes execution of privileged functions in the list of events to be audited by the information system and configures auditing features of operating systems, databases, and applications to record security-related events, to include logon/logoff and all failed access attempts.

References: NIST Special Publication 800-92.

Priority and Baseline Allocation:

P1	LOW AU-2	MOD AU-2 (3) (4)	HIGH AU-2 (3) (4)
-----------	-----------------	-------------------------	--------------------------

AU-3 CONTENT OF AUDIT RECORDS

Applicability: All Information Systems

Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.

Control Enhancements:

1. The information system includes session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the audit records for audit events identified by type, location, or subject.

Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

2. The organization centrally manages the content of audit records generated by individual components throughout the system.

References: None.

Priority and Baseline Allocation:

P1	LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)
-----------	-----------------	---------------------	--------------------------

AU-4 AUDIT STORAGE CAPACITY

Applicability: All Information Systems

Control: Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW AU-4	MOD AU-4	HIGH AU-4
-----------	-----------------	-----------------	------------------

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Applicability: All Information Systems

Control: The information system:

- a. Alerts designated organizational officials in the event of an audit processing failure; and
- b. Takes the following additional actions: overwrite oldest audit records (low impact system); shut down information system (moderate and high impact systems).

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

1. The information system provides a warning when allocated audit record storage volume reaches 75 percent of maximum audit record storage capacity.
2. The information system provides a real-time alert when the following audit failure events occur: any critical device failure; any administrator account failure; all relevant user activity that could lead to an incident or attempted security breach.

References: None.

Priority and Baseline Allocation:

P1	LOW AU-5	MOD AU-5	HIGH AU-5 (1) (2)
-----------	-----------------	-----------------	--------------------------

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Applicability: All Information Systems

Control: The organization:

- a. Reviews and analyzes information system audit records *at least weekly* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
- b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: Related control: AU-7.

Control Enhancements:

1. The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.
3. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

References: None.

Priority and Baseline Allocation:

P1	LOW AU-6	MOD AU-6 (1) (3)	HIGH AU-6 (1) (3)
-----------	-----------------	-------------------------	--------------------------

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Applicability: Moderate and High Impact Information Systems

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.

Control Enhancements:

1. The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

References: None.

Priority and Baseline Allocation:

P2	LOW Not Selected	MOD AU-7 (1)	HIGH AU-7 (1)
-----------	-------------------------	---------------------	----------------------

AU-8 TIME STAMPS

Applicability: All Information Systems

Control: The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.

Control Enhancements:

1. The information system synchronizes internal information system clocks at least hourly with a NIST Internet Time Service server.

References: <http://tf.nist.gov/tf-cgi/servers.cgi>

Priority and Baseline Allocation:

P2	LOW AU-8	MOD AU-8 (1)	HIGH AU-8 (1)
-----------	-----------------	---------------------	----------------------

AU-9 PROTECTION OF AUDIT INFORMATION

Applicability: All Information Systems

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.

Control Enhancements:

2. The information system backs up audit records at least weekly onto a different system or media than the system being audited.

References: None.

Priority and Baseline Allocation:

P1	LOW AU-9	MOD AU-9 (2)	HIGH AU-9 (2)
-----------	-----------------	---------------------	----------------------

AU-10 NON-REPUDIATION

Applicability: Moderate and High Impact Information Systems

Control: The information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. 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 received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Control Enhancements:

5. The organization employs FIPS 140-2 validated cryptography to implement digital signatures.

Enhancement Supplemental Guidance: Related control: SC-13.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AU-10 (5)	HIGH AU-10 (5)
-----------	-------------------------	----------------------	-----------------------

AU-11 AUDIT RECORD RETENTION

Applicability: All Information Systems

Control: The organization retains audit records for 30 days (low impact systems), 60 days (moderate impact systems), or 90 days (high impact systems) to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	LOW AU-11	MOD AU-11	HIGH AU-11
-----------	------------------	------------------	-------------------

AU-12 AUDIT GENERATION

Applicability: All Information Systems

Control: The information system:

- a. Provides audit record generation capability for the list of auditable events defined in AU-2 at all information system components where audit capability is deployed;
- b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and
- c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Supplemental Guidance: Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.

Control Enhancements:

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

Enhancement Supplemental Guidance: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

References: None.

Priority and Baseline Allocation:

P3	LOW AU-12	MOD AU-12	HIGH AU-12 (1)
-----------	------------------	------------------	-----------------------