



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.16-02 v2024-02

Published: 2024-02-23

**Audit And Accountability
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	3
Document History Log	3
Approval	3
1. Introduction	4
1.1. Purpose	4
1.2. Scope	4
1.3. Point of Contact(s)	5
1.4. Applicability	5
1.5. Applicable Documents	5
1.5.1. Federal Information Processing Standards (FIPS)	5
1.5.2. National Institute of Standards and Technology (NIST)	5
1.5.3. National Aeronautics and Space Administration (NASA)	5
1.5.4. Cancellations, Updates, Consolidations	5
2. Security Controls	5
2.1. Audit Events (AU-2)	5
2.1.1. Information System Owner (ISO)	6
2.1.2. Information System Security Officer (ISSO)	6
2.2. Content of Audit Records (AU-3)	6
2.2.1. Information System Security Officer (ISSO)	6
2.3. Audit Storage Capacity (AU-4)	6
2.3.1. Information System Owner (ISO)	6
2.4. Response to Audit Processing Failures (AU-5)	6
2.4.1. Information System Security Officer (ISSO)	6
2.5. Audit Review, Analysis, and Reporting (AU-6)	7
2.5.1. Information System Owner (ISO)	7
2.6. Audit Reduction and Report Generation (AU-7)	7
2.6.1. Information System Owner (ISO)	7
2.7. Time Stamps (AU-8)	7
2.7.1. Information System Owner (ISO)	7
2.8. Protection of Audit Information (AU-9)	7
2.8.1. Senior Agency Information Security Officer (SAISO)	7
2.8.2. Information System Owner (ISO)	7
2.9. Non-Repudiation (AU-10)	8
2.9.1. Information System Owner (ISO)	8
2.10. Audit Record Retention (AU-11)	8
2.10.1. Information System Owner (ISO)	8
2.11. Audit Generation (AU-12)	8
2.11.1. Information System Owner (ISO)	8
Appendix A: Acronyms	8

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-06	Initial Draft
1.1	2013-04-30	Extended for 1 year.
1.2	2014-04-24	Extended while revision 4 updates are incorporated into the handbook.
1.3	2015-03-03	Revised for Rev 4 controls & ODVS, updated TOC
1.4	2017-02-14	Extended for updates
1.5	2017-04-13	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.6	2018-07-31	Updated to new format
1.7	2019-11-06	Annual review; no changes
1.8	2021-09-22	Updated with NIST 800-53 Rev. 5 provisions.
1.9	2022-01-19	Minor reference correction to para 2.1
2.0	2023-01-31	Annual update and reference correction Subsection 1.5.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update. Acronym corrected

Approval

Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems), and in the selection and implementation of information security controls (FIPS 200, Minimum Security Requirements for Federal Information and Information Systems and NIST Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations), in a manner consistent with the Risk Management Framework (NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy). NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information and Information Systems, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of NIST SP 800-53 Revision 5.

NPR 2810.1, Security of Information Technology, designates this handbook as a guide of NASA's Audit and Accountability (AU) information security controls. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [AU-1](#).

This handbook supports implementation of requirements in NPR 2810.1, Security of Information Technology (IT) and NPD 2810.1E, NASA Information Security Policy. It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organization-defined values are integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS).

1.1. Purpose

The Audit and Accountability control family relates to the documentation and management of events that occur on or to information system components. Generally, the controls help to answer the questions of "who," "what," "where," "when," and sometimes "how" revolving around various types of information system activities and events (i.e., who logged into a given machine, when, and from where, etc.). Such audit trails are used for individual accountability, intrusion detection, and problem identification. Audit details are stored in logs which are used to produce useful, actionable information by applying data analysis techniques to detect anomalous trends and patterns that may be cause for concern. The logs can be used both retroactively to determine the causes of an adverse event, and proactively to detect and take action to avert an imminent adverse event.

1.2. Scope

The provisions of this Handbook apply to all systems owned and operated by NASA. Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. Portions of NASA handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, such as a NASA Policy Directive or NASA Procedural Requirement.

This Handbook and the policy/procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4. Applicability

This handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

1.5. Applicable Documents

1.5.1. Federal Information Processing Standards (FIPS)

- [FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*](#)
- [FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#)

1.5.2. National Institute of Standards and Technology (NIST)

- [NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)
- [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)
- [NIST SP 800-92, *Guide to Computer Security Log Management*](#)

1.5.3. National Aeronautics and Space Administration (NASA)

- [NPD 2810.1, *NASA Information Security Policy*](#)
- [NPR 1441.1, *NASA Records Management Program Requirements*](#)
- [NPR 2810.1, *Security of Information and Information Systems*](#)
- [NASA-SPEC-2661.ODVr5, *NASA's Organization-Defined Values for NIST SP 800-53 Revision 5*](#)

1.5.4. Cancellations, Updates, Consolidations

- ITS-HBK 2810.16-01, Audit and Accountability

2. SECURITY CONTROLS

2.1. Audit Events (**AU-2**)

2.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure the capability to audit the auditable events detailed in [NASA-SPEC-2661.ODVr5](#).
- Ensure the capability to automatically report audit information.

2.1.2. Information System Security Officer (ISSO)

The ISSO shall:

- Identify those auditable events which may best inform after-the-fact investigative efforts.
- Establish the frequency of auditing for the system.
- Adjust as necessary, the frequency of audit activities.
- Document rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.

2.2. Content of Audit Records ([AU-3](#))

2.2.1. Information System Security Officer (ISSO)

The ISSO shall:

- Ensure that system audit records provide sufficient information to understand the details of recorded events.
- Information should include:
 - Date and time of occurrence;
 - Affected system component;
 - Type of event;
 - Affected user(s); and
 - Outcome.

2.3. Audit Storage Capacity ([AU-4](#))

2.3.1. Information System Owner (ISO)

The ISO shall:

- Allocate audit record storage capacity for an information system in accordance with Agency records retention requirements.

2.4. Response to Audit Processing Failures ([AU-5](#))

2.4.1. Information System Security Officer (ISSO)

The ISSO shall:

- Work with the ISO to determine and implement additional actions to be taken in the event of an audit logging

process failure.

2.5. Audit Review, Analysis, and Reporting (AU-6)

2.5.1. Information System Owner (ISO)

The ISO shall:

- Ensure the review of audit records for unusual or suspicious activity in a manner consistent with organization-defined values.
 - Reviews should include system logs of activities of users with respect to the enforcement of information system access controls.
- Ensure the frequency and level of detail of reviews reflects the risk associated with the information system.
- Report unusual or suspicious activities or violations as security incidents to the Security Operations Center (SOC).

2.6. Audit Reduction and Report Generation (AU-7)

2.6.1. Information System Owner (ISO)

The ISO shall:

- Review and analyze information system audit records at least once every 30 days for indications of inappropriate or unusual activity; and
- Report findings to the ISO, CISO, ISSO and/or SOC as appropriate.

2.7. Time Stamps (AU-8)

2.7.1. Information System Owner (ISO)

The ISO shall:

- Ensure that the capability exists to automatically synchronize the internal clocks of information system components in a manner consistent with organization-defined values.

2.8. Protection of Audit Information (AU-9)

2.8.1. Senior Agency Information Security Officer (SAISO)

The SAISO shall:

- Ensure the availability of an Agency-wide repository for auditable event information.
- Ensure the provision of sufficient resources for Agency-wide audit record management.

2.8.2. Information System Owner (ISO)

The ISO shall:

- Ensure sufficient storage capacity resources for the archival of audit records.
- Ensure the protection of audit information and audit logging tools from unauthorized access, modification and deletion and notify the Center CISO and SAISO upon detection of unauthorized access, modification or deletion of audit information.

2.9. Non-Repudiation ([AU-10](#))

2.9.1. Information System Owner (ISO)

The ISO shall:

- Ensure that digital signatures are validated using cryptographic schemes in a manner consistent with organization-defined values.

2.10. Audit Record Retention ([AU-11](#))

2.10.1. Information System Owner (ISO)

The ISO shall:

- Ensure the archival of audit records in a manner consistent with organization-defined values and [NPR 1441.1](#).

2.11. Audit Generation ([AU-12](#))

2.11.1. Information System Owner (ISO)

The ISO shall:

- Ensure the capability to generate audits for information system components in a manner consistent with organization-defined values.

APPENDIX A: ACRONYMS

CISO	Center Chief Information Security Officer
CSPD	Cybersecurity and Privacy Division
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HBK	Handbook
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
NASA	National Aeronautics and Space Administration

NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
RISCS	Risk Information Security Compliance System
SACL	System Access Control List
SAISO	Senior Agency Information Security Officer
SOC	Security Operations Center
SP	Special Publication
XML	Extensible Markup Language