



**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 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

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

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

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

14 **Authority**

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

21
22 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding
23 on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be
24 interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or
25 any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and
26 is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

27 **NIST Technical Series Policies**

28 [Copyright, Use, and Licensing Statements](#)
29 [NIST Technical Series Publication Identifier Syntax](#)

30 **How to Cite this NIST Technical Series Publication:**

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

34 **Author ORCID iDs**

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

37 **Public Comment Period**
38 October 11, 2023 – November 29, 2023

39 **Submit Comments**
40 log-mgmt@nist.gov
41
42 National Institute of Standards and Technology
43 Attn: Applied Cybersecurity Division, Information Technology Laboratory
44 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

45 **All comments are subject to release under the Freedom of Information Act (FOIA).**
46

47 **Abstract**

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

55 **Keywords**

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

57 **Reports on Computer Systems Technology**

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

68 **Audience**

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

73 **Acknowledgments**

74 The authors thank everyone who has contributed to this publication or the original NIST SP 800-
75 92.

76 **Note to Reviewers**

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

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

98 **Trademark Information**

99 All names are registered trademarks or trademarks of their respective companies.

100 **Call for Patent Claims**

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

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

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

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

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

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

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

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

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

126	Table of Contents	
127	Executive Summary	1
128	1. Introduction	2
129	1.1. Purpose and Scope	2
130	1.2. Requirements for Federal Agencies	3
131	1.3. Publication Structure	3
132	2. How to Use This Publication	5
133	3. INV, Update Logging-Related Inventories	6
134	3.1. INV-1, Update the Inventory of Log Source Types.....	6
135	3.2. INV-2, Update the Logging Infrastructure Inventory.....	7
136	3.3. INV-3, Update the Logging Use Case Inventory	7
137	3.4. INV-4, Update the Requirements Inventory	8
138	3.5. INV-5, Update the Work Role Inventory	9
139	4. TS, Define Target State	11
140	4.1. TS-1, Forecast Future Changes to Logging Inventories	11
141	4.2. TS-2, Define Target State for Log Generation	12
142	4.3. TS-3, Define Target State for Log Storage and Transfer	13
143	4.4. TS-4, Define Target State for Log Access.....	15
144	4.5. TS-5, Define Target State for Log Disposal	15
145	5. GRC, Document Gaps and Their Root Causes	17
146	5.1. GRC-1, Scope and Plan the Assessment	17
147	5.2. GRC-2, Conduct the Assessment and Document Findings	17
148	6. PMG, Develop a Plan to Mitigate the Gaps	19
149	6.1. PMG-1, Draft the Plan	19
150	6.2. PMG-2, Revise Affected Policies	20
151	6.3. PMG-3, Address Feedback on Draft Plan and Policies.....	20
152	References	22
153	Appendix A. Glossary	24
154	Appendix B. Crosswalk to NIST Guidance and Frameworks	26
155	Appendix C. Change Log	27

156

157 **Executive Summary**

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

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

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

180 **1. Introduction**

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

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

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

202 **1.1. Purpose and Scope**

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

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

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

221 1.2. Note for Federal Agencies

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

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

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

243 1.3. Publication Structure

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

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

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

258 2. How to Use This Publication

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

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

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

274 Each play includes the following components:

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

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

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

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

294 3. INV, Update Logging-Related Inventories

295 [\[Tasks\]](#)

[\[Next Play\]](#)

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

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

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

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

308 3.1. INV-1, Update the Inventory of Log Source Types

309 [\[Tasks\]](#) [\[Examples\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

327 **Examples** of log source types include:

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

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

336 **3.2. INV-2, Update the Logging Infrastructure Inventory**

337 [\[Tasks\]](#) [\[Examples\]](#) [\[Previous Play\]](#) [\[Next Play\]](#)

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

343 **Tasks to perform** include the following:

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

349 **Examples** of logging infrastructure components include:

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

362 **3.3. INV-3, Update the Logging Use Case Inventory**

363 [\[Tasks\]](#) [\[Examples\]](#) [\[Previous Play\]](#) [\[Next Play\]](#)

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

369 **Tasks to perform** include the following:

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

374 **Examples** of possible use cases include:

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

388 **3.4. INV-4, Update the Requirements Inventory**

389 [[Tasks](#)] [[Examples](#)] [[Previous Play](#)] [[Next Play](#)]

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

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

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

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

401 **Examples** of sources of requirements include:

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

409 **3.5. INV-5, Update the Work Role Inventory**

410 [[Tasks](#)] [[Examples](#)] [[Previous Play](#)] [[Next Play](#)]

411 **Summary:** Update the inventory of cybersecurity logging-related work roles that your personnel
412 or third parties perform. Each work role includes one or more tasks, and each task is associated
413 with one or more knowledge and skill statements, as defined in NIST SP 800-181 [SP800-
414 181r1]. There are two desired outcomes: to confirm that all necessary work roles and tasks are
415 assigned and to inform the organization’s training and process documentation planning.

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

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

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

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

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

471 4. TS, Define Target State

472 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

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

493 4.1. TS-1, Forecast Future Changes to Logging Inventories

494 [\[Tasks\]](#) [\[Examples\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

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

508 **Examples** of possible changes include:

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

520 **4.2. TS-2, Define Target State for Log Generation**

521 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

545 10. **TS-2.10:** Determine how log generation should or must be protected.

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

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

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

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

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

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

566 4.3. **TS-3, Define Target State for Log Storage and Transfer**

567 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

574 1. **TS-3.1:** Determine how long each log event should or must be preserved at the log
575 source.

576 2. **TS-3.2:** Determine which events, if any, should or must be transferred to a log
577 infrastructure from log sources, which log infrastructure systems should receive the
578 transferred event data, and which data characteristics should or must be transferred for
579 each event. This may necessitate estimating network bandwidth needs for log transfers.

580 3. **TS-3.3:** Determine how event correlation across log sources should or must be performed
581 within the log infrastructure.

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

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

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

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

619 **4.4. TS-4, Define Target State for Log Access**

620 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

644 **4.5. TS-5, Define Target State for Log Disposal**

645 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

- 656 3. **TS-5.3:** Define requirements for monitoring, validating, and testing the safeguarding of
657 log disposal (to avoid unauthorized destruction of logs).
658

659 **5. GRC, Document Gaps and Their Root Causes**

660 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

665 **Tasks to perform** include the following:

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

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

675 **5.1. GRC-1, Scope and Plan the Assessment**

676 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

686 **5.2. GRC-2, Conduct the Assessment and Document Findings**

687 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

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

697 **6. PMG, Develop a Plan to Mitigate the Gaps**

698 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

709 **6.1. PMG-1, Draft the Plan**

710 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

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

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

731 **6.2. PMG-2, Revise Affected Policies**

732 [\[Tasks\]](#)

[\[Previous Play\]](#) [\[Next Play\]](#)

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

735 **Tasks to perform** include the following:

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

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

745 **6.3. PMG-3, Address Feedback on Draft Plan and Policies**

746 [\[Tasks\]](#)

[\[Previous Play\]](#)

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

749 **Tasks to perform** include the following:

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

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

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

777 **References**

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

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

786 [NIST-CRSW] National Institute of Standards and Technology (2021) Security Measures
787 for “EO-Critical Software” Use Under Executive Order (EO) 14028.
788 (National Institute of Standards and Technology, Gaithersburg, MD), July
789 9, 2021. Available at [https://www.nist.gov/itl/executive-order-improving-
790 nations-cybersecurity/security-measures-eo-critical-software-use-2](https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2)

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

798 [OMB22-09] Office of Management and Budget (2022) Moving the U.S. Government
799 Toward Zero Trust Cybersecurity Principles. (The White House,
800 Washington, DC), OMB Memorandum M-22-09, January 26, 2022.
801 Available at [https://www.whitehouse.gov/wp-content/uploads/2022/01/M-
802 22-09.pdf](https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)

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

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

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

816 [SP800-181r1] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2020)
817 Workforce Framework for Cybersecurity (NICE Framework). (National
818 Institute of Standards and Technology, Gaithersburg, MD), NIST Special
819 Publication (SP) 800-181, Rev. 1. [https://doi.org/10.6028/NIST.SP.800-
820 181r1](https://doi.org/10.6028/NIST.SP.800-181r1)

- 821 [SP800-207] Rose SW, Borchert O, Mitchell S, Connelly S (2020) Zero Trust
822 Architecture. (National Institute of Standards and Technology,
823 Gaithersburg, MD), NIST Special Publication (SP) 800-207.
824 <https://doi.org/10.6028/NIST.SP.800-207>
- 825 [SP800-218] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software
826 Development Framework (SSDF) Version 1.1: Recommendations for
827 Mitigating the Risk of Software Vulnerabilities. (National Institute of
828 Standards and Technology, Gaithersburg, MD), NIST Special Publication
829 (SP) 800-218. <https://doi.org/10.6028/NIST.SP.800-218>

830 **Appendix A. Glossary**

831 **active storage**

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

833 **cold data storage**

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

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

837 **event aggregation**

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

840 **event correlation**

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

842 **event forwarding**

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

845 **log**

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

848 **log access**

849 Reading log entries.

850 **log analysis**

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

852 **log clearing**

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

854 **log destruction**

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

856 **log entry**

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

858 **log generation**

859 Creating new log entries.

860 **log management**

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

862 **log management infrastructure**

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

865 **log normalization**

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

867 **log preservation**

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

870 **log reduction**

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

872 **log retention**

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

874 **log rotation**

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

876 **log storage**

877 Retaining log entries for a period of time.

878 **log transfer**

879 Copying log entries from one logical asset to another.

880 **Appendix B. Crosswalk to NIST Guidance and Frameworks**

881 This appendix provides a crosswalk between each log management planning play and selected
882 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

883 **Appendix C. Change Log**

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

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