NIST Special Publication
NIST SP 800-92r1 ipd

Cybersecurity Log Management Planning Guide

Initial Public Draft

Karen Scarfone
Murugiah Souppaya

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-92r1.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-92r1 ipd

Cybersecurity Log Management Planning Guide

Initial Public Draft

Karen Scarfone
Scarfone Cybersecurity

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-92r1.ipd

October 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:

Scarfone KA, Souppaya MP (2023) Cybersecurity Log Management Planning Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-92r1 ipd.
https://doi.org/10.6028/NIST.SP.800-92r1.ipd

Author ORCID iDs

Karen Scarfone: 0000-0001-6334-9486
Murugiah Souppaya: 0000-0002-8055-8527

Public Comment Period
October 11, 2023 – November 29, 2023

Submit Comments
log-mgmt@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

A log is a record of events that occur within an organization's computing assets, including physical and virtual platforms, networks, services, and cloud environments. Log management is the process for generating, transmitting, storing, accessing, and disposing of log data. It facilitates log usage and analysis for many purposes, including identifying and investigating cybersecurity incidents, finding operational issues, and ensuring that records are stored for the required period of time. This document defines a playbook intended to help any organization plan improvements to its cybersecurity log management.

Keywords

auditing; cybersecurity artifacts; incident response; log management; logging; threat detection.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Audience

This publication has been created for cybersecurity staff and program managers; system, network, and application administrators; incident response teams; and others who perform duties related to cybersecurity log management. Its content is intended to be relevant to any organization. Certain portions of the document are specific to federal agencies.

Acknowledgments

The authors thank everyone who has contributed to this publication or the original NIST SP 800-92.

Note to Reviewers

NIST welcomes public comments on any aspect of this publication, including the following questions asked on behalf of the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA):

1. This revision is informed by NIST SP 800-207 and the NCCoE's Zero Trust Architecture project calling out data analytics for zero trust purposes. Should the scope of this publication be expanded to directly support and map to zero trust?
2. Should this publication be expanded to include log management implementation guidance?
3. Are there additional considerations for different types of log sources that should be included in this publication (e.g., on-premises, cloud, managed services, or hybrid)?
4. Should the standardization of log management planning to facilitate the sharing of cyber threats or incidents be included?
5. Should guidance on how to determine the purposefulness of logging categories and types be included?
6. Should guidance for determining storage retention periods be included?
7. Should this publication address how new technologies may change log management planning (e.g., blockchains, zero trust, generative AI, quantum computing)?
8. Should this publication address how and which major triggers may necessitate reviewing or changing log management plans?
9. Should this publication address storage costs and offer guidance on prioritizations and trade-offs for cost-effective log management planning?

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: log-mgmt@nist.gov

Table of Contents

Executive Summary

A *log* is a record of the events that occur within an organization's computing assets, including physical and virtual platforms, networks, services, and cloud environments. *Log management* is the process for generating, transmitting, storing, accessing, and disposing of log data. It facilitates log usage and analysis for many purposes, including identifying and investigating cybersecurity incidents, finding operational issues, and ensuring that records are stored for the required period of time. Logging and log management practices are part of many cybersecurity and privacy-related laws and regulations. They are also an important part of numerous standards, guidance, and other sets of recommendations for every sector.

The purpose of this document is to help all organizations improve their log management so that they have the log data they need. This document's scope is organization-wide cybersecurity log management planning; all other aspects of logging and log management are out of scope. The document defines a playbook for cybersecurity log management planning with actionable steps that organizations can take for planning improvements to their log management practices. While the plays in the playbook are not comprehensive, they are noteworthy and generally beneficial to organizations. The plays intentionally avoid any recommendations on the details of log management. Log management needs are incredibly variable from one organization to another and frequently change.

This playbook can help organizations identify and prioritize their needs and determine how to best meet those needs. There is no "correct" way for an organization to use the playbook. An organization may choose to use it as the start of its own new playbook for log management planning, integrate it with an existing log management playbook, or use its information as reference material when considering its plans, policies, and processes.

1. Introduction

A *log* is a record of the events that occur within an organization's computing assets, including physical and virtual platforms, networks, services, and cloud environments. Logs are composed of log entries, and each *entry* contains information related to a specific *event*, which is an observable occurrence in a computing asset. Logs serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing useful data for investigating malicious activity. Many logs contain records that are relevant for cybersecurity, such as operating system logs that capture system events and audit records, application logs that capture application operational and security events, and cybersecurity software logs that record routine events, adverse events, and possible malicious activity.

Log management is the process for generating, transmitting, storing, accessing, and disposing of log data. It facilitates an organization's log usage and analysis. Log management can benefit an organization in many ways. For example, it helps ensure that records are stored in sufficient detail for an appropriate period of time. The continuous monitoring and analysis of logs are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing useful information for resolving such problems. Logs can also be useful for performing auditing and forensic analysis, supporting the organization's internal investigations, establishing baselines, verifying that assets operate as intended, and identifying operational trends and long-term problems.

Logging and log management practices are part of many cybersecurity and privacy-related laws, regulations, standards, guidance, and recommendations for every sector.

1.1. Purpose and Scope

The purpose of this document is to help all organizations improve their log management so that they have the log data they need. The document's scope is cybersecurity log management **planning**. All other aspects of logging and log management, including implementing log management technology and making use of log data, are out of scope. The log plan is informed by the activities that will leverage the logs to inform security and operational decisions.

This document replaces the original NIST Special Publication (SP) 800-92 [SP800-92], which was released in 2006. That material was developed at a time when many organizations were just starting to think about log management. With the wealth of information now available on log management, this revision of NIST SP 800-92 focuses on high-level guidance for organization-wide improvement, not the details of implementation nor the capabilities of particular technologies.

The main content of this publication is a playbook for cybersecurity log management planning. The playbook provides actionable steps that organizations can take to plan improvements to their log management practices in support of recommended practices and regulatory requirements. The playbook contains four high-level plays, each of which is a practice that involves two or more tasks (or other lower-level plays). The playbook and the plays are not comprehensive, but the listed plays are noteworthy and generally beneficial to organizations. Section 2 provides additional information on how to make use of the playbook and plays.

1.2. Note for Federal Agencies

This document does not introduce any new requirements for federal agencies. Federal agencies seeking the latest requirements should consult Office of Management and Budget (OMB) Memoranda, including M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* [OMB21-31], and M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* [OMB22-09].

The guidance in this document helps inform and is informed by several other NIST publications and projects, including:

- NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* [SP800-53r5], particularly the Audit and Accountability (AU) family of security controls
- NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* [SP800-61r2], in terms of generating logs that are subsequently used to find and investigate cybersecurity incidents
- NIST SP 800-207, *Zero Trust Architecture* [SP800-207] and the NCCoE's Zero Trust Architecture project, from the perspective of supporting data analytics for zero trust purposes
- NIST SP 800-218, *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities* [SP800-218] and the NCCoE's Software Supply Chain and DevOps Security Practices project, especially in terms of generating and storing artifacts from secure software development practices
- *Cybersecurity Framework*, particularly within the Protect and Detect Functions

1.3. Publication Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 discusses how this publication could be used.
- Section 3 specifies plays for characterizing the current state of cybersecurity logging by updating several logging-related inventories.
- Section 4 contains plays for defining the target state for an organization's cybersecurity logging.
- Section 5 defines plays for assessing and documenting gaps between the current state and target state, as well as the root causes of those gaps.
- Section 6 provides plays for developing a plan to fill the gaps.
- The References section lists all references used throughout the document.
- Appendix A contains a glossary of key terms.
- Appendix B provides a crosswalk between the log management planning plays and selected NIST guidance documents and frameworks.

257 • Appendix C provides the change log for this document.

2. How to Use This Publication

Sections 3 through 6 of this publication define the following high-level plays, as well as their component tasks and plays:

- **INV, Update Logging-Related Inventories** (Section 3): Characterize the current state of your organization's cybersecurity logging.
- **TS, Define Target State** (Section 4): Define the target state for your organization's cybersecurity logging.
- **GRC, Document Gaps and Their Root Causes** (Section 5): Document the gaps between the current cybersecurity logging state and the target state, and identify the root causes of each gap.
- **PMG, Develop a Plan to Mitigate the Gaps** (Section 6): Develop a plan for addressing the root causes of the identified gaps in order to reach the target state.

There is no "correct" way to use the playbook. An organization may choose to use it as the start of its own new playbook for log management planning, integrate it with an existing log management playbook, or use its information as reference material when considering its own plans, policies, and processes.

Each play includes the following components:

- **Unique ID number** (for example, INV-5)
- **Title** (for example, Update the Work Role Inventory)
- **Summary**, to include the play's desired outcome
- **Tasks to perform**. Each task is briefly stated and has a unique identifier based on its play's ID. Tasks that need a more detailed explanation are either defined as separate plays or have additional explanatory text following them under the label **supporting information for tasks**. Each list of tasks is assumed to typically be performed sequentially unless otherwise noted by the phrase "not necessarily in order."

Some plays also include **examples related to the play**, such as possible roles and responsibilities, use cases, or sources of requirements.

In addition to the plays themselves, Appendix B contains **crosswalks** that indicate how performing each play and its tasks can most significantly help an organization achieve recommended outcomes, controls, and other concepts from a variety of NIST resources.

The plays and tasks are intentionally focused on important actions to perform for planning and, thus, avoid any recommendations on the details of log management. Log management needs are incredibly variable from one organization to another and frequently change, so this playbook avoids specifying who is responsible for planning or performing any of the plays or tasks. Rather, this playbook helps organizations identify and prioritize their needs and determine how to best meet those needs.

3. INV, Update Logging-Related Inventories

[Tasks] [Next Play]

Summary: Characterize the current state of your organization's cybersecurity logging through a set of inventories. This is not an assessment, only information gathering. The desired outcome is a reasonably comprehensive, up-to-date snapshot of the people, processes, and technologies that are involved with cybersecurity logging.

Tasks to perform include the following (not necessarily in order):

1. INV-1, Update the Inventory of Log Source Types
2. INV-2, Update the Logging Infrastructure Inventory
3. INV-3, Update the Logging Use Case Inventory
4. INV-4, Update the Requirements Inventory
5. INV-5, Update the Work Role Inventory

Supporting information for tasks: There are interdependencies between these tasks, so changes to one inventory may necessitate changes to other inventories.

3.1. INV-1, Update the Inventory of Log Source Types

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Update the inventory of your organization's types of log sources. A *log source* is a computing asset (e.g., operating system, application, cloud-based service, container) that is capable of generating cybersecurity log entries. The desired outcome is a reasonably comprehensive, up-to-date picture of all of the types of cybersecurity log data currently available to your organization.

Tasks to perform include the following (not necessarily in order):

1. **INV-1.1:** Determine which characteristics to record in the inventory for each log source type. Basic configuration information is generally the minimum to collect. Examples of additional details include copies of logging procedures and other documentation and the identities of each log source within each log source type (essentially, a log source inventory).
2. **INV-1.2:** Update the inventory to reflect standard configurations for logging and which types of assets use each standard configuration.
3. **INV-1.3:** Update the inventory to reflect exceptions to standard configurations for logging, the nature of each exception, and which types of assets employ each exception.
4. **INV-1.4:** Update the inventory to reflect all other types of assets not included in #2 or #3 with representative samples of their logging configurations.

Examples of log source types include:

- Networks, including network infrastructure devices and the traffic they carry
- Software (e.g., firmware, operating systems, and applications)

- Cloud environments, including virtualization and container technologies
- Technology management solutions (e.g., asset management, configuration management, mobile device management, patch management, vulnerability management)
- Identity, authentication, and authorization technologies
- Threat detection/prevention technologies (e.g., anti-malware, data loss prevention, email filtering)

3.2. INV-2, Update the Logging Infrastructure Inventory

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Update the inventory of your organization's cybersecurity logging infrastructure components. The *logging infrastructure* encompasses the hardware, software, systems, services, and networks used to transmit, store, analyze, and dispose of log data generated by the log sources. The desired outcome is a comprehensive, up-to-date picture of all of the logging infrastructure components that are currently part of your organization.

Tasks to perform include the following:

1. **INV-2.1:** Update the inventory so that it reflects the current set of logging infrastructure components.
2. **INV-2.2:** Update the characteristics recorded for each component in the inventory.
3. **INV-2.3:** Update the logging infrastructure architecture diagrams and other documentation to reflect the updates from INV-2.1 and INV-2.2.

Examples of logging infrastructure components include:

- Centralized systems that perform security information and event monitoring (SIEM) and provide bulk storage and other analytical workflows or services
- Cold data storage
- Cyber threat intelligence feeds from third-party services
- Data lakes that act as centrally accessible log storage with log sources that provide data to the data lake and log analysis technologies that receive log data from the data lake instead of or in addition to the log sources that directly provide data to each log analysis technology
- Domain Name System (DNS) logging system
- Managed services for log monitoring and analysis
- Security orchestration, automation, and response (SOAR) implementation
- User behavior monitoring and analytics

3.3. INV-3, Update the Logging Use Case Inventory

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Update the organization's inventory of logging use cases and the desired outcomes of each use case. This information is valuable when developing or updating logging policies. One desired outcome is that all logging is done for a purpose and not just for the sake of collecting log data. Another desired outcome is that all logging use cases are taken into consideration when defining the target state for cybersecurity log management.

Tasks to perform include the following:

1. **INV-3.1:** Document summaries of the known logging use cases and the desired outcome of each.
2. **INV-3.2:** Share the use cases with stakeholders, solicit their feedback, and make revisions if needed.

Examples of possible use cases include:

- Continuous monitoring
- Early detection of malicious behavior, potentially malicious behavior, and advanced threats that involve all user and non-user accounts
- Evidence of compliance with a standard/compliance reporting
- Evidence of verification of the functional and security operations of the components
- Incident response
- Passive DNS request analysis
- Security operations
- SIEM tools
- Software development artifact capture, for continuous integration/continuous delivery (CI/CD)
- Threat detection and investigation, including threat hunting
- Zero trust implementation

3.4. INV-4, Update the Requirements Inventory

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Update the inventory of existing requirements that are applicable to your organization's cybersecurity logging. Requirements may come from applicable laws, regulations, standards, and internal policies. The desired outcome is a reasonably comprehensive set of current requirements for your organization's cybersecurity logging.

Tasks to perform include the following (not necessarily in order):

1. **INV-4.1:** Confirm that all requirements already in the inventory are still applicable, and remove outdated requirements.
2. **INV-4.2:** Identify all new requirements applicable to existing log source types or logging use cases.

3. **INV-4.3:** Identify all requirements applicable to new log source types or new logging use cases.

Examples of sources of requirements include:

- General laws and regulations (e.g., GDPR)
- Sector-specific laws and regulations (e.g., HIPAA, NERC)
- Federal agency-specific requirements (e.g., OMB memoranda; FISMA/NIST Risk Management Framework; EO 14028, Section 8 [EO14028])
- Standards that the organization chooses to follow (e.g., ISO 27001)
- The organization's cybersecurity, privacy, and data retention policies
- Requirements and policies of a parent organization/enterprise

3.5. INV-5, Update the Work Role Inventory

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Update the inventory of cybersecurity logging-related work roles that your personnel or third parties perform. Each work role includes one or more tasks, and each task is associated with one or more knowledge and skill statements, as defined in NIST SP 800-181 [SP800-181r1]. There are two desired outcomes: to confirm that all necessary work roles and tasks are assigned and to inform the organization's training and process documentation planning.

Tasks to perform include the following (not necessarily in order):

1. **INV-5.1:** Confirm that all roles already in the inventory are still applicable.
2. **INV-5.2:** Identify any new roles, and add them to the inventory.
3. **INV-5.3:** Update which tasks are associated with each role.
4. **INV-5.4:** Update which knowledge and skill statements are associated with each task.
5. **INV-5.5:** Share the updated work role inventory with stakeholders, solicit their feedback, and make revisions if needed.
6. **INV-5.6:** Disseminate the updated work role inventory information to affected parties.

Examples of parties within an organization who may have log management responsibilities include the following. Note that many of these responsibilities may also be performed by third parties, such as managed security service providers and cloud service providers, for some of the organization's assets.

- **System and network administrators** who
  - Configure logging and synchronize timestamps on individual systems and network devices
  - Configure systems and devices to forward log data to the appropriate logging infrastructure systems for analysis, storage, or other processing
  - Report on the results of log management activities

    - Perform regular maintenance of the logs and logging software
    - Handle authorized requests from security administrators, auditors, compliance officers, legal counsel, and others who need copies of log data
- **Security administrators** who
    - Manage, secure, and monitor log management infrastructures
    - Implement, secure, manage, and maintain a passive DNS logging system
    - Configure logging and synchronize timestamps on security devices and services (e.g., firewalls, antivirus servers, VPNs, SASE)
    - Configure security devices and services to forward log data to the appropriate logging infrastructure systems for analysis, storage, or other processing
    - Identify the changes needed to system logging configurations (e.g., which entries and data fields must be sent to the centralized log servers) and inform system-level administrators of the necessary changes
    - Report on the results of log management activities
    - Assist others with configuring logging and performing log analysis
    - Test and implement upgrades and updates to the log management infrastructure's components
- **Operations personnel** who
    - Archive log data to removable media and dispose of that log data properly once it is no longer needed
    - Monitor logging configurations and operational statuses for individual systems, networks, and the log management infrastructure to identify logging failures (e.g., a failure of a log management infrastructure component) and potentially unauthorized changes
    - Initiate appropriate responses to events, including incident handling and operational problems
- **Computer security incident response teams** who use log data when investigating and handling incidents
- **Application developers** whose applications perform logging
- **Information security officers** who oversee the log management infrastructures
- **Chief information officers (CIOs)** who oversee the technology resources that generate, transmit, and store the logs
- **Auditors** who use log data when performing audits
- **Compliance officers** who use log data when verifying compliance or documenting evidence of compliance
- Individuals involved in the **procurement of software or software services** that can or should generate cybersecurity log data

4. TS, Define Target State

[Tasks] [Previous Play] [Next Play]

Summary: Define the target state for your organization's cybersecurity logging. The *target state* is a combination of (mandatory) requirements from all applicable laws, regulations, standards, and internal policies and (desired) goals and objectives for log management based on balancing the organization's reduction of risk and the need for logging resilience with the time and resources needed to perform log management functions. The desired outcome is an integrated set of prioritized requirements, goals, and objectives for your organization's cybersecurity logging. This set should be updated periodically and as major changes occur, like the impending implementation of a new law or regulation, the introduction of new technology, or the observation of new threats.

Tasks to perform include the following (not necessarily in order):

1. TS-1, Forecast Future Changes to Logging Inventories
2. TS-2, Define Target State for Log Generation
3. TS-3, Define Target State for Log Storage and Transfer
4. TS-4, Define Target State for Log Access
5. TS-5, Define Target State for Log Disposal

Supporting information for tasks: There are interdependencies between these tasks. For example, generating a higher volume of logs may necessitate increasing resources for log storage. Conversely, a firm limit on log storage resources may necessitate generating less log data, being more selective about which generated log data is stored, or reducing how long some log data is stored.

4.1. TS-1, Forecast Future Changes to Logging Inventories

[Tasks] [Examples] [Previous Play] [Next Play]

Summary: Forecast future changes to the organization's logging inventories (e.g., log source types, infrastructure, use cases, requirements, and work roles), and consider their potential effects on each other and the organization's logging practices. This includes known changes and educated guesses about future changes. The desired outcome is a set of prioritized future changes that inform the target states for the organization's logging.

Tasks to perform include the following (not necessarily in order):

1. **TS-1.1:** Forecast future changes to log source types.
2. **TS-1.2:** Forecast future changes to the logging infrastructure.
3. **TS-1.3:** Forecast future changes to logging use cases.
4. **TS-1.4:** Forecast future changes to requirements.
5. **TS-1.5:** Forecast future changes to work roles.

Supporting information for the tasks: There are interdependencies between these tasks. Future changes identified by one task may necessitate other types of changes.

Examples of possible changes include:

1. **TS-1.1 examples:** Adding a new type of computing device or application to the organization; upgrading an application to a version with much more detailed log generation capabilities
2. **TS-1.2 examples:** Migrating log storage from on-premises to cloud-based; adding a new log analysis technology; improving logging infrastructure resilience
3. **TS-1.3 example:** Identifying and implementing a new use case; a passive DNS logging system
4. **TS-1.4 example:** Complying with a new law going into effect next year that requires a longer data retention period
5. **TS-1.5 example:** Transitioning some logging responsibilities to a parent organization or a managed security service provider (MSSP)

4.2. TS-2, Define Target State for Log Generation

[Tasks] [Previous Play] [Next Play]

Summary: Define the log generation-related requirements and goals for each of your organization's cybersecurity log source types. The desired outcome is a comprehensive set of prioritized requirements and goals for cybersecurity log generation that help define your organization's target state.

Tasks to perform include the following (not necessarily in order):

1. **TS-2.1:** For each type of log source, determine whether it should be required, recommended, not recommended, or prohibited.
2. **TS-2.2:** Determine which types of events each log source should or must log and which types of events each log source should not or must not log.
3. **TS-2.3:** Determine which data characteristics should or must be logged for each type of event, including the log source identity and other metadata, and which types of data characteristics should not or must not be logged.
4. **TS-2.4:** Determine whether the log source might intentionally or inadvertently capture sensitive data, including personal information, passwords, private keys, and access tokens.
5. **TS-2.5:** Determine how frequently each type of event should or must be logged.
6. **TS-2.6:** Determine how to handle log generation errors.
7. **TS-2.7:** Determine when logs should or must record cleartext data instead of or in addition to encrypted data.
8. **TS-2.8:** Determine how clock synchronization should or must be performed for all log sources.
9. **TS-2.9:** Determine what timestamp formats should or must be used for all log sources, as well as supporting information to be captured (e.g., time zones).

10. **TS-2.10:** Determine how log generation should or must be protected.
11. **TS-2.11:** Define how the protection of log generation should or must be monitored and validated to ensure that logging is enabled and functioning normally.

Supporting information for tasks: Recording more log data is not necessarily better. Generally, organizations should only require logging the necessary data and also have recommendations for which other types and sources of data should be logged if resources permit. Some organizations choose to have all or nearly all log data generated and stored for at least a short period of time in case it is needed; this approach favors security considerations over usability and resource usage.

When establishing requirements and recommendations, organizations should be flexible since each host is different and will log different amounts of data than other hosts. The logging behavior of a host may also change rapidly due to an upgrade, patch, or configuration change.

Organizations may permit administrators to temporarily reconfigure log sources during adverse conditions, such as unsuccessful malware attacks that cause the same type of log entry to be generated many times. These configuration changes should be performed as a last resort and be as precise as possible. Log source administrators should inform logging infrastructure administrators of such configuration changes to ensure that log management processes are modified if needed.

In some cases, software licenses may need to be upgraded in order to generate the required or desired information for logs.

For more information on log generation in the context of incident response, see NIST SP 800-61, Rev. 2, *Computer Security Incident Handling Guide* [SP800-61r2].

4.3. TS-3, Define Target State for Log Storage and Transfer

[Tasks] [Previous Play] [Next Play]

Summary: Define your organization's log storage and transfer-related requirements and goals. This should take log source types, log event types, system locations, and any other pertinent attributes into account. The desired outcome is a comprehensive set of prioritized requirements and goals for cybersecurity log storage and transfer that help define your organization's target state.

Tasks to perform include the following (not necessarily in order):

1. **TS-3.1:** Determine how long each log event should or must be preserved at the log source.
2. **TS-3.2:** Determine which events, if any, should or must be transferred to a log infrastructure from log sources, which log infrastructure systems should receive the transferred event data, and which data characteristics should or must be transferred for each event. This may necessitate estimating network bandwidth needs for log transfers.
3. **TS-3.3:** Determine how event correlation across log sources should or must be performed within the log infrastructure.

4. **TS-3.4:** Determine how log data should or must be transferred to the log infrastructure, including out-of-band methods where appropriate, and how frequently log data should or must be transferred.
5. **TS-3.5:** Determine how the confidentiality, integrity, and availability of each log event should or must be protected while in storage at the log source, while in the log infrastructure, while being transferred from the log source to the log infrastructure, and while being transferred from one log infrastructure component to another.
6. **TS-3.6:** Determine how much log storage space should or must be available at the log sources and the log infrastructure.
7. **TS-3.7:** Determine how to handle log storage and log transfer errors at the log sources and the log infrastructure.
8. **TS-3.8:** Determine if and when each type of log event should or must be transferred from active storage to cold data storage for data retention purposes.
9. **TS-3.9:** Determine which log format/type to use (if this is an option).
10. **TS-3.10:** Determine how the protection of log storage and transfers should or must be monitored and validated to ensure their confidentiality, integrity, and availability.

Supporting information for tasks: Completing these tasks effectively designs the high-level architecture of the log infrastructure, such as the logical and physical locations of centralized log data storage and various log analysis services. When most organizations only had one or a few closely related logging use cases, a centralized logging server or group of servers could often handle all of an organization's logging infrastructure needs. Now, organizations often have several diverse logging use cases and magnitudes more data to process and store, so more complex logging architectures have become commonplace. For example, some organizations use a massive data lake to hold all of their security log data instead of a centralized log management and analysis service. Each logging use case probably has one or more different tools that consume log data, and these tools can retrieve data from the data lake instead of having to interact with all of the log sources. This can be much more efficient in terms of time, network bandwidth, and especially storage.

Another consideration when performing these tasks is the possibility of another entity, such as a parent organization or an outsourcer, taking care of some or all of your centralized log storage needs in the future. Log storage needs are highly variable over time, although they generally continue to increase. Cloud-based log storage can provide rapid scalability that on-premises log storage often cannot.

Organizations will also need to determine whether their original logs need to be preserved for a certain period of time or if preserving log data copied to a centralized log server or storage is acceptable. In many environments, original logs only need to be preserved if they may be needed as evidence.

4.4. TS-4, Define Target State for Log Access

[Tasks] [Previous Play] [Next Play]

Summary: Define your organization's log access-related requirements and goals. This should take the access needs of auditors, law enforcement, courts, and other government agencies into account. The desired outcome is a comprehensive set of prioritized requirements and goals for cybersecurity log access that help define your organization's target state.

Tasks to perform include the following (not necessarily in order):

1. **TS-4.1:** Identify the access-related policy requirements for log sources and transferred logs for each type of log event.
    a. **TS-4.1a:** Determine who/what should or must be able to locally and remotely access log data.
    b. **TS-4.1b:** Determine who/what should or must be able to directly access logs versus indirectly access logs (e.g., through a SIEM, through a read-only interface).
    c. **TS-4.1c:** Determine how local and remote access to log data itself should or must be logged.
    d. **TS-4.1d:** Determine how local and remote access to log data should or must be protected (e.g., encryption).
2. **TS-4.2:** Determine how log preservation orders, such as a legal requirement to protect and prevent the alteration and destruction of particular log records, must be handled from a technical standpoint.
3. **TS-4.3:** Determine how inadvertent and intentional disclosures of sensitive information recorded in logs must be handled.
4. **TS-4.4:** Determine how the protection of log access should or must be monitored and validated to ensure that only authorized parties can access the appropriate logs.

4.5. TS-5, Define Target State for Log Disposal

[Tasks] [Previous Play] [Next Play]

Summary: Define your organization's log disposal-related requirements and goals. The desired outcome is a comprehensive set of prioritized requirements and goals for cybersecurity log disposal that help define your organization's target state.

Tasks to perform include the following (not necessarily in order):

1. **TS-5.1:** Identify the disposal-related policy requirements for each type of log event at the log source level. Determine how and when each type of log event should or must be disposed of.
2. **TS-5.2:** Identify the disposal-related policy requirements for each type of log event at the log infrastructure level. Determine how and when each type of log event should or must be disposed of.

3. **TS-5.3:** Define requirements for monitoring, validating, and testing the safeguarding of log disposal (to avoid unauthorized destruction of logs).

5. GRC, Document Gaps and Their Root Causes

[Tasks] [Previous Play] [Next Play]

Summary: Document the implementation gaps between the current cybersecurity logging state and the target state, and identify the root causes of each gap. The desired outcome is a list of implementation gaps with an assessment of the relative risk posed by each gap and the root causes of each gap.

Tasks to perform include the following:

1. GRC-1, Scope and Plan the Assessment
2. GRC-2, Conduct the Assessment and Document Findings

Supporting information for tasks: Root cause analysis should go beyond superficial observations and determine the underlying factors. For example, suppose that one log source is generating a much lower volume of log data than other similar log sources. Assessment indicates that this is primarily due to logging configuration errors. Root cause analysis should not stop there; it should determine why this log source is misconfigured (e.g., poor enforcement of requirements, an approved exception to policy that needs to be reassessed, human error, possible compromise of the log source, lack of log storage space).

5.1. GRC-1, Scope and Plan the Assessment

[Tasks] [Previous Play] [Next Play]

Summary: Scope the gap analysis, and determine how the gap analysis will be performed. The desired outcome is an assessment plan.

Tasks to perform include the following (not necessarily in order):

1. **GRC-1.1:** Determine how comprehensive the gap analysis should be. For example, the gap analysis could include all of the most critical systems, all security configuration baselines, and a sampling of non-baselined logging sources that includes representatives of all identified logging use cases.
2. **GRC-1.2:** Plan the assessment (e.g., utilizing automation, conducting interviews, performing manual reviews of certain components).

5.2. GRC-2, Conduct the Assessment and Document Findings

[Tasks] [Previous Play] [Next Play]

Summary: Execute the assessment plan for identifying gaps and their root causes. The desired outcome is a stakeholder-reviewed list of findings.

Tasks to perform include the following (not necessarily in order):

1. **GRC-2.1:** Conduct the assessment: document all gaps from the target state, characterize each gap and assess its risk, identify the root causes of each gap, and estimate the relative importance of each root cause in regards to all the gaps and the magnitude of the cost of addressing it.

2. **GRC-2.2:** Summarize the findings, get stakeholder feedback, and make revisions as needed.

6. PMG, Develop a Plan to Mitigate the Gaps

[Tasks] [Previous Play] [Next Play]

Summary: Develop a plan for addressing the root causes of the identified gaps in order to reach the target state. The project plan takes the relative importance of each gap, the resources needed to address each root cause, and the dependencies among items (e.g., expanding centralized log storage capacity before significantly increasing the volume of logs being sent to that storage) into account. The desired outcome is a project plan that, when executed, has addressed the root causes and filled the identified gaps.

Tasks to perform include the following (with the first two not necessarily in order):

1. PMG-1, Draft the Plan
2. PMG-2, Revise Affected Policies
3. PMG-3, Address Feedback on Draft Plan and Policies

6.1. PMG-1, Draft the Plan

[Tasks] [Previous Play] [Next Play]

Summary: Draft the plan for addressing the root causes of identified gaps. The desired outcome is a project plan draft that is ready for stakeholder review and feedback.

Tasks to perform include the following (not necessarily in order):

1. **PMG-1.1:** Identify any changes to logging-related inventories (e.g., log source types, infrastructure, use cases, requirements, and work roles).
2. **PMG-1.2:** Develop cost estimates for the resources needed to address the gaps for people, processes, and technology, including both one-time and ongoing costs. This may include adding tools and technologies to automate aspects of log management, adjusting technical configuration baselines and guidance, updating affected procedures and processes, retraining staff with log management-related responsibilities, and establishing a logging test environment.
3. **PMG-1.3:** Include provisions in the plan for creating a plan of action and milestones and using compensating controls until gaps are remediated.
4. **PMG-1.4:** Incorporate the timing of other projects that may affect logging (e.g., the pending replacement of a major enterprise application).
5. **PMG-1.5:** Include information on how often the plan itself will be reviewed and updated, such as a scheduled annual review, audit results that indicate a significant problem, the announcement of new legal or regulatory requirements, and feedback from logging infrastructure and system administrators on logging requirements.
6. **PMG-1.6:** Ensure that all elements of the plan are harmonized.

6.2. PMG-2, Revise Affected Policies

[Tasks] [Previous Play] [Next Play]

Summary: Revise the organization's policies to support the draft project plan. The desired outcome is a set of draft revised policies that are ready for stakeholder review and feedback.

Tasks to perform include the following:

1. **PMG-2.1:** Identify which policies may be affected by the draft project plan. This may include policies for software procurement, custom software development, and other topics where cybersecurity logging capabilities are a vital part but not the focus.
2. **PMG-2.2:** Revise the affected policies so that they incorporate the organization's updated set of requirements, goals, and objectives.
3. **PMG-2.3:** Ensure that changes to all affected policies are harmonized.

Supporting information for tasks: It may be appropriate to specify future effective dates for certain policy changes, depending on the timeframes for the corresponding items in the draft project plan.

6.3. PMG-3, Address Feedback on Draft Plan and Policies

[Tasks] [Previous Play]

Summary: Address stakeholder feedback on the draft plan and policies. The desired outcome is a final project plan and policy set.

Tasks to perform include the following:

1. **PMG-3.1:** Identify all stakeholders who should be invited to provide feedback on the draft plan and/or policies. It may be particularly important to get feedback from the following:
    - Legal counsel to ensure that the plan will adequately address all legal, regulatory, compliance, and other requirements and that the logging itself is performed in compliance with privacy laws
    - System administrators and others who will be altering log generation, storage, transfer, access, and disposal practices to ensure that the changes are feasible and will not cause unexpected problems (e.g., a legacy system being configured to log every auditable event could generate an enormous number of log entries, impact the host's performance, and cause log entries to be overwritten too quickly)
    - Any parent or child organizations (subsidiaries, etc.)
2. **PMG-3.2:** Share the draft plan and policies with stakeholders, and encourage them to provide feedback within a particular timeframe.
3. **PMG-3.3:** Review and adjudicate the feedback. Consider the point of view of each stakeholder and the effect that addressing each comment may have on other parts of the draft plan and policies.

4. **PMG-3.4:** Revise the draft plan and policies to address the feedback based on the adjudications. This includes harmonizing changes throughout the documents.
    - If stakeholder feedback results in significant changes to the draft plan or policies, this play may need to be repeated so that affected stakeholders can provide feedback on the changes.
    - If stakeholder feedback is not needed, the revised plan and policies should be finalized and communicated to all affected parties.

Supporting information for tasks: It may be appropriate to specify future effective dates for certain policy changes, depending on the timeframes for the corresponding items in the draft project plan.

References

[CSF11] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[EO14028] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-202100401, May 12, 2021. Available at https://www.govinfo.gov/app/details/DCPD-202100401

[NIST-CRSW] National Institute of Standards and Technology (2021) Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028. (National Institute of Standards and Technology, Gaithersburg, MD), July 9, 2021. Available at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2

[OMB21-31] Office of Management and Budget (2021) Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents. (The White House, Washington, DC), OMB Memorandum M-21-31, August 27, 2021. Available at https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[OMB22-09] Office of Management and Budget (2022) Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. (The White House, Washington, DC), OMB Memorandum M-22-09, January 26, 2022. Available at https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[SP800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-61, Rev. 2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP800-92] Kent K, Souppaya MP (2006) Guide to Computer Security Log Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-92. https://doi.org/10.6028/NIST.SP.800-92

[SP800-181r1] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[SP800-207] Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-207. https://doi.org/10.6028/NIST.SP.800-207

[SP800-218] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

Appendix A. Glossary

active storage
Data that is stored in a manner that facilitates frequent use and ease of access. ([OMB21-31], adapted)

cold data storage
Data that is stored in a manner that minimizes costs while still allowing some level of access and use. ([OMB21-31], adapted)

Note: The original NIST SP 800-92 [SP800-92] used the term "log archival" instead of "cold data storage."

event aggregation
The consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event. [SP800-92]

event correlation
Finding relationships between two or more log entries. [SP800-92]

event forwarding
Obtaining events from logging sources in near real-time on an automated basis, and storing them centrally. ([OMB21-31], adapted)

log
A record of events occurring within an organization's computing assets, including physical and virtual platforms, networks, services, and cloud environments. ([SP800-92], adapted)

log access
Reading log entries.

log analysis
Studying log entries to identify events of interest or suppress log entries for insignificant events. [SP800-92]

log clearing
Removing all entries from a log that precede a certain date and time. [SP800-92]

log destruction
Deleting a log or a log's entries in such a way that the deleted log data cannot be recovered.

log entry
An individual record within a log of an event that has occurred within a system or network. ([EO14028], adapted)

log generation
Creating new log entries.

log management
The process for generating, transmitting, storing, accessing, and disposing of log data. ([SP800-92], adapted)

log management infrastructure
The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. [SP800-92]

log normalization
Converting each log data field to a particular data representation and categorizing it consistently. [SP800-92]

log preservation
Keeping logs that normally would be discarded because they contain records of activity of particular interest. [SP800-92]

log reduction
Removing unneeded entries from a log to create a new log that is smaller. [SP800-92]

log retention
Archiving logs on a regular basis as part of standard operational activities. [SP800-92]

log rotation
Closing a log file and opening a new log file when the first log file is considered to be complete. [SP800-92]

log storage
Retaining log entries for a period of time.

log transfer
Copying log entries from one logical asset to another.

Appendix B. Crosswalk to NIST Guidance and Frameworks

This appendix provides a crosswalk between each log management planning play and selected NIST guidance documents and frameworks.

Play	**NIST SP 800-53, Rev. 5** [SP800-53r5]	**CSF 1.1** [CSF11]	**EO 14028 Security Measures** [NIST-CRSW]
INV-1, Update the Inventory of Log Source Types	AU-2, AU-12, CM-2, CM-6, CM-8	ID.AM-2, ID.AM-4	SM 1.3, SM 2.1, SM 3.1, SM 3.3
INV-2, Update the Logging Infrastructure Inventory	CM-8	ID.AM-1, ID.AM-2, ID.AM-4	SM 2.1, SM 3.1
INV-3, Update the Logging Use Case Inventory	AU-1	ID.GV-1	SM 1.3
INV-4, Update the Requirements Inventory	AU-1, AU-2	ID.GV-3	N/A
INV-5, Update the Work Role Inventory	AU-1	ID.AM-6	SM 5.1, SM 5.2
TS-1, Forecast Future Changes to Logging Inventories	AU-1	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	SM 4.1
TS-2, Define Target State for Log Generation	AU-1	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	SM 4.1
TS-3, Define Target State for Log Storage and Transfer	AU-1	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	SM 4.1
TS-4, Define Target State for Log Access	AU-1	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	SM 4.1
TS-5, Define Target State for Log Disposal	AU-1	ID.GV-1, ID.GV-2, ID.GV-3, ID.GV-4	SM 4.1
GRC-1, Scope and Plan the Assessment	RA-1	ID.RM-1	SM 4.1
GRC-2, Conduct the Assessment and Document Findings	RA-3	ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5	SM 4.1
PMG-1, Draft the Plan	AU-1, RA-7	ID.RA-6	SM 4.1
PMG-2, Revise Affected Policies	AU-1	ID.GV-1, ID.GV-4	SM 4.1
PMG-3, Address Feedback on Draft Plan and Policies	AU-1, RA-7	ID.GV-1, ID.GV-4, ID.RA-6	SM 4.1

Appendix C. Change Log

In October 2023, the following changes were made to this report:

- Performed a full rewrite and reorganization of the previous content to improve clarity and usability and to remove outdated content
- Reformatted all content to follow the latest NIST technical publication template