



NIST Special Publication 800
NIST SP 800-172Ar3 ipd

Assessing Enhanced Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd>

NIST Special Publication 800
NIST SP 800-172Ar3 ipd

Assessing Enhanced Security Requirements for Controlled Unclassified Information

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd>

September 2025



U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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 [1]. 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 [2].

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:

Ross R, Pillitteri V (2025) Assessing Enhanced Security Requirements for Controlled Unclassified Information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-172Ar3 ipd. <https://doi.org/10.6028/NIST.SP.800-172Ar3.ipd>

Author ORCID iDs

Ron Ross: 0000-0002-1099-9757

Victoria Pillitteri: 0000-0002-7446-7506

Public Comment Period

September 29, 2025 – November 14, 2025

Submit Comments

800-171comments@list.nist.gov

National Institute of Standards and Technology

Attn: Computer Security Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments submitted during the public comment period will be posted to the NIST Protecting Controlled Unclassified Information Project page. with contact information redacted. All technical content will be posted as submitted, so commenters should not include information they do not wish to be posted (e.g., personal or business information).

Additional information about this publication is available at <https://csrc.nist.gov/pubs/sp/800/172/A/r3/ipd>, including related content, potential updates, and document history.

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

1 **Abstract**

2 The protection of controlled unclassified information (CUI) resident in nonfederal systems and
3 organizations is of paramount importance to federal agencies and can directly impact the ability
4 of the Federal Government to successfully conduct its essential missions and functions. This
5 publication provides federal agencies with assessment procedures for the security
6 requirements in NIST SP 800-172. The assessment procedures are flexible and can be tailored to
7 the needs of federal agencies and assessors. Security requirement assessments can be
8 conducted as (1) self-assessments; (2) independent, third-party assessments; or (3)
9 government-sponsored assessments. The assessments can be conducted with varying degrees
10 of rigor based on federal agency-defined depth and coverage attributes. The findings and
11 evidence produced during the assessments can be used to facilitate risk-based decisions by
12 organizations related to the security requirements.

13 **Keywords**

14 assessment; assessment procedure; assurance; enhanced security requirement; enhanced
15 security requirement assessment; controlled unclassified information; Executive Order 13556;
16 nonfederal organization; nonfederal system; security assessment.

17 **Reports on Computer Systems Technology**

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

28 **Audience**

29 This publication serves a diverse group of individuals and organizations in the public and private
30 sectors, including individuals with:

- 31 • System development life cycle responsibilities (e.g., program managers,
32 mission/business owners, information owners/stewards, system designers and
33 developers, system/security engineers, systems integrators)
- 34 • Acquisition or procurement responsibilities (e.g., contracting officers)
- 35 • System, security, or risk management and oversight responsibilities (e.g., authorizing
36 officials, chief information officers, chief information security officers, system owners,
37 information security managers)
- 38 • Security assessment and monitoring responsibilities (e.g., auditors, system evaluators,
39 assessors, independent verifiers/validators, analysts)

40 The above roles and responsibilities can be viewed from two perspectives:

- 41 • *Federal perspective*: The entity establishing and conveying security assessment
42 requirements in contractual vehicles or other types of agreements
- 43 • *Nonfederal perspective*: The entity responding to and complying with the security
44 assessment requirements set forth in contracts or agreements

45 **Note to Reviewers**

46 The following significant changes have been made in the initial public draft (ipd) of SP 800-
47 172Ar3 (Revision 3):

- 48 • The restructuring of the assessment procedure syntax to align with SP 800-53A [5]
- 49 • The addition of assessment procedures for the new and revised enhanced security
50 requirements in draft SP 800-172r3 [3]
- 51 • The addition of a references section to provide source assessment procedures from SP
52 800-53A [5]
- 53 • A one-time change to the publication version number to align with SP 800-172, Revision
54 3 [3]

55 NIST is specifically interested in comments, feedback, and recommendations on the following
56 topics:

- 57 • The alignment of the assessment procedures to SP 800-53A [5]
- 58 • The ease-of-use of the assessment procedures in conducting assessments of the CUI
59 enhanced security requirements
- 60 • The usefulness of the information in supplementary Appendices C, D, and E

61 Reviewers are encouraged to comment on all or parts of SP 800-172Ar3 ipd. NIST requests that
62 all comments be submitted to 800-171comments@list.nist.gov by 11:59 p.m. Eastern Standard
63 Time (EST) on November 14, 2025. Commenters are encouraged to use the comment template
64 provided with the document announcement.

65 Comments received in response to this request will be posted on the Protecting CUI [project site](#)
66 after the due date. Submitters' names and affiliations (when provided) will be included, while
67 contact information will be removed.

68 **Call for Patent Claims**

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

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

- 78 a) assurance in the form of a general disclaimer to the effect that such party does not hold
79 and does not currently intend holding any essential patent claim(s); or
- 80 b) assurance that a license to such essential patent claim(s) will be made available to
81 applicants desiring to utilize the license for the purpose of complying with the guidance
82 or requirements in this ITL draft publication either:
- 83 i. under reasonable terms and conditions that are demonstrably free of any unfair
84 discrimination; or
- 85 ii. without compensation and under reasonable terms and conditions that are
86 demonstrably free of any unfair discrimination.

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

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

94 Such statements should be addressed to: 800-171comments@list.nist.gov

95	Table of Contents	
96	1. Introduction	1
97	1.1. Purpose and Applicability.....	1
98	1.2. Organization of This Publication	1
99	2. The Fundamentals	3
100	2.1. Assessment Procedures	3
101	2.2. Assurance Cases	5
102	3. The Procedures	7
103	3.1. Access Control.....	7
104	3.2. Awareness and Training.....	18
105	3.3. Audit and Accountability.....	21
106	3.4. Configuration Management.....	24
107	3.5. Identification and Authentication	30
108	3.6. Incident Response	36
109	3.7. Maintenance	39
110	3.8. Media Protection	40
111	3.9. Personnel Security	43
112	3.10. Physical Protection.....	45
113	3.11. Risk Assessment	47
114	3.12. Security Assessment and Monitoring	54
115	3.13. System and Communications Protection.....	57
116	3.14. System and Information Integrity	69
117	3.15. Planning.....	83
118	3.16. System and Services Acquisition	85
119	3.17. Supply Chain Risk Management.....	86
120	References	92
121	Appendix A. Acronyms	93
122	Appendix B. Glossary	94
123	Appendix C. Summary of Enhanced Security Requirements	96
124	Appendix D. Security Requirement Assessments	100
125	Appendix E. Organization-Defined Parameters	104
126	Appendix F. Change Log	112

127 **List of Tables**

128 **Table 1. Enhanced security requirement families3**

129 **Table 2. Enhanced security requirements.....96**

130 **Table 3. Summary of assessment preparation phase101**

131 **Table 4. Summary of assessment plan development phase102**

132 **Table 5. Summary of assessment execution phase103**

133 **Table 6. Summary of assessment analysis, documentation, and reporting phase103**

134 **Table 7. Organization-defined parameters104**

135

136 **Acknowledgments**

137 The authors gratefully acknowledge and appreciate the contributions from individuals and
138 organizations in the public and private sectors whose constructive comments improved the
139 overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank
140 the NIST technical editing and production staff — Jim Foti, Jeff Brewer, Eduardo Takamura,
141 Jeremy Licata, Isabel Van Wyk, and Cristina Ritfeld — for their outstanding support in preparing
142 this document for publication.

143 **1. Introduction**

144 The security assessment process gathers information and produces evidence to determine the
145 effectiveness of security requirements by:

- 146 • Identifying potential problems or shortfalls in security and risk management programs
- 147 • Identifying security weaknesses and deficiencies in systems and the environments in
148 which those systems operate
- 149 • Prioritizing risk mitigation decisions and activities
- 150 • Confirming that identified security weaknesses and deficiencies in the system and
151 environment of operation have been addressed
- 152 • Supporting continuous monitoring activities and providing information security
153 situational awareness

154 **1.1. Purpose and Applicability**

155 The purpose of this publication is to provide procedures for assessing the security requirements
156 in NIST Special Publication (SP) 800-172, *Enhanced Security Requirements for Protecting*
157 *Controlled Unclassified Information* [3]. Organizations can use the assessment procedures to
158 generate evidence that the security requirements have been satisfied. The scope of the security
159 assessments conducted using the procedures described in this publication is guided and
160 informed by the system security plans for systems that process, store, or transmit CUI. The
161 assessment procedures offer the flexibility to customize assessments based on organizational
162 policies and requirements, known threat and vulnerability information, system and platform
163 dependencies, operational considerations, and tolerance for risk.¹

164 **1.2. Organization of This Publication**

165 The remainder of this special publication is organized as follows:

- 166 • Section 2 describes the fundamental concepts associated with assessments of security
167 requirements, including assessment procedures, methods, objects, and assurance cases
168 that can be created using the evidence produced during assessments. This section
169 mirrors the material included SP 800-171A, Sec. 2, with minor updates to reflect the
170 enhanced security requirements and assessment procedures.
- 171 • Section 3 provides assessment procedures for the security requirements in SP 800-172
172 [3], including assessment objectives and potential assessment methods and objects for
173 each procedure.

174

¹ The term *risk* refers to risks to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation. See SP 800-39 [4] for additional information on organizational risk management and risk tolerance.

175 The following sections provide additional information to support the assessment of security
176 requirements for the protection of CUI:

- 177 • References
- 178 • Appendix A: Acronyms
- 179 • Appendix B: Glossary
- 180 • Appendix C: Summary of Enhanced Security Requirements
- 181 • Appendix D: Security Requirement Assessments
- 182 • Appendix E: Organization-Defined Parameters
- 183 • Appendix F: Change Log

The contents of this publication can be used for many different assessment-related purposes to determine organizational compliance with the security requirements. The broad range of potential assessment methods and objects listed in this publication does not necessarily reflect and should not be directly associated with actual compliance or noncompliance. Rather, the selection of specific potential assessment methods and objects from the list provided can help generate a picture of overall compliance with the security requirements. There is no expectation about the number of methods or objects needed to determine compliance with the security requirements. Moreover, the entire list of potential assessment objects should not be viewed as required artifacts needed to determine compliance. Organizations have the flexibility to determine the specific methods and objects that provide sufficient evidence to support claims of compliance.

184

185 **2. The Fundamentals**

186 The process used by organizations and assessors to assess the security requirements in SP 800-
187 172 [3] includes (1) preparing for the assessment, (2) developing a security assessment plan, (3)
188 conducting the assessment, and (4) documenting, analyzing, and reporting the assessment
189 results. The remainder of this section describes the structure and content of the procedures
190 used to assess the security requirements and the importance of assurance cases in providing
191 the evidence necessary to determine compliance with the requirements.

192 **2.1. Assessment Procedures**

193 The enhanced security requirements in SP 800-172 [3] are organized into 17 families, as
194 illustrated in Table 1.

195 **Table 1. Enhanced security requirement families**

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response		Supply Chain Risk Management

196 The assessment procedures in Sec. 3 are grouped by similar family designations to ensure the
197 completeness and consistency of assessments. The procedures have been derived from and are
198 sourced to the assessment procedures in SP 800-53A [5].

199 An assessment procedure consists of an assessment *objective* and a set of potential
200 assessment methods and objects that can be used to conduct the assessment. Each potential
201 assessment objective includes a determination statement related to the security requirement.
202 If there is an organization-defined parameter (ODP) in the security requirement, then the
203 assessment objective begins with a determination statement related to the definition of the
204 ODP. The determination statements are linked to the content of the security requirements to
205 help ensure traceability of the assessment results to the requirements.

206 Assessment objects identify the specific items being assessed and can include specifications,
207 mechanisms, activities, and individuals. Specifications are the documented artifacts² (e.g.,
208 plans, policies, procedures, requirements, functional and assurance specifications, design
209 documentation, architectures) associated with a system. Mechanisms are the hardware,
210 software, and firmware safeguards implemented within a system. Activities are the protection-
211 related actions supporting a system that involve people (e.g., conducting system backup

² Artifacts may be in formats other than documents (e.g., databases; Governance, Risk, and Compliance [GRC] tools; Open Security Controls Assessment Language [OSCAL]).

212 operations, exercising an incident response plan, monitoring network traffic). Individuals are
213 the people applying the specifications, mechanisms, or activities described above.

214 Assessment methods define the nature and extent of the assessor's actions and are used to
215 facilitate understanding, achieve clarification, or obtain evidence. The assessment methods
216 include *examine*, *interview*, and *test*. The examine method is the process of reviewing, studying,
217 inspecting, or analyzing assessment objects. The interview method is the process of holding
218 discussions with individuals or groups about assessment objects. The test method is the process
219 of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to
220 compare actual with expected behavior. Assessment methods include attributes of *depth* and
221 *coverage*, which define the rigor, scope, and level of effort for the assessment as well as the
222 degree of assurance that the security requirements have been satisfied. See SP 800-53A,
223 Appendix D [5].

224 The structure and content of an assessment procedure are provided in the example below.

225 **03.01.01E Dual Authorization**

Security Requirement Name

226 **ASSESSMENT OBJECTIVE**

227 *Determine if:*

Determination Statement for Security Requirement

228 **A.03.01.01E.ODP[01]: *privileged commands and/or other actions requiring dual***
229 ***authorization are defined.***

230 **A.03.01.01E:** dual authorization is enforced for **<A.03.01.01E.ODP[01]: *privileged***
231 ***commands and/or other actions*>.**

232 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

233 **Examine**

234 [SELECT FROM: Access control policy; procedures addressing access enforcement
235 and dual authorization; system design documentation; system configuration settings
236 and associated documentation; list of actions requiring dual authorization; list of
237 privileged commands requiring dual authorization; list of approved authorizations
238 (user privileges); system security plan; other relevant documents or records].

239 **Interview**

240 [SELECT FROM: Personnel with access enforcement responsibilities; system/network
241 administrators; system personnel with information security responsibilities].

242 **Test**

243 [SELECT FROM: Dual authorization mechanisms implementing access control policy].

244 **REFERENCES**

245 Source Assessment Procedures: [AC-03\(02\)](#)

246 Determination statements have alphanumeric identifiers. Each determination statement begins
247 with the letter “A” to indicate that it is part of an assessment procedure. The next sequence of
248 numbers followed by the letter “E” indicates the enhanced security requirement identifier from
249 SP 800-172 [3] (and the specific control item if it is a multi-part requirement) that is the target
250 of the assessment. Organization-defined parameters are indicated by the letters “ODP.” If there
251 are multiple ODPs in the determination statement, the ODP number is indicated in a square
252 bracket (e.g., [A.03.01.04E.ODP\[01\]](#)). Square brackets are also used to denote when an
253 assessment procedure further decomposes a requirement into more granular determination
254 statements (e.g., [A.03.10.03E.a\[01\]](#), [A.03.10.03E.a\[02\]](#), [A.03.10.03E.a\[03\]](#), [A.03.10.03E.a\[04\]](#)).

255 The application of an assessment procedure to a security requirement produces assessment
256 results or *findings*. The findings are compiled and used as evidence to determine whether the
257 security requirement has been *satisfied* or *other than satisfied*. A finding of satisfied indicates
258 that the assessment objective has been met, producing a fully acceptable result. A finding of
259 other than satisfied indicates that there are potential anomalies that may need to be addressed
260 by the organization. A finding of other than satisfied may also indicate that the assessor was
261 unable to obtain sufficient information to make the specific determination called for in the
262 determination statement.

263 2.2. Assurance Cases

264 Building an effective assurance case to determine compliance with security requirements
265 involves compiling evidence from a variety of sources and conducting different types of
266 activities during an assessment. An *assurance case* is a body of evidence organized into an
267 argument demonstrating that some claim about a system is true. For security assessments
268 conducted using the procedures in this publication, that claim is “compliance” with the security
269 requirements in SP 800-172 [3]. Assessors obtain evidence during security assessments to allow
270 designated officials³ to make objective determinations about compliance with the security
271 requirements. The evidence needed to make such determinations can be obtained from various
272 sources, including independent, third-party assessments or other types of assessments,
273 depending on the needs of the organization establishing the requirements and the organization
274 conducting the assessments.

275 For example, many technical security requirements are satisfied by security capabilities that are
276 built into commercial information technology products and systems. Product assessments are
277 typically conducted by independent, third-party testing organizations.⁴ These assessments
278 examine the security functions of products and established configuration settings. Assessments
279 can also be conducted to demonstrate compliance with industry, national, or international
280 security standards as well as developer and vendor claims. Since many information technology
281 products are assessed by commercial testing organizations and then subsequently deployed in

³ A *designated official* is either internal or external to a nonfederal organization and has the responsibility to determine organizational compliance with the security requirements.

⁴ Examples of third-party testing organizations include Common Criteria Testing Laboratories that evaluate IT products in accordance with ISO/IEC 15408 [6] and Cryptographic Module Validation Program Testing Laboratories that evaluate cryptographic modules in accordance with Federal Information Processing Standards (FIPS) 140 [7].

282 hundreds of thousands of systems, these types of assessments can be carried out at a greater
283 level of depth and provide deeper insights into the security capabilities of the products.

284 The evidence needed to determine compliance with the security requirements is obtained by
285 assessing the implementation of the safeguards and countermeasures selected to satisfy the
286 requirements. Assessors can build on previously developed materials that started with the
287 specification of the information security needs of the organization and were further improved
288 during the design, development, and implementation of the system. These materials provide
289 the initial evidence for an assurance case.

290 Assessments can be conducted by system developers, system integrators, auditors, system
291 owners, or the security staffs of organizations. The assessors or assessment teams bring
292 available information about the system together, such as the results of component product
293 assessments. The assessors can conduct additional system-level assessments using the
294 assessment methods and procedures contained in this publication and the implementation
295 information provided by the nonfederal organization in its system security plan. Assessments
296 can be used to compile and evaluate the evidence needed by organizations to help determine
297 the effectiveness of the safeguards implemented to protect CUI, the actions needed to mitigate
298 security risks to the organization, and compliance with the security requirements.

The assessment procedures in this publication are based on and sourced to the assessment procedures in SP 800-53A [5]. For additional information and guidance on preparing for security assessments, developing assessment plans, conducting assessments, and analyzing assessment report results, consult SP 800-53A [5].

299

300 3. The Procedures

301 This section provides assessment procedures for the security requirements defined in SP 800-
302 172 [3]. Organizations that conduct security requirement assessments can develop their
303 security assessment plans by using the information provided in the assessment procedures and
304 selecting the specific POTENTIAL ASSESSMENT METHODS AND OBJECTS that meet the
305 organization’s needs. Organizations also have flexibility in defining the level of rigor and detail
306 associated with the assessment based on the assurance requirements of the organization.

307 3.1. [Access Control](#)

308 03.01.01E Dual Authorization

309 ASSESSMENT OBJECTIVE

310 *Determine if:*

311 **A.03.01.01E.ODP[01]: *privileged commands and/or other actions requiring dual***
312 ***authorization are defined.***

313 **A.03.01.01E:** dual authorization is enforced for **<A.03.01.01E.ODP[01]: *privileged***
314 ***commands and/or other actions*>.**

315 POTENTIAL ASSESSMENT METHODS AND OBJECTS

316 **Examine**

317 [SELECT FROM: Access control policy; procedures addressing access enforcement
318 and dual authorization; system design documentation; system configuration settings
319 and associated documentation; list of actions requiring dual authorization; list of
320 privileged commands requiring dual authorization; list of approved authorizations
321 (user privileges); system security plan; other relevant documents or records].

322 **Interview**

323 [SELECT FROM: Personnel with access enforcement responsibilities; system/network
324 administrators; system developers; personnel with information security
325 responsibilities].

326 **Test**

327 [SELECT FROM: Dual authorization mechanisms implementing access control policy].

328 REFERENCES

329 Source Assessment Procedures: [AC-03\(02\)](#)

330 **03.01.02E Non-Organizationally Owned Systems - Restricted Use**

331 **ASSESSMENT OBJECTIVE**

332 *Determine if:*

333 **A.03.01.02E.ODP[01]: *restrictions on the use of non-organizationally owned***
334 ***systems or system components to process, store, or transmit CUI are defined.***

335 **A.03.01.02E:** the use of non-organizationally owned systems or system components
336 to process, store, or transmit CUI is restricted using **<A.03.01.02E.ODP[01]:**
337 ***restrictions*>**.

338 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

339 **Examine**

340 [SELECT FROM: Access control policy; procedures addressing the use of external
341 systems; system design documentation; system configuration settings and
342 associated documentation; system connection or processing agreements; account
343 management documents; system audit records; other relevant documents or
344 records].

345 **Interview**

346 [SELECT FROM: Personnel with responsibilities for restricting or prohibiting the use
347 of non-organizationally owned systems, system components, or devices;
348 system/network administrators; personnel with information security
349 responsibilities].

350 **Test**

351 [SELECT FROM: Mechanisms implementing restrictions on the use of non-
352 organizationally owned systems, components, or devices].

353 **REFERENCES**

354 Source Assessment Procedures: [AC-20\(03\)](#)

355 **03.01.03E Withdrawn**

356 Addressed by 03.01.09E, 03.01.10E, and 03.01.03.

357 **03.01.04E Concurrent Session Control**

358 **ASSESSMENT OBJECTIVE**

359 *Determine if:*

360 **A.03.01.04E.ODP[01]: *accounts and/or account types for which to limit the number***
361 ***of concurrent sessions is defined.***

362 **A.03.01.04E.ODP[02]: the number of concurrent sessions to be allowed for each**
363 **account and/or account type is defined.**

364 **A.03.01.04E:** the number of concurrent sessions for each **<A.03.01.04E.ODP[01]:**
365 **account and/or account types>** is limited to **<A.03.01.04E.ODP[02]: number>**.

366 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

367 **Examine**

368 [SELECT FROM: Access control policy; procedures addressing concurrent session
369 control; system design documentation; system configuration settings and associated
370 documentation; security plan; system security plan; other relevant documents or
371 records].

372 **Interview**

373 [SELECT FROM: System/network administrators; personnel with information security
374 responsibilities; system developers].

375 **Test**

376 [SELECT FROM: Mechanisms implementing access control policy for concurrent
377 session control].

378 **REFERENCES**

379 Source Assessment Procedures: [AC-10](#)

380 **03.01.05E Remote Access Monitoring and Control**

381 **ASSESSMENT OBJECTIVE**

382 *Determine if:*

383 **A.03.01.05E[01]:** automated mechanisms are employed to monitor remote access
384 methods.

385 **A.03.01.05E[02]:** automated mechanisms are employed to control remote access
386 methods.

387 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

388 **Examine**

389 [SELECT FROM: Access control policy; procedures addressing remote access to the
390 system; system design documentation; system configuration settings and associated
391 documentation; system audit records; system monitoring records; system security
392 plan; other relevant documents or records].

393 **Interview**
394 [SELECT FROM: System/network administrators; personnel with information security
395 responsibilities; system developers].

396 **Test**
397 [SELECT FROM: Automated mechanisms monitoring and controlling remote access
398 methods].

399 **REFERENCES**

400 Source Assessment Procedures: [AC-17\(01\)](#)

401 **03.01.06E Protection of Remote Access Mechanism Information**

402 **ASSESSMENT OBJECTIVE**

403 *Determine if:*

404 **A.03.01.06E:** information about remote access mechanisms is protected from
405 unauthorized use and disclosure.

406 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

407 **Examine**

408 [SELECT FROM: Access control policy; procedures addressing remote access to the
409 system; system security plan; other relevant documents or records].

410 **Interview**

411 [SELECT FROM: Personnel with responsibilities for implementing or monitoring
412 remote access to the system; system users with knowledge of information about
413 remote access mechanisms; personnel with information security responsibilities].

414 **REFERENCES**

415 Source Assessment Procedures: [AC-17\(06\)](#)

416 **03.01.07E Automated Audit Actions for Account Management**

417 **ASSESSMENT OBJECTIVE**

418 *Determine if:*

419 **A.03.01.07E[01]:** automated mechanisms are used to audit account creation actions.

420 **A.03.01.07E[02]:** automated mechanisms are used to audit account modification
421 actions.

422 **A.03.01.07E[03]:** automated mechanisms are used to audit account enabling
423 actions.

424 **A.03.01.07E[04]:** automated mechanisms are used to audit account disabling
425 actions.

426 **A.03.01.07E[05]:** automated mechanisms are used to audit account removal actions.

427 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

428 **Examine**

429 [SELECT FROM: Access control policy; procedures addressing account management;
430 system design documentation; system configuration settings and associated
431 documentation; notifications or alerts of account creation, modification, enabling,
432 disabling, and removal actions; system audit records; system security plan; other
433 relevant documents or records].

434 **Interview**

435 [SELECT FROM: Personnel with account management responsibilities;
436 system/network administrators; personnel with information security
437 responsibilities].

438 **Test**

439 [SELECT FROM: Automated mechanisms implementing account management
440 functions].

441 **REFERENCES**

442 Source Assessment Procedures: [AC-02\(04\)](#)

443 **03.01.08E Account Monitoring for Atypical Usage**

444 **ASSESSMENT OBJECTIVE**

445 *Determine if:*

446 **A.03.01.08E.ODP[01]:** *atypical usage for which to monitor system accounts is*
447 *defined.*

448 **A.03.01.08E.ODP[02]:** *personnel or roles to report atypical usage are defined.*

449 **A.03.01.08E.a:** system accounts are monitored for **<A.03.01.08E.ODP[01]: atypical**
450 **usage>.**

451 **A.03.01.08E.b:** atypical usage of system accounts is reported to
452 **<A.03.01.08E.ODP[02]: personnel or roles>.**

453 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

454 **Examine**

455 [SELECT FROM: Access control policy; procedures addressing account management;
456 system design documentation; system configuration settings and associated

457 documentation; system monitoring records; system audit records; audit tracking and
458 monitoring reports; system security plan; other relevant documents or records].

459 **Interview**

460 [SELECT FROM: Personnel with account management responsibilities;
461 system/network administrators; personnel with information security
462 responsibilities].

463 **Test**

464 [SELECT FROM: Mechanisms implementing account management functions].

465 **REFERENCES**

466 Source Assessment Procedure: [AC-02\(12\)](#)

467 **03.01.09E Attribute-Based Access Control**

468 **ASSESSMENT OBJECTIVE**

469 *Determine if:*

470 **A.03.01.09E.ODP[01]: *attributes to assume access permissions are defined.***

471 **A.03.01.09E.a[01]:** the attribute-based access control policy is enforced over defined
472 subjects.

473 **A.03.01.09E.a[02]:** the attribute-based access control policy is enforced over defined
474 objects.

475 **A.03.01.09E.b:** access is controlled based upon **<A.03.01.09E.ODP[01]: *attributes*>**.

476 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

477 **Examine**

478 [SELECT FROM: Access control policy; procedures addressing access enforcement;
479 system design documentation; system configuration settings and associated
480 documentation; list of subjects and objects (i.e., users and resources) requiring
481 enforcement of attribute-based access control policies; system audit records; system
482 security plan; other relevant documents or records].

483 **Interview**

484 [SELECT FROM: Personnel with access enforcement responsibilities; system/network
485 administrators; personnel with information security responsibilities].

486 **Test**

487 [SELECT FROM: Mechanisms implementing access enforcement functions].

488 **REFERENCES**

489 Source Assessment Procedures: [AC-03\(13\)](#)

490 **03.01.10E Object Security Attributes**

491 **ASSESSMENT OBJECTIVE**

492 *Determine if:*

493 **A.03.01.10E.ODP[01]: security attributes to be associated with information, source,**
494 **and destination objects are defined.**

495 **A.03.01.10E.ODP[02]: information objects to be associated with information**
496 **security attributes are defined.**

497 **A.03.01.10E.ODP[03]: source objects to be associated with information security**
498 **attributes are defined.**

499 **A.03.01.10E.ODP[04]: destination objects to be associated with information**
500 **security attributes are defined.**

501 **A.03.01.10E.ODP[05]: information flow control policies as a basis for the**
502 **enforcement of flow control decisions are defined.**

503 **A.03.01.10E: <A.03.01.10E.ODP[01]: security attributes> associated with**
504 **<A.03.01.10E.ODP[02]: information objects>, <A.03.01.10E.ODP[03]: source**
505 **objects>, and <A.03.01.10E.ODP[04]: destination objects> are used to enforce**
506 **<A.03.01.10E.ODP[05]: information flow control policies> as a basis for flow control**
507 **decisions.**

508 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

509 **Examine**

510 [SELECT FROM: Access control policy; information flow control policies; procedures
511 addressing information flow enforcement; system design documentation; system
512 configuration settings and associated documentation; list of security attributes and
513 associated source and destination objects; system audit records; system security
514 plan; other relevant documents or records].

515 **Interview**

516 [SELECT FROM: System/network administrators; personnel with information security
517 responsibilities; system developers].

518 **Test**

519 [SELECT FROM: Mechanisms implementing information flow enforcement policy].

520 **REFERENCES**

521 Source Assessment Procedure: [AC-04\(01\)](#)

522 **03.01.11E Role-Based Access Control**

523 **ASSESSMENT OBJECTIVE**

524 *Determine if:*

525 **A.03.01.11E.ODP[01]: roles and users authorized to assume such roles are defined.**

526 **A.03.01.11E.a:** a role-based access control policy over defined subjects and objects
527 is enforced.

528 **A.03.01.11E.b:** access is controlled based upon **<A.03.01.11E.ODP[01] roles and**
529 **authorized users>.**

530 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

531 **Examine**

532 [SELECT FROM: Access control policy; role-based access control policies; procedures
533 addressing access enforcement; system design documentation; system configuration
534 settings and associated documentation; list of roles, users, and associated privileges
535 required to control system access; system audit records; system security plan; other
536 relevant documents or records].

537 **Interview**

538 [SELECT FROM: Organizational personnel with access enforcement responsibilities;
539 system/network administrators; organizational personnel with information security
540 responsibilities; system developers].

541 **Test**

542 [SELECT FROM: Mechanisms implementing role-based access control policy].

543 **REFERENCES**

544 Source Assessment Procedure: [AC-03\(07\)](#)

545 **03.01.12E Physical or Logical Separation of CUI Flows**

546 **ASSESSMENT OBJECTIVE**

547 *Determine if:*

548 **A.03.01.12E.ODP[01]: mechanisms and/or techniques to separate CUI flows are**
549 **defined.**

550 **A.03.01.12E:** CUI flows are logically or physically separated using
551 **<A.03.01.12E.ODP[01] mechanisms and/or techniques>.**

552 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

553 **Examine**

554 [SELECT FROM: Information flow enforcement policy; information flow control

555 policies; procedures addressing information flow enforcement; system design
556 documentation; system configuration settings and associated documentation; list of
557 required separation of information flows by information types; list of mechanisms
558 and/or techniques used to logically or physically separate information flows; system
559 audit records; system security plan; other relevant documents or records].

560 **Interview**

561 [SELECT FROM: Organizational personnel with information flow enforcement
562 responsibilities; system/network administrators; organizational personnel with
563 information security responsibilities; system developers].

564 **Test**

565 [SELECT FROM: Mechanisms implementing information flow enforcement
566 functions].

567 **REFERENCES**

568 Source Assessment Procedure: [AC-04\(21\)](#)

569 **03.01.13E Metadata**

570 **ASSESSMENT OBJECTIVE**

571 *Determine if:*

572 **A.03.01.13E.ODP[01]: metadata on which to base enforcement of information flow**
573 **control is defined.**

574 **A.03.01.13E:** information flow control based on <**A.03.01.13E.ODP[01]: metadata**>
575 is enforced.

576 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

577 **Examine**

578 [SELECT FROM: Access control policy; information flow control policies; procedures
579 addressing information flow enforcement; system design documentation; system
580 configuration settings and associated documentation; system audit records; system
581 security plan; other relevant documents or records].

582 **Interview**

583 [SELECT FROM: System/network administrators; organizational personnel with
584 information security responsibilities; system developers].

585 **Test**

586 [SELECT FROM: Mechanisms implementing information flow enforcement policy].

587 **REFERENCES**

588 Source Assessment Procedure: [AC-04\(06\)](#)

589 **03.01.14E Security Policy Filters**

590 **ASSESSMENT OBJECTIVE**

591 *Determine if:*

592 **A.03.01.14E.ODP[01]: security policy filters are defined.**

593 **A.03.01.14E.ODP[02]: information flows are defined.**

594 **A.03.01.14E.ODP[03]: one or more of the following PARAMETER VALUES is/are**
595 **selected: {Block; Strip; Modify; Quarantine} in response to a filter processing**
596 **failure.**

597 **A.03.01.14E.ODP[04]: security policy addressing a filter processing failure is**
598 **defined.**

599 **A.03.01.14E.a:** information flow control is enforced using **<A.03.01.14E.ODP[01]**
600 **security policy filters>** as a basis for flow control decisions **for**
601 **<A.03.01.14E.ODP[02] information flows>**.

602 **A.03.01.14E.b:** **<A.03.01.14E.ODP[03]: SELECTED PARAMETER VALUE(S)>** data after
603 **a filter processing failure in accordance with <A.03.01.14E.ODP[04] security policy>**.

604 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

605 **Examine**

606 [SELECT FROM: Access control policy; information flow control policies; procedures
607 addressing information flow enforcement; system design documentation; system
608 configuration settings and associated documentation; list of security policy filters
609 regulating flow control decisions; system audit records; system security plan; other
610 relevant documents or records].

611 **Interview**

612 [SELECT FROM: System/network administrators; organizational personnel with
613 information security responsibilities; system developers].

614 **Test**

615 [SELECT FROM: Mechanisms implementing information flow enforcement policy;
616 security policy filters].

617 **REFERENCES**

618 Source Assessment Procedure: [AC-04\(08\)](#)

619 **03.01.15E Data Type Identifiers**

620 **ASSESSMENT OBJECTIVE**

621 *Determine if:*

622 **A.03.01.15E.ODP[01]: data type identifiers are defined.**

623 **A.03.01.15E:** when transferring information between security domains,
624 **<A.03.01.15E.ODP[01]: data type identifiers>** are used to validate data that is
625 essential for information flow decisions.

626 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

627 **Examine**

628 [SELECT FROM: Access control policy; information flow control policies; procedures
629 addressing information flow enforcement; system design documentation; system
630 configuration settings and associated documentation; list of data type identifiers;
631 system audit records; system security plan; other relevant documents or records].

632 **Interview**

633 [SELECT FROM: System/network administrators; organizational personnel with
634 information security responsibilities; system developers].

635 **Test**

636 [SELECT FROM: Mechanisms implementing information flow enforcement policy].

637 **REFERENCES**

638 Source Assessment Procedure: [AC-04\(12\)](#)

639 **03.01.16E Decomposition Into Policy-Relevant Subcomponents**

640 **ASSESSMENT OBJECTIVE**

641 *Determine if:*

642 **A.03.01.16E.ODP[01]: policy-relevant subcomponents into which to decompose**
643 **CUI for submission to policy enforcement mechanisms are defined.**

644 **A.03.01.16E:** when transferring information between different security domains, CUI
645 is decomposed into **<A.03.01.16E.ODP[01]: policy-relevant subcomponents>** for
646 submission to policy enforcement mechanisms

647 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

648 **Examine**

649 [SELECT FROM: Access control policy; information flow control policies; procedures
650 addressing information flow enforcement; system design documentation; system
651 configuration settings and associated documentation; system audit records; system
652 security plan; other relevant documents or records].

653 **Interview**

654 [SELECT FROM: System/network administrators; personnel with information security
655 responsibilities; system developers].

656 **Test**

657 [SELECT FROM: Mechanisms implementing information flow enforcement policy].

658 **REFERENCES**

659 Source Assessment Procedure: [AC-04\(13\)](#)

660 **03.01.17E Detection of Unsanctioned CUI**

661 **ASSESSMENT OBJECTIVE**

662 *Determine if:*

663 **A.03.01.17E.ODP[01]:** unsanctioned CUI to be detected is defined.

664 **A.03.01.17E.ODP[02]:** a security policy that prohibits the transfer of unsanctioned
665 information is defined.

666 **A.03.01.17E.a:** when transferring information between different security domains,
667 information is examined for the presence of **<A.03.01.17E.ODP[01] unsanctioned
668 information>**.

669 **A.03.01.17E.b:** the transfer of CUI defined in 03.01.17E.a is prohibited in accordance
670 with **<A.03.01.17E.ODP[02] security policy>**.

671 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

672 **Examine**

673 [SELECT FROM: Access control policy; information flow control policies; procedures
674 addressing information flow enforcement; system design documentation; system
675 configuration settings and associated documentation; list of unsanctioned
676 information types and associated information; system audit records; system security
677 plan; other relevant documents or records].

678 **Interview**

679 [SELECT FROM: Organizational personnel with information security responsibilities;
680 system developers].

681 **Test**

682 [SELECT FROM: Mechanisms implementing information flow enforcement policy].

683 **REFERENCES**

684 Source Assessment Procedure: [AC-04\(15\)](#)

685 **3.2. [Awareness and Training](#)**

686 **03.02.01E Advanced Literacy and Awareness Training**

687 **ASSESSMENT OBJECTIVE**

- 688 *Determine if:*
- 689 **A.03.02.01E.ODP[01]: indicators of malicious code are defined.**
- 690 **A.03.02.01E.ODP[02]: the frequency at which to update security literacy training**
691 **content is defined.**
- 692 **A.03.02.01E.ODP[03]: events which cause security literacy training content to be**
693 **updated are defined.**
- 694 **A.03.02.01E.a.01:** security literacy training on the advanced persistent threat is
695 provided.
- 696 **A.03.02.01E.a.02:** security literacy training on recognizing suspicious
697 communications and anomalous behavior in systems using **<A.03.02.01E.ODP[01]:**
698 **indicators of malicious code>** is provided.
- 699 **A.03.02.01E.a.03:** security literacy training on the cyber threat environment is
700 provided.
- 701 **A.03.02.01E.b:** security literacy training content is updated **<A.03.02.01E.ODP[02]:**
702 **frequency>** and following **<A.03.02.01E.ODP[03]: events>**.

703 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

704 **Examine**

705 [SELECT FROM: System security plan; security literacy and awareness training policy;
706 procedures addressing security literacy and awareness training implementation;
707 security literacy and awareness training curriculum; security literacy and awareness
708 training materials; other relevant documents or records].

709 **Interview**

710 [SELECT FROM: Personnel who receive security literacy and awareness training;
711 personnel with responsibilities for security literacy and awareness training;
712 personnel with information security responsibilities].

713 **REFERENCES**

714 Source Assessment Procedures: [AT-02\(04\)](#), [AT-02\(05\)](#), [AT-02\(06\)](#)

715 **03.02.02E Literacy and Awareness Training Practical Exercises**

716 **ASSESSMENT OBJECTIVE**

717 *Determine if:*

718 **A.03.02.02E:** practical exercises in literacy training that simulate events and
719 incidents are provided.

720 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

721 **Examine**
722 [SELECT FROM: System security plan; security literacy and awareness training policy;
723 procedures addressing security literacy and awareness training implementation;
724 security awareness training curriculum; security awareness training materials; other
725 relevant documents or records].

726 **Interview**
727 [SELECT FROM: Personnel who receive security literacy and awareness training;
728 personnel with responsibilities for security awareness training; personnel with
729 information security responsibilities].

730 **Test**
731 [SELECT FROM: Mechanisms implementing cyber-attack simulations in practical
732 exercises].

733 **REFERENCES**

734 Source Assessment Procedures: [AT-02\(01\)](#)

735 **03.02.03E Literacy and Awareness Training Feedback**

736 **ASSESSMENT OBJECTIVE**

737 *Determine if:*

738 **A.03.02.03E.ODP[01]: *personnel to whom feedback on organizational training***
739 ***results will be provided are assigned.***

740 **A.03.02.03E:** feedback on organizational training results is provided to
741 **<A.03.02.03E.ODP[01]: *personnel*>.**

742 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

743 **Examine**

744 [SELECT FROM: Security awareness training policy; procedures addressing security
745 literacy and awareness training records; security literacy and awareness training
746 records; security plan; other relevant documents or records].

747 **Interview**

748 [SELECT FROM: Personnel with security and awareness training record retention
749 responsibilities].

750 **Test**

751 [SELECT FROM: Mechanisms supporting the management of security literacy and
752 awareness training records].

753 **REFERENCES**

754 Source Assessment Procedures: [AT-06](#)

755 **03.02.04E Anti-Counterfeit Training**

756 **ASSESSMENT OBJECTIVE**

757 *Determine if:*

758 **A.03.02.04E.ODP[01]: *personnel or roles requiring training to detect counterfeit***
759 ***system components are defined.***

760 **A.03.02.04E: <A.03.02.04E.ODP[01]: *personnel or roles*>** are trained to detect
761 counterfeit system components.

762 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

763 **Examine**

764 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
765 risk management plan; system and services acquisition policy; anti-counterfeit plan;
766 anti-counterfeit policy and procedures; media disposal policy; media protection
767 policy; incident response policy; training materials addressing counterfeit system
768 components; training records on the detection and prevention of counterfeit
769 components entering the system; system security plan; other relevant documents or
770 records].

771 **Interview**

772 [SELECT FROM: Personnel with information security responsibilities; personnel with
773 supply chain risk management responsibilities; personnel with responsibilities for
774 anti-counterfeit policies, procedures, and training].

775 **Test**

776 [SELECT FROM: Processes for anti-counterfeit training].

777 **REFERENCES**

778 Source Assessment Procedures: [SR-11\(01\)](#)

779 **3.3. [Audit and Accountability](#)**

780 **03.03.01E Audit Record Storage in Separate Environment**

781 **ASSESSMENT OBJECTIVE**

782 *Determine if:*

783 **A.03.03.01E:** audit records are stored in a repository that is part of a physically
784 different system or system component than the system or component being
785 audited.

786 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

787 **Examine**

788 [SELECT FROM: Audit and accountability policy; system security plan; procedures
789 addressing protection of audit information; system design documentation; system
790 configuration settings and associated documentation; system or media storing
791 backups of system audit records; system audit records; other relevant documents or
792 records].

793 **Interview**

794 [SELECT FROM: Personnel with audit and accountability responsibilities; personnel
795 with information security responsibilities; system/network administrators; system
796 developers].

797 **Test**

798 [SELECT FROM: Mechanisms implementing the backing up of audit records].

799 **REFERENCES**

800 Source Assessment Procedures: [AU-09\(02\)](#)

801 **03.03.02E Real-Time Alerts for Audit Processing Failures**

802 **ASSESSMENT OBJECTIVE**

803 *Determine if:*

804 **A.03.03.02E.ODP[01]: *real-time period requiring alerts when audit failure events***
805 ***(defined in A.03.03.02E.ODP[03]) occur is defined.***

806 **A.03.03.02E.ODP[02]: *personnel, roles, and/or locations to be alerted in real time***
807 ***when audit failure events (defined in A.03.03.02E.ODP[03]) occur are defined.***

808 **A.03.03.02E.ODP[03]: *audit logging failure events requiring real-time alerts are***
809 ***defined.***

810 **A.03.03.02E:** an alert is provided within **<A.03.03.02E.ODP[01]: *real-time period*>** to
811 **<A.03.03.02E.ODP[02]: *personnel, roles, and/or locations*>** when
812 **<A.03.03.02E.ODP[03]: *audit logging failure events*>** occur.

813 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

814 **Examine**

815 [SELECT FROM: Audit and accountability policy; procedures addressing response to
816 audit processing failures; system design documentation; system security plan;
817 system configuration settings and associated documentation; system audit records;
818 other relevant documents or records].

819 **Interview**

820 [SELECT FROM: Personnel with audit and accountability responsibilities; personnel
821 with information security responsibilities; system/network administrators; system
822 developers].

823 REFERENCES

824 Source Assessment Procedures: [AU-05\(02\)](#)

825 03.03.03E Dual Authorization for Audit Information and Actions

826 ASSESSMENT OBJECTIVE

827 *Determine if:*

828 **A.03.03.03E.ODP[01]:** *one or more of the following PARAMETER VALUES is/are*
829 *selected: {movement; deletion}.*

830 **A.03.03.03E.ODP[02]:** *audit information for which dual authorization is to be*
831 *enforced is defined.*

832 **A.03.03.03E:** dual authorization is enforced for the <**A.03.03.03E.ODP[01]:**
833 **SELECTED PARAMETER VALUE(S)**> of <**A.03.03.03E.ODP[02]: audit information**>.

834 POTENTIAL ASSESSMENT METHODS AND OBJECTS

835 Examine

836 [SELECT FROM: Audit and accountability policy; system security plan; access control
837 policy and procedures; procedures addressing protection of audit information;
838 system design documentation; system configuration settings and associated
839 documentation; access authorizations; system audit records; other relevant
840 documents or records].

841 Interview

842 [SELECT FROM: Personnel with audit and accountability responsibilities; personnel
843 with information security responsibilities; system/network administrators].

844 Test

845 [SELECT FROM: Mechanisms implementing the enforcement of dual authorization].

846 REFERENCES

847 Source Assessment Procedures: [AU-09\(05\)](#)

848 03.03.04E Integrated Analysis of Audit Records

849 ASSESSMENT OBJECTIVE

850 *Determine if:*

851 **A.03.03.04E.ODP[01]: one or more of the following PARAMETER VALUES is/are**
852 **selected: {vulnerability scanning information; performance data; system**
853 **monitoring information; <A.03.03.04E.ODP[02] data or information collected from**
854 **other sources>}**.

855 **A.03.03.04E.ODP[02]: data or information collected from other sources to be**
856 **analyzed is defined (if selected).**

857 **A.03.03.04E:** analysis of audit records is integrated with analysis of
858 **<A.03.03.04E.ODP[01]: SELECTED PARAMETER VALUE(S)>** to further enhance the
859 ability to identify inappropriate or unusual activity.

860 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

861 **Examine**

862 [SELECT FROM: Audit and accountability policy; system security plan; procedures
863 addressing audit review, analysis, and reporting; system design documentation;
864 system configuration settings and associated documentation; integrated analysis of
865 audit records, vulnerability scanning information, performance data, network
866 monitoring information and associated documentation; other relevant documents
867 or records].

868 **Interview**

869 [SELECT FROM: Personnel with audit review, analysis, and reporting responsibilities;
870 personnel with information security responsibilities].

871 **Test**

872 [SELECT FROM: Mechanisms implementing the capability to integrate analysis of
873 audit records with analysis of data or information sources].

874 **REFERENCES**

875 Source Assessment Procedures: [AU-06\(05\)](#)

876 **3.4. [Configuration Management](#)**

877 **03.04.01E Withdrawn**

878 Addressed by 03.04.08E, 03.14.04E, 03.17.03E, 03.17.04E, 03.17.05E, 03.04.01 (SP
879 800-171), 03.04.03 (SP 800-171), and 03.04.10 (SP 800-171).

880 **03.04.02E Automated Unauthorized Component Detection**

881 **ASSESSMENT OBJECTIVE**

882 *Determine if:*

883 **A.03.04.02E.ODP[01]: automated mechanisms used to detect the presence of**
884 **unauthorized or misconfigured system components are defined.**

885 **A.03.04.02E.ODP[02]: one or more of the following PARAMETER VALUES is/are**
886 **selected: {disable network access by unauthorized or misconfigured system**
887 **components; isolate unauthorized or misconfigured system components; notify**
888 **<A.03.04.02E.ODP[03] personnel or roles>.**

889 **A.03.04.02E.ODP[03]: personnel or roles to be notified when unauthorized or**
890 **misconfigured system components are detected are defined (if selected).**

891 **A.03.04.02E.a:** the presence of unauthorized or misconfigured system components
892 is detected using **<A.03.04.02E.ODP[01]: automated mechanisms>.**

893 **A.03.04.02E.b:** one or more of the following actions is/are taken when unauthorized
894 or misconfigured system components are detected: **<A.03.04.02E.ODP[02]:**
895 **SELECTED PARAMETER VALUE(S)>.**

896 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

897 **Examine**

898 [SELECT FROM: Configuration management policy; procedures addressing system
899 component inventory and configuration settings; configuration management plan;
900 system configuration settings and associated documentation; system component
901 inventory; system design documentation; change control records; common secure
902 configuration checklists; alerts or notifications of unauthorized components within
903 the system; system monitoring records; system maintenance records; system audit
904 records; system security plan; other relevant documents or records].

905 **Interview**

906 [SELECT FROM: Personnel with component inventory and security configuration
907 management responsibilities; personnel with responsibilities for managing
908 automated mechanisms implementing unauthorized system component detection;
909 personnel with information security responsibilities; system/network administrators;
910 system developers].

911 **Test**

912 [SELECT FROM: Processes for the detection of unauthorized or misconfigured system
913 components; automated processes for taking action when unauthorized or
914 misconfigured system components are detected; automated mechanisms
915 supporting and/or implementing the detection of unauthorized or misconfigured
916 system components; automated mechanisms supporting and/or implementing
917 actions taken when unauthorized or misconfigured system components are
918 detected].

919 **REFERENCES**

920 Source Assessment Procedure: [CM-06\(01\)](#), [CM-6\(02\)](#), [CM-08\(03\)](#)

921 **03.04.03E Automated Maintenance of System Component Inventory**

922 **ASSESSMENT OBJECTIVE**

923 *Determine if:*

924 **A.03.04.03E.ODP[01]: *automated mechanisms used to maintain the currency of the***
925 ***system component inventory are defined.***

926 **A.03.04.03E.ODP[02]: *automated mechanisms used to maintain the completeness***
927 ***of the system component inventory are defined.***

928 **A.03.04.03E.ODP[03]: *automated mechanisms used to maintain the accuracy of***
929 ***the system component inventory are defined.***

930 **A.03.04.03E.ODP[04]: *automated mechanisms used to maintain the availability of***
931 ***the system component inventory are defined.***

932 **A.03.04.03E[01]: <A.03.04.03E.ODP[01]: *automated mechanisms*>** are used to
933 maintain the currency of the system component inventory.

934 **A.03.04.03E[02]: <A.03.04.03E.ODP[02]: *automated mechanisms*>** are used to
935 maintain the completeness of the system component inventory.

936 **A.03.04.03E[03]: <A.03.04.03E.ODP[03]: *automated mechanisms*>** are used to
937 maintain the accuracy of the system component inventory.

938 **A.03.04.03E[04]: <A.03.04.03E.ODP[04]: *automated mechanisms*>** are used to
939 maintain the availability of the system component inventory.

940 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

941 **Examine**

942 [SELECT FROM: Configuration management policy; procedures addressing system
943 component inventory; configuration management plan; system security plan;
944 system design documentation; system component inventory; change control
945 records; system maintenance records; system audit records; other relevant
946 documents or records].

947 **Interview**

948 [SELECT FROM: Personnel with component inventory management responsibilities;
949 personnel with information security responsibilities; system developers;
950 system/network administrators].

951 **Test**

952 [SELECT FROM: Processes for maintaining the system component inventory;

953 automated mechanisms supporting and/or implementing the system component
954 inventory].

955 REFERENCES

956 Source Assessment Procedures: [CM-08\(02\)](#)

957 **03.04.04E Automation Support for Baseline Configuration**

958 ASSESSMENT OBJECTIVE

959 *Determine if:*

960 **A.03.04.04E.ODP[01]: automated mechanisms for maintaining the baseline**
961 **configuration of the system are defined.**

962 **A.03.04.04E[01]:** the currency of the baseline configuration of the system is
963 maintained using **<A.03.04.04E.ODP[01]: automated mechanisms>.**

964 **A.03.04.04E[02]:** the completeness of the baseline configuration of the system is
965 maintained using **<A.03.04.04E.ODP[01]: automated mechanisms>.**

966 **A.03.04.04E[03]:** the accuracy of the baseline configuration of the system is
967 maintained using **<A.03.04.04E.ODP[01]: automated mechanisms>.**

968 **A.03.04.04E[04]:** the availability of the baseline configuration of the system is
969 maintained using **<A.03.04.04E.ODP[01]: automated mechanisms>.**

970 POTENTIAL ASSESSMENT METHODS AND OBJECTS

971 **Examine**

972 [SELECT FROM: Configuration management policy; procedures addressing the
973 baseline configuration of the system; configuration management plan; system
974 design documentation; system architecture and configuration documentation;
975 system configuration settings and associated documentation; system component
976 inventory; configuration change control records; system security plan; other
977 relevant documents or records].

978 **Interview**

979 [SELECT FROM: Personnel with configuration management responsibilities;
980 personnel with information security responsibilities; system/network
981 administrators].

982 **Test**

983 [SELECT FROM: Processes for managing baseline configurations; automated
984 mechanisms implementing baseline configuration maintenance].

985 REFERENCES

986 Source Assessment Procedures: [CM-02\(02\)](#)

987 **03.04.05E Dual Authorization for System Changes**

988 **ASSESSMENT OBJECTIVE**

989 *Determine if:*

990 **A.03.04.05E.ODP[01]: system components requiring dual authorization for changes**
991 **are defined.**

992 **A.03.04.05E.ODP[02]: system-level information requiring dual authorization for**
993 **changes is defined.**

994 **A.03.04.05E[01]: dual authorization for implementing changes to**
995 **<A.03.04.05E.ODP[01]: system components> is enforced.**

996 **A.03.04.05E[02]: dual authorization for implementing changes to**
997 **<A.03.04.05E.ODP[02]: system-level information> is enforced.**

998 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

999 **Examine**

1000 [SELECT FROM: Configuration management policy; procedures addressing access
1001 restrictions for changes to the system; configuration management plan; system
1002 design documentation; system architecture and configuration documentation;
1003 system configuration settings and associated documentation; change control
1004 records; system audit records; system component inventory; system information
1005 types; system security plan; other relevant documents or records].

1006 **Interview**

1007 [SELECT FROM: Personnel with dual authorization enforcement responsibilities for
1008 implementing system changes; personnel with information security responsibilities;
1009 system/network administrators].

1010 **Test**

1011 [SELECT FROM: Processes for managing access restrictions to change; mechanisms
1012 implementing dual authorization enforcement].

1013 **REFERENCES**

1014 Source Assessment Procedures: [CM-05\(04\)](#)

1015 **03.04.06E Retention of Previous Configurations**

1016 **ASSESSMENT OBJECTIVE**

1017 *Determine if:*

1018 **A.03.04.06E.ODP[01]: *the number of previous baseline configuration versions to be***
1019 ***retained is defined.***

1020 **A.03.04.06E: <A.03.04.06E.ODP[01]: number>** previous versions of baseline
1021 configurations of the system are retained to support rollback.

1022 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1023 **Examine**

1024 [SELECT FROM: Configuration management policy; procedures addressing the
1025 baseline configuration of the system; configuration management plan; system
1026 architecture and configuration documentation; system configuration settings and
1027 associated documentation; copies of previous baseline configuration versions;
1028 system security plan; other relevant documents or records].

1029 **Interview**

1030 [SELECT FROM: Personnel with configuration management responsibilities;
1031 personnel with information security responsibilities; system/network
1032 administrators].

1033 **Test**

1034 [SELECT FROM: Processes for managing baseline configurations].

1035 **REFERENCES**

1036 Source Assessment Procedures: [CM-02\(03\)](#)

1037 **03.04.07E Testing, Validation, and Documentation of Changes**

1038 **ASSESSMENT OBJECTIVE**

1039 *Determine if:*

1040 **A.03.04.07E[01]:** changes to the system are tested before finalizing the
1041 implementation of the changes.

1042 **A.03.04.07E[02]:** changes to the system are validated before finalizing the
1043 implementation of the changes.

1044 **A.03.04.07E[03]:** changes to the system are documented before finalizing the
1045 implementation of the changes.

1046 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1047 **Examine**

1048 [SELECT FROM: Configuration management policy; configuration management plan;
1049 procedures addressing system configuration change control; system architecture
1050 and configuration documentation; system design documentation; test records;
1051 system configuration settings and associated documentation; validation records;

1052 change control records; system audit records; system security plan; other relevant
1053 documents or records].

1054 **Interview**

1055 [SELECT FROM: Personnel with configuration change control responsibilities;
1056 personnel with information security responsibilities; members of change control
1057 board or similar; system/network administrators; system developers].

1058 **Test**

1059 [SELECT FROM: Processes for configuration change control; mechanisms supporting
1060 and/or implementing, testing, validating, and documenting system changes].

1061 **REFERENCES**

1062 Source Assessment Procedures: [CM-03\(02\)](#)

1063 **03.04.08E Centralized Repository**

1064 **ASSESSMENT OBJECTIVE**

1065 *Determine if:*

1066 **A.03.04.08E:** a centralized repository for the inventory of system components is
1067 provided.

1068 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1069 **Examine**

1070 [SELECT FROM: Configuration management policy; procedures addressing system
1071 component inventory; configuration management plan; system design
1072 documentation; system security plan; system component inventory; system
1073 configuration settings and associated documentation; change control records;
1074 system security plan; other relevant documents or records].

1075 **Interview**

1076 [SELECT FROM: Organizational personnel with component inventory management
1077 responsibilities; organizational personnel with security responsibilities].

1078 **Test**

1079 [SELECT FROM: Organizational processes for managing the system component
1080 inventory; mechanisms supporting and/or implementing system component
1081 inventory].

1082 **REFERENCES**

1083 Source Assessment Procedures: [CM-08\(07\)](#)

1084 **3.5. [Identification and Authentication](#)**

1085 **03.05.01E Cryptographic Bidirectional Authentication**

1086 **ASSESSMENT OBJECTIVE**

1087 *Determine if:*

1088 **A.03.05.01E.ODP[01]: *devices and/or types of devices requiring the use of***
1089 ***cryptographically based bidirectional authentication to authenticate before***
1090 ***establishing a system connection are defined.***

1091 **A.03.05.01E: <A.03.05.01E.ODP[01]: *devices and/or types of devices*>** are
1092 authenticated before establishing a system connection using bidirectional
1093 authentication that is cryptographically based.

1094 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1095 **Examine**

1096 [SELECT FROM: Identification and authentication policy; system security plan;
1097 procedures addressing device identification and authentication; system design
1098 documentation; configuration settings and associated documentation; list of devices
1099 requiring unique identification and authentication; device connection reports; other
1100 relevant documents or records].

1101 **Interview**

1102 [SELECT FROM: Personnel with operational responsibilities for device identification
1103 and authentication; personnel with information security responsibilities;
1104 system/network administrators; system developers].

1105 **Test**

1106 [SELECT FROM: Mechanisms supporting and/or implementing device authentication
1107 capabilities; cryptographically based bidirectional authentication mechanisms].

1108 **REFERENCES**

1109 Source Assessment Procedures: [IA-03\(01\)](#)

1110 **03.05.02E Password Managers**

1111 **ASSESSMENT OBJECTIVE**

1112 *Determine if:*

1113 **A.03.05.02E.ODP[01]: *password managers employed for generating and managing***
1114 ***passwords are defined.***

1115 **A.03.05.02E: <A.03.05.02E.ODP[01]: *password managers*>** are employed to
1116 generate and manage passwords.

1117 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

- 1118 **Examine**
- 1119 [SELECT FROM: Identification and authentication policy; procedures addressing
- 1120 identifier management; system security plan; system design documentation;
- 1121 mechanisms providing dynamic binding of identifiers and authenticators; system
- 1122 configuration settings and associated documentation; system audit records; other
- 1123 relevant documents or records].
- 1124 **Interview**
- 1125 [SELECT FROM: Personnel with identification and authentication management
- 1126 responsibilities; personnel with information security responsibilities;
- 1127 system/network administrators].
- 1128 **Test**
- 1129 [SELECT FROM: Mechanisms supporting and/or implementing account management
- 1130 capabilities; mechanisms supporting and/or implementing identification and
- 1131 authentication management capabilities for the system].
- 1132 **REFERENCES**
- 1133 Source Assessment Procedures: [IA-05\(18\)](#)

1134 **03.05.03E Device Attestation**

1135 **ASSESSMENT OBJECTIVE**

1136 *Determine if:*

1137 ***A.03.05.03E.ODP[01]: the configuration management process employed to handle***

1138 ***device identification and authentication based on attestation is defined.***

1139 **A.03.05.03E:** device identification and authentication are handled based on

1140 attestation by **<A.03.05.02E.ODP[01]: configuration management process>**.

1141 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1142 **Examine**

1143 [SELECT FROM: Identification and authentication policy; system security plan;

1144 procedures addressing device identification and authentication; procedures

1145 addressing device configuration management; system design documentation;

1146 system configuration settings and associated documentation; configuration

1147 management records; change control records; system audit records; other relevant

1148 documents or records].

1149 **Interview**
1150 [SELECT FROM: Personnel with operational responsibilities for device identification
1151 and authentication; personnel with information security responsibilities;
1152 system/network administrators].

1153 **Test**
1154 [SELECT FROM: Mechanisms supporting and/or implementing device identification
1155 and authentication capabilities; mechanisms supporting and/or implementing
1156 configuration management; cryptographic mechanisms supporting device
1157 attestation].

1158 **REFERENCES**

1159 Source Assessment Procedures: [IA-03\(04\)](#)

1160 **03.05.04E No Embedded Unencrypted Static Authenticators**

1161 **ASSESSMENT OBJECTIVE**

1162 *Determine if:*

1163 **A.03.05.04E:** unencrypted static authenticators are not embedded in applications or
1164 other forms of static storage.

1165 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1166 **Examine**

1167 [SELECT FROM: Identification and authentication policy; system security plan;
1168 procedures addressing authenticator management; system design documentation;
1169 system configuration settings and associated documentation; logical access scripts;
1170 application code reviews for detecting unencrypted static authenticators; other
1171 relevant documents or records].

1172 **Interview**

1173 [SELECT FROM: Personnel with authenticator management responsibilities;
1174 personnel with information security responsibilities; system/network administrators;
1175 system developers].

1176 **Test**

1177 [SELECT FROM: Mechanisms supporting and/or implementing authenticator
1178 management capabilities; mechanisms implementing authentication in
1179 applications].

1180 **REFERENCES**

1181 Source Assessment Procedures: [IA-05\(07\)](#)

1182 **03.05.05E Expiration of Cached Authenticators**

1183 **ASSESSMENT OBJECTIVE**

1184 *Determine if:*

1185 **A.03.05.05E.ODP[01]: the time period after which the use of cached authenticators**
1186 **is prohibited is defined.**

1187 **A.03.05.05E:** the use of cached authenticators is prohibited after
1188 **<A.03.05.05E.ODP[01]: time period>.**

1189 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1190 **Examine**

1191 [SELECT FROM: Identification and authentication policy; procedures addressing
1192 authenticator management; system security plan; system design documentation;
1193 system configuration settings and associated documentation; system audit records;
1194 other relevant documents or records].

1195 **Interview**

1196 [SELECT FROM: Personnel with authenticator management responsibilities;
1197 personnel with information security responsibilities; system/network administrators;
1198 system developers].

1199 **Test**

1200 [SELECT FROM: Mechanisms supporting and/or implementing authenticator
1201 management capabilities].

1202 **REFERENCES**

1203 Source Assessment Procedures: [IA-05\(13\)](#)

1204 **03.05.06E Identity Proofing**

1205 **ASSESSMENT OBJECTIVE**

1206 *Determine if:*

1207 **A.03.05.06E.a:** users who require accounts for logical access to systems based on
1208 appropriate identity assurance level requirements as specified in applicable
1209 standards and guidelines are identity-proofed.

1210 **A.03.05.06E.b:** user identities are resolved to a unique individual.

1211 **A.03.05.06E.c[01]:** identity evidence is collected.

1212 **A.03.05.06E.c[02]:** identity evidence is validated.

1213 **A.03.05.06E.c[03]:** identity evidence is verified.

1214 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1215 **Examine**

1216 [SELECT FROM: Identification and authentication policy; procedures addressing
1217 identity proofing; system security plan; other relevant documents or records].

1218 **Interview**

1219 [SELECT FROM: Personnel with system operations responsibilities; personnel with
1220 information security responsibilities; system/network administrators; system
1221 developers; personnel with identification and authentication responsibilities].

1222 **Test**

1223 [SELECT FROM: Mechanisms supporting and/or implementing identification and
1224 authentication capabilities].

1225 **REFERENCES**

1226 Source Assessment Procedure: [IA-12](#)

1227 **03.05.07E Identity Providers and Authorization Servers**

1228 **ASSESSMENT OBJECTIVE**

1229 *Determine if:*

1230 **A.03.05.07E.ODP[01]: an *identification and authentication policy is defined.***

1231 **A.03.05.07E.ODP[02]: *mechanisms supporting authentication and authorization***
1232 ***decisions are defined.***

1233 **A.03.05.07E[01]:** identity providers are employed to manage user, device, and non-
1234 person entity identities, attributes, and access rights supporting authentication
1235 decisions in accordance with **<A.03.05.07E.ODP[01]: *policy*>** using
1236 **<A.03.05.07E.ODP[02]: *mechanisms*>**.

1237 **A.03.05.07E[02]:** identity providers are employed to manage user, device, and non-
1238 person entity identities, attributes, and access rights supporting authorization
1239 decisions in accordance with **<A.03.05.07E.ODP[01]: *policy*>** using
1240 **<A.03.05.07E.ODP[02]: *mechanisms*>**.

1241 **A.03.05.07E[03]:** authorization servers are employed to manage user, device, and
1242 non-person entity identities, attributes, and access rights supporting authentication
1243 decisions in accordance with **<A.03.05.07E.ODP[01]: *policy*>** using
1244 **<A.03.05.07E.ODP[02]: *mechanisms*>**.

1245 **A.03.05.07E[02]:** authorization servers are employed to manage user, device, and
1246 non-person entity identities, attributes, and access rights supporting authorization
1247 decisions in accordance with **<A.03.05.07E.ODP[01]: *policy*>** using
1248 **<A.03.05.07E.ODP[02]: *mechanisms*>**.

1249 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1250 **Examine**

1251 [SELECT FROM: Identification and authentication policy; procedures addressing user
1252 and device identification and authentication; system security plan; system design
1253 documentation; system configuration settings and associated documentation; other
1254 relevant documents or records].

1255 **Interview**

1256 [SELECT FROM: Organizational personnel with system operations responsibilities;
1257 organizational personnel with information security responsibilities; system/network
1258 administrators; organizational personnel with account management responsibilities;
1259 system developers].

1260 **Test**

1261 [SELECT FROM: Mechanisms supporting and/or implementing identification and
1262 authentication capabilities and access rights].

1263 **REFERENCES**

1264 Source Assessment Procedure: [IA-13](#)

1265 **3.6. [Incident Response](#)**

1266 **03.06.01E Security Operations Center**

1267 **ASSESSMENT OBJECTIVE**

1268 *Determine if:*

1269 **A.03.06.01E[01]:** a security operations center is established.

1270 **A.03.06.01E[02]:** a security operations center is maintained.

1271 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1272 **Examine**

1273 [SELECT FROM: Incident response policy; contingency planning policy; procedures
1274 addressing incident handling; procedures addressing the security operations center
1275 operations; mechanisms supporting dynamic response capabilities; system security
1276 plan; contingency plan; incident response plan; other relevant documents or
1277 records].

- 1278 **Interview**
- 1279 [SELECT FROM: Personnel with incident handling responsibilities; personnel with
1280 information security responsibilities; security operations center personnel;
1281 personnel with contingency planning responsibilities].
- 1282 **Test**
- 1283 [SELECT FROM: Mechanisms that support and/or implement the security operations
1284 center capability; mechanisms that support and/or implement the incident handling
1285 process].
- 1286 **REFERENCES**
- 1287 Source Assessment Procedures: [IR-04\(14\)](#)

1288 **03.06.02E Integrated Incident Response Team**

1289 **ASSESSMENT OBJECTIVE**

1290 *Determine if:*

1291 **A.03.06.02E.ODP[01]: *the time period within which an integrated incident***
1292 ***response team can be deployed is defined.***

1293 **A.03.06.02E[01]:** an integrated incident response team is established.

1294 **A.03.06.02E[02]:** an integrated incident response team is maintained.

1295 **A.03.06.02E[03]:** the integrated incident response team can be deployed to any
1296 location identified by the organization in **<A.03.06.02E.ODP[01]: *time period*>**.

1297 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1298 **Examine**

1299 [SELECT FROM: Incident response policy; procedures addressing incident handling;
1300 procedures addressing incident response planning; incident response plan; system
1301 security plan; other relevant documents or records].

1302 **Interview**

1303 [SELECT FROM: Personnel with incident handling responsibilities; personnel with
1304 information security responsibilities; members of the integrated incident response
1305 team].

1306 **REFERENCES**

1307 Source Assessment Procedures: [IR-04\(11\)](#)

1308 **03.06.03E Behavior Analysis**

1309 **ASSESSMENT OBJECTIVE**

1310 *Determine if:*

1311 **A.03.06.03E.ODP[01]: environments or resources that may contain or be related to**
1312 **anomalous or suspected adversarial behavior are defined.**

1313 **A.03.06.03E:** anomalous or suspected adversarial behavior in or related to
1314 **<A.03.06.03E.ODP[01]: environments or resources>** is analyzed.

1315 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1316 **Examine**

1317 [SELECT FROM: Incident response policy; procedures addressing system monitoring
1318 tools and techniques; incident response plan; system monitoring logs or records;
1319 system monitoring tools and techniques documentation; system configuration
1320 settings and associated documentation; system security plan; system component
1321 inventory; network diagram; system protocols documentation; list of acceptable
1322 thresholds for false positives and false negatives; other relevant documents or
1323 records].

1324 **Interview**

1325 [SELECT FROM: Personnel with information security responsibilities; system/network
1326 administrators].

1327 **Test**

1328 [SELECT FROM: Processes for detecting anomalous behavior].

1329 **REFERENCES**

1330 Source Assessment Procedures: [IR-04\(13\)](#)

1331 **03.06.04E Automated Tracking, Data Collection, and Analysis for Incident Monitoring**

1332 **ASSESSMENT OBJECTIVE**

1333 *Determine if:*

1334 **A.03.06.04E.ODP[01]: automated mechanisms used to track incidents are defined.**

1335 **A.03.06.04E.ODP[02]: automated mechanisms used to collect incident information**
1336 **are defined.**

1337 **A.03.06.04E.ODP[03]: automated mechanisms used to analyze incident**
1338 **information are defined.**

1339 **A.03.06.04E[01]:** incidents are tracked using **<A.03.06.04E.ODP[01]: automated**
1340 **mechanisms>**.

1341 **A.03.06.04E[02]:** incident information is collected using **<A.03.06.04E.ODP[02]:**
1342 **automated mechanisms>**.

1343 **A.03.06.04E[03]:** incident information is analyzed using **<A.03.06.04E.ODP[03]:**
1344 **automated mechanisms>**.

1345 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1346 **Examine**

1347 [SELECT FROM: Incident response policy; procedures addressing incident
1348 monitoring; incident response records and documentation; system security plan;
1349 incident response plan; other relevant documents or records].

1350 **Interview**

1351 [SELECT FROM: Personnel with incident monitoring responsibilities; personnel with
1352 information security responsibilities].

1353 **Test**

1354 [SELECT FROM: Incident monitoring capability for the organization; automated
1355 mechanisms supporting and/or implementing the tracking and documenting of
1356 system security incidents].

1357 **REFERENCES**

1358 Source Assessment Procedures: [IR-05\(01\)](#)

1359 **3.7. [Maintenance](#)**

1360 **03.07.01E Software Updates and Patches for Maintenance Tools**

1361 **ASSESSMENT OBJECTIVE**

1362 *Determine if:*

1363 **A.03.07.01E:** maintenance tools are inspected to ensure that the latest software
1364 updates and patches are installed.

1365 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1366 **Examine**

1367 [SELECT FROM: Maintenance policy; procedures addressing system maintenance
1368 tools; system maintenance tools and associated documentation; list of personnel
1369 authorized to use maintenance tools; maintenance tool usage records; maintenance
1370 records; system security plan; other relevant documents or records].

1371 **Interview**

1372 [SELECT FROM: Personnel with system maintenance responsibilities; personnel with
1373 information security responsibilities].

1374 **Test**

1375 [SELECT FROM: Processes for inspecting maintenance tools; processes for
1376 maintenance tool updates; mechanisms supporting and/or implementing the
1377 inspection of maintenance tools; mechanisms supporting and/or implementing
1378 maintenance tool updates].

1379 **REFERENCES**

1380 Source Assessment Procedures: [MA-03\(06\)](#)

1381 **3.8. [Media Protection](#)**

1382 **03.08.01E Dual Authorization for Media Sanitization**

1383 **ASSESSMENT OBJECTIVE**

1384 *Determine if:*

1385 **A.03.08.01E.ODP[01]: *system media containing CUI to be sanitized requiring dual***
1386 ***authorization is defined.***

1387 **A.03.08.01E:** dual authorization for the sanitization of **<A.03.08.01E.ODP[01]:**
1388 ***system media***> is enforced.

1389 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1390 **Examine**

1391 [SELECT FROM: System media protection policy; procedures addressing media
1392 sanitization and disposal; dual authorization policy and procedures; list of system
1393 media requiring dual authorization for sanitization; authorization records; media
1394 sanitization records; audit records; system security plan; other relevant documents
1395 or records].

1396 **Interview**

1397 [SELECT FROM: Personnel with system media sanitization responsibilities; personnel
1398 with information security responsibilities; system/network administrators].

1399 **Test**

1400 [SELECT FROM: Processes requiring dual authorization for media sanitization;
1401 mechanisms supporting and/or implementing media sanitization; mechanisms
1402 supporting and/or implementing dual authorization].

1403 **REFERENCES**

1404 Source Assessment Procedures: [MP-06\(07\)](#)

1405 **03.08.02E Dual Authorization for System Backup Deletion and Destruction**

1406 **ASSESSMENT OBJECTIVE**

1407 *Determine if:*

1408 **A.03.08.02E.ODP[01]: system backup information for which to enforce dual**
1409 **authorization in order to delete or destroy is defined.**

1410 **A.03.08.02E:** dual authorization for the deletion or destruction of
1411 **<A.03.08.02E.ODP[01]: system backup information>** is enforced.

1412 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1413 **Examine**

1414 [SELECT FROM: Contingency planning policy; procedures addressing system backup;
1415 contingency plan; system design documentation; system configuration settings and
1416 associated documentation; system-generated list of dual authorization credentials
1417 or rules; logs or records of the deletion or destruction of backup information; system
1418 security plan; other relevant documents or records]

1419 **Interview**

1420 [SELECT FROM: Personnel with system backup responsibilities; personnel with
1421 information security responsibilities].

1422 **Test**

1423 [SELECT FROM: Mechanisms supporting and/or implementing dual authorization;
1424 mechanisms supporting and/or implementing the deletion and/or destruction of
1425 backup information].

1426 **REFERENCES**

1427 Source Assessment Procedures: [CP-09\(07\)](#)

1428 **03.08.03E Testing System Backups for Reliability and Integrity**

1429 **ASSESSMENT OBJECTIVE**

1430 *Determine if:*

1431 **A.03.08.03E.ODP[01]: the frequency at which to test backup information for media**
1432 **reliability is defined.**

1433 **A.03.08.03E.ODP[02]: the frequency at which to test backup information for**
1434 **information integrity is defined.**

1435 **A.03.08.03E[01]:** backup information is tested **<A.03.08.03E.ODP[01]: frequency>** to
1436 verify media reliability.

1437 **A.03.08.03E[02]:** backup information is tested **<A.03.08.03E.ODP[02]: frequency>** to

1438 verify information integrity.

1439 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1440 **Examine**

1441 [SELECT FROM: Contingency planning policy; procedures addressing system backup;
1442 contingency plan; system backup test results; contingency plan test documentation;
1443 contingency plan test results; system security plan; other relevant documents or
1444 records].

1445 **Interview**

1446 [SELECT FROM: Personnel with system backup responsibilities; personnel with
1447 information security responsibilities].

1448 **Test**

1449 [SELECT FROM: Processes for conducting system backups; mechanisms supporting
1450 and/or implementing system backups].

1451 **REFERENCES**

1452 Source Assessment Procedures: [CP-09\(01\)](#)

1453 **03.08.04E System Recovery and Reconstitution**

1454 **ASSESSMENT OBJECTIVE**

1455 *Determine if:*

1456 **A.03.08.04E.ODP[01]: a time period consistent with recovery time and recovery**
1457 **point objectives for the recovery of the system is determined.**

1458 **A.03.08.04E.ODP[02]: a time period consistent with recovery time and recovery**
1459 **point objectives for the reconstitution of the system is determined.**

1460 **A.03.08.04E[01]:** the recovery of the system to a known state is provided within
1461 **<A.03.08.07E.ODP[01]: time period>** after a disruption, compromise, or failure.

1462 **A.03.08.04E[02]:** the reconstitution of the system to a known state is provided
1463 within **<A.03.08.07E.ODP[02]: time period>** after a disruption, compromise, or
1464 failure.

1465 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1466 **Examine**

1467 [SELECT FROM: Contingency planning policy; procedures addressing system backup;
1468 contingency plan; system backup test results; contingency plan test results;
1469 contingency plan test documentation; redundant secondary system for system
1470 backups; locations of redundant secondary backup systems; system security plan;
1471 other relevant documents or records].

1472 **Interview**

1473 [SELECT FROM: Organizational personnel with contingency planning, recovery,
1474 and/or reconstitution responsibilities; organizational personnel with information
1475 security responsibilities].

1476 **Test**

1477 [SELECT FROM: Organizational processes implementing system recovery and
1478 reconstitution operations; mechanisms supporting and/or implementing system
1479 recovery and reconstitution operations].

1480 **REFERENCES**

1481 Source Assessment Procedures: [CP-10](#)

1482 **3.9. [Personnel Security](#)**

1483 **03.09.01E Withdrawn**

1484 Addressed by 03.09.01.

1485 **03.09.02E Withdrawn**

1486 Addressed by 03.01.01 and 03.09.01.

1487 **03.09.03E Access Agreements**

1488 **ASSESSMENT OBJECTIVE**

1489 *Determine if:*

1490 **A.03.09.03E.ODP[01]: *the frequency at which to review and update access***
1491 ***agreements is defined.***

1492 **A.03.09.03E.ODP[02]: *the frequency at which to re-sign access agreements to***
1493 ***maintain access systems processing, storing, or transmitting CUI is defined.***

1494 **A.03.09.03E.a:** access agreements are developed and documented for systems
1495 processing, storing, or transmitting CUI.

1496 **A.03.09.03E.b[01]:** access agreements are reviewed **<A.03.09.03E.ODP[01]:**
1497 ***frequency*>.**

1498 **A.03.09.03E.b[02]:** access agreements are updated <**A.03.09.03E.ODP[01]:**
1499 **frequency**>.

1500 **A.03.09.03E.c.01:** individuals requiring access to CUI and systems processing,
1501 storing, or transmitting CUI sign appropriate access agreements prior to being
1502 granted access.

1503 **A.03.09.03E.c.02:** individuals requiring access to CUI and systems processing,
1504 storing, or transmitting CUI re-sign access agreements to maintain access when
1505 access agreements have been updated or <**A.03.09.03E.ODP[02]: frequency**>.

1506 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1507 **Examine**

1508 [SELECT FROM: Personnel security policy; personnel security procedures; procedures
1509 addressing access agreements for systems processing, storing, or transmitting CUI;
1510 access control policy; access control procedures; access agreements (including non-
1511 disclosure agreements, acceptable use agreements, rules of behavior, and conflict-
1512 of-interest agreements); documentation of access agreement reviews, updates, and
1513 re-signing; system security plan; other relevant documents or records].

1514 **Interview**

1515 [SELECT FROM: Personnel with personnel security responsibilities; personnel who
1516 have signed and/or resigned access agreements; personnel with information
1517 security responsibilities].

1518 **Test**

1519 [SELECT FROM: Processes for reviewing, updating, and re-signing access agreements;
1520 mechanisms supporting reviewing, updating, and re-signing of access agreements].

1521 **REFERENCES**

1522 Source Assessment Procedures: [PS-06](#)

1523 **03.09.04E Citizenship Requirements**

1524 **ASSESSMENT OBJECTIVE**

1525 *Determine if:*

1526 **A.03.09.04E.ODP[01]:** citizenship requirements to be met by individuals to access a
1527 system processing, storing, or transmitting CUI are defined.

1528 **A.03.09.04E:** individuals accessing a system processing, storing, or transmitting CUI
1529 meet <**A.03.09.04E.ODP[01] citizenship requirements**>.

1530 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1531 **Examine**

1532 [SELECT FROM: Personnel security policy; access control policy, procedures
1533 addressing personnel screening; records of screened personnel; screening criteria;
1534 records of access authorizations; system security plan; other relevant documents or
1535 records].

1536 **Interview**

1537 [SELECT FROM: Personnel with personnel security responsibilities; personnel with
1538 information security responsibilities].

1539 **Test**

1540 [SELECT FROM: Processes for ensuring valid access authorizations for accessing CUI
1541 and systems requiring citizenship; processes for additional personnel screening].

1542 **REFERENCES**

1543 Source Assessment Procedures: [PS-03\(04\)](#)

1544 **3.10. [Physical Protection](#)**

1545 **03.10.01E Intrusion Alarms and Surveillance Equipment**

1546 **ASSESSMENT OBJECTIVE**

1547 *Determine if:*

1548 **A.03.10.01E[01]:** physical access to the facility where the system resides is
1549 monitored using physical intrusion alarms.

1550 **A.03.10.01E[02]:** physical access to the facility where the system resides is
1551 monitored using physical surveillance equipment.

1552 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1553 **Examine**

1554 [SELECT FROM: Physical and environmental protection policy; procedures addressing
1555 physical access monitoring; physical access monitoring records; physical access log
1556 reviews; physical access logs or records; system security plan; other relevant
1557 documents or records].

1558 **Interview**

1559 [SELECT FROM: Personnel with physical access monitoring responsibilities; personnel
1560 with incident response responsibilities; personnel with information security
1561 responsibilities].

1562 **Test**

1563 [SELECT FROM: Processes for monitoring physical intrusion alarms and surveillance
1564 equipment; mechanisms supporting and/or implementing physical intrusion alarms

1565 and surveillance equipment; mechanisms supporting and/or implementing physical
1566 access monitoring].

1567 **REFERENCES**

1568 Source Assessment Procedures: [PE-06\(01\)](#)

1569 **03.10.02E Delivery and Removal of System Components**

1570 **ASSESSMENT OBJECTIVE**

1571 *Determine if:*

1572 **A.03.10.02E.ODP[01]: *the types of system components to be authorized and***
1573 ***controlled when entering the facility are defined.***

1574 **A.03.10.02E.ODP[02]: *the types of system components to be authorized and***
1575 ***controlled when exiting the facility are defined.***

1576 **A.03.10.02E.a[01]: <A.03.10.02E.ODP[01]: *types of system components*>** are
1577 authorized when entering the facility.

1578 **A.03.10.02E.a[02]: <A.03.10.02E.ODP[01]: *types of system components*>** are
1579 controlled when entering the facility.

1580 **A.03.10.02E.a[03]: <A.03.10.02E.ODP[02]: *types of system components*>** are
1581 authorized when exiting the facility.

1582 **A.03.10.02E.a[04]: <A.03.10.02E.ODP[02]: *types of system components*>** are
1583 controlled when exiting the facility.

1584 **A.03.10.02E.b:** records of the system components entering and exiting the facility
1585 are maintained.

1586 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1587 **Examine**

1588 [SELECT FROM: Physical and environmental protection policy; procedures addressing
1589 the delivery and removal of system components from the facility; facility housing the
1590 system; records of items entering and exiting the facility; system security plan; other
1591 relevant documents or records].

1592 **Interview**

1593 [SELECT FROM: Personnel with responsibilities for controlling system components
1594 entering and exiting the facility; personnel with information security
1595 responsibilities].

1596 **Test**

1597 [SELECT FROM: Process for authorizing, monitoring, and controlling system-related
1598 items entering and exiting the facility; mechanisms supporting and/or implementing,

1599 authorizing, monitoring, and controlling system components entering and exiting
1600 the facility].

1601 **REFERENCES**

1602 Source Assessment Procedures: [PE-16](#)

1603 **3.11. [Risk Assessment](#)**

1604 **03.11.01E Threat Awareness Program**

1605 **ASSESSMENT OBJECTIVE**

1606 *Determine if:*

1607 **A.03.11.01E:** a threat awareness program that includes a cross-organization
1608 information-sharing capability for threat intelligence is implemented.

1609 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1610 **Examine**

1611 [SELECT FROM: Information security program plan; threat awareness program
1612 policy; threat awareness program procedures; risk assessment results relevant to
1613 threat awareness; documentation about the cross-organization information-sharing
1614 capability; other relevant documents or records].

1615 **Interview**

1616 [SELECT FROM: Personnel with information security program planning and plan
1617 implementation responsibilities; personnel responsible for the threat awareness
1618 program; personnel responsible for the cross-organization information-sharing
1619 capability; personnel with information security responsibilities; external personnel
1620 with whom threat awareness information is shared by the organization].

1621 **Test**

1622 [SELECT FROM: Processes for implementing the threat awareness program;
1623 processes for implementing the cross-organization information-sharing capability;
1624 mechanisms supporting and/or implementing the threat awareness program;
1625 mechanisms supporting and/or implementing the cross-organization information-
1626 sharing capability].

1627 **REFERENCES**

1628 Source Assessment Procedures: [PM-16](#)

1629 **03.11.02E Threat Hunting**

1630 **ASSESSMENT OBJECTIVE**

- 1631 *Determine if:*
- 1632 **A.03.11.02E.ODP[01]: *the frequency at which to employ the threat-hunting***
- 1633 ***capability is defined.***
- 1634 **A.03.11.02E.a.01[01]:** a cyber threat capability is established to search for indicators
- 1635 of compromise in organizational systems.
- 1636 **A.03.11.02E.a.01[02]:** a cyber threat capability is maintained to search for indicators
- 1637 of compromise in organizational systems.
- 1638 **A.03.11.02E.a.02[01]:** a cyber threat capability is established to detect, track, and
- 1639 disrupt threats that evade existing safeguards.
- 1640 **A.03.11.02E.a.02[02]:** a cyber threat capability is maintained to detect, track, and
- 1641 disrupt threats that evade existing safeguards.
- 1642 **A.03.11.02E.b:** the threat-hunting capability is employed<**A.03.11.02E.ODP[01]:**
- 1643 ***frequency***>.

1644 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1645 **Examine**

1646 [SELECT FROM: Risk assessment policy; assessment reports; audit records and/or

1647 event logs; threat-hunting capability; system security plan; other relevant

1648 documents or records].

1649 **Interview**

1650 [SELECT FROM: Personnel with threat-hunting responsibilities; system/network

1651 administrators; personnel with information security responsibilities].

1652 **Test**

1653 [SELECT FROM: Processes for assessments and audits; mechanisms or tools

1654 supporting and/or implementing threat-hunting capabilities].

1655 **REFERENCES**

1656 Source Assessment Procedures: [RA-10](#)

1657 **03.11.03E Predictive Cyber Analytics**

1658 **ASSESSMENT OBJECTIVE**

1659 *Determine if:*

1660 **A.03.11.03E.ODP[01]: *advanced automation capabilities to predict and identify***
1661 ***risks are defined.***

1662 **A.03.11.03E.ODP[02]: *systems or system components in which advanced***
1663 ***automation and analytics capabilities are to be employed are defined.***

1664 **A.03.11.03E.ODP[03]: *advanced analytics capabilities to predict and identify risks***
1665 ***are defined.***

1666 **A.03.11.03E[01]: <A.03.11.03E.ODP[01]: *advanced automation capabilities*> are**
1667 **employed to predict and identify risks to <A.03.11.03E.ODP[02]: *systems or system***
1668 ***components*>.**

1669 **A.03.11.03E[02]: <A.03.11.03E.ODP[03]: *advanced analytics capabilities*> are**
1670 **employed to predict and identify risks to <A.03.11.03E.ODP[02]: *systems or system***
1671 ***components*>.**

1672 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1673 **Examine**

1674 [SELECT FROM: Risk assessment policy; security planning policy and procedures;
1675 procedures addressing organizational assessments of risk; risk assessment; risk
1676 assessment results; risk assessment reviews; risk assessment updates; risk reports;
1677 system security plan; other relevant documents or records].

1678 **Interview**

1679 [SELECT FROM: Personnel with risk assessment responsibilities; personnel with
1680 information security responsibilities].

1681 **Test**

1682 [SELECT FROM: Processes for risk assessment; mechanisms supporting and/or
1683 conducting, documenting, reviewing, disseminating, and updating the risk
1684 assessment].

1685 **REFERENCES**

1686 Source Assessment Procedures: [RA-03\(04\)](#)

1687 **03.11.04E Withdrawn**

1688 Addressed by 03.15.01E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171), and 03.15.02
1689 (SP 800-171).

1690 **03.11.05E Withdrawn**

1691 Addressed by 03.11.01E, 03.11.03E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171),
1692 03.12.01 (SP 800-171), and 03.12.03 (SP 800-171).

1693 **03.11.06E Withdrawn**

1694 Addressed by 03.12.03E, 03.11.01 (SP 800-171), 03.11.04 (SP 800-171), 03.12.01 (SP
1695 800-171), 03.12.03 (SP 800-171), and 03.17.03 (SP 800-171).

1696 **03.11.07E Withdrawn**

1697 Addressed by 03.17.01 (SP 800-171).

1698 **03.11.08E Dynamic Threat Awareness**

1699 **ASSESSMENT OBJECTIVE**

1700 *Determine if:*

1701 **A.03.11.08E.ODP[01]: the means to determine the current cyber threat**
1702 **environment on an ongoing basis are defined.**

1703 **A.03.11.08E:** the current cyber threat environment is determined on an ongoing
1704 basis using **<A.03.11.08E.ODP[01]: means>**.

1705 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1706 **Examine**

1707 [SELECT FROM: Risk assessment policy; security planning policy and procedures;
1708 procedures addressing organizational assessments of risk; risk assessment; risk
1709 assessment results; risk assessment reviews; risk assessment updates; risk reports;
1710 system security plan; other relevant documents or records].

1711 **Interview**

1712 [SELECT FROM: Personnel with risk assessment responsibilities; personnel with
1713 information security responsibilities].

1714 **Test**

1715 [SELECT FROM: Processes for risk assessment; mechanisms supporting and/or
1716 conducting, documenting, reviewing, disseminating, and updating the risk
1717 assessment].

1718 **REFERENCES**

1719 Source Assessment Procedures: [RA-03\(03\)](#)

1720 **03.11.09E Indicators of Compromise**

1721 **ASSESSMENT OBJECTIVE**

1722 *Determine if:*

1723 **A.03.11.09E.ODP[01]: *sources that provide indicators of compromise are defined.***

1724 **A.03.11.09E.ODP[02]: *personnel or roles to whom indicators of compromise are to***
1725 ***be distributed are defined.***

1726 **A.03.11.09E[01]: indicators of compromise provided by <A.03.11.09E.ODP[01]:**
1727 ***sources*> are discovered.**

1728 **A.03.11.09E[02]: indicators of compromise provided by <A.03.11.09E.ODP[01]:**
1729 ***sources*> are collected.**

1730 **A.03.11.09E[03]: indicators of compromise provided by <A.03.11.09E.ODP[01]:**
1731 ***sources*> are distributed to <A.03.11.09E.ODP[02]: *personnel or roles*>.**

1732 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1733 **Examine**

1734 [SELECT FROM: System and information integrity policy; system and information
1735 integrity procedures; procedures addressing system monitoring; system design
1736 documentation; system monitoring tools and techniques documentation; system
1737 configuration settings and associated documentation; system monitoring logs or
1738 records; system audit records; system security plan; other relevant documents or
1739 records].

1740 **Interview**

1741 [SELECT FROM: System/network administrators; personnel with information security
1742 responsibilities; system developers; personnel installing, configuring, and/or
1743 maintaining the system; personnel responsible for monitoring system hosts].

1744 **Test**

1745 [SELECT FROM: Processes for system monitoring; processes for the discovery,
1746 collection, distribution, and use of indicators of compromise; mechanisms
1747 supporting and/or implementing a system monitoring capability; mechanisms
1748 supporting and/or implementing the discovery, collection, distribution, and use of
1749 indicators of compromise].

1750 **REFERENCES**

1751 Source Assessment Procedures: [SI-04\(24\)](#)

1752 **03.11.10E Criticality Analysis**

1753 **ASSESSMENT OBJECTIVE**

1754 *Determine if:*

1755 **A.03.11.10E.ODP[01]: *systems, system components, or system services to be***
1756 ***analyzed for criticality are defined.***

1757 **A.03.11.10E.ODP[02]: *decision points in the system development life cycle when a***
1758 ***criticality analysis is to be performed are defined.***

1759 **A.03.11.10E:** critical system components and functions are identified by performing
1760 a criticality analysis for <**A.03.11.10E.ODP[01]: *systems, system components, or***
1761 ***system services***> at <**A.03.11.10E.ODP[02]: *decision points***>.

1762 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1763 **Examine**

1764 [SELECT FROM: Risk assessment policy; assessment reports; criticality analysis
1765 and/or finalized criticality for each component and/or subcomponent; audit records
1766 and/or event logs; analysis reports; system security plan; other relevant documents
1767 or records].

1768 **Interview**

1769 [SELECT FROM: Personnel with assessment and auditing responsibilities; personnel
1770 with criticality analysis responsibilities; system/network administrators; personnel
1771 with information security responsibilities].

1772 **Test**

1773 [SELECT FROM: Processes for assessments and audits; mechanisms and/or tools
1774 supporting and/or implementing assessments and auditing].

1775 **REFERENCES**

1776 Source Assessment Procedures: [RA-09](#)

1777 **03.11.11E Discoverable Information**

1778 **ASSESSMENT OBJECTIVE**

1779 *Determine if:*

1780 **A.03.11.11E.ODP[01]: *corrective actions to be taken if information about the***
1781 ***system is discoverable are defined.***

1782 **A.03.11.11E[01]:** discoverable information about the system is identified.

1783 **A.03.11.11E[02]:** <**A.03.11.11E.ODP[01]: *corrective actions***> are taken when
1784 information about the system is confirmed as discoverable.

1785 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1786 **Examine**

1787 [SELECT FROM: Procedures addressing vulnerability scanning; assessment report;
1788 penetration test results; vulnerability scanning results; risk assessment report;
1789 records of corrective actions taken on discoverable information; incident response
1790 records; audit records; system security plan; other relevant documents or records].

1791 **Interview**

1792 [SELECT FROM: Personnel with vulnerability scanning and/or penetration testing
1793 responsibilities; personnel with vulnerability scan analysis responsibilities; personnel
1794 responsible for risk response; personnel responsible for incident management and
1795 response; personnel with information security responsibilities].

1796 **Test**

1797 [SELECT FROM: Processes for vulnerability scanning; processes for risk response;
1798 processes for incident management and response; mechanisms and/or tools
1799 supporting and/or implementing vulnerability scanning; mechanisms supporting
1800 and/or implementing risk response; mechanisms supporting and/or implementing
1801 incident management and response].

1802 **REFERENCES**

1803 Source Assessment Procedures: [RA-05\(04\)](#)

1804 **03.11.12E Automated Means for Sharing Threat Intelligence**

1805 **ASSESSMENT OBJECTIVE**

1806 *Determine if:*

1807 **A.03.11.12E:** automated mechanisms are employed to maximize the effectiveness of
1808 sharing threat intelligence information.

1809 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1810 **Examine**

1811 [SELECT FROM: Information security program plan; threat awareness program
1812 policy; threat awareness program procedures; risk assessment results related to
1813 threat awareness; documentation about the cross-organization information-sharing
1814 capability; other relevant documents or records].

- 1815 **Interview**
- 1816 [SELECT FROM: Personnel with information security program planning and plan
1817 implementation responsibilities; personnel responsible for the threat awareness
1818 program; personnel responsible for the cross-organization information-sharing
1819 capability; personnel with information security responsibilities; external personnel
1820 with whom threat awareness information is shared by the organization].
- 1821 **Test**
- 1822 [SELECT FROM: Processes for implementing the threat awareness program;
1823 processes for implementing the cross-organization information-sharing capability;
1824 automated mechanisms supporting and/or implementing the threat awareness
1825 program; automated mechanisms supporting and/or implementing the cross-
1826 organization information-sharing capability].
- 1827 **REFERENCES**
- 1828 Source Assessment Procedures: [PM-16\(01\)](#)
- 1829 **3.12. [Security Assessment and Monitoring](#)**
- 1830 **03.12.01E Penetration Testing**
- 1831 **ASSESSMENT OBJECTIVE**
- 1832 *Determine if:*
- 1833 **A.03.12.01E.ODP[01]: *the frequency at which to conduct penetration testing on***
1834 ***systems or system components is defined.***
- 1835 **A.03.12.01E.ODP[02]: *systems or system components on which penetration testing***
1836 ***is to be conducted are defined.***
- 1837 **A.03.12.01E: penetration testing is conducted <A.03.12.01E.ODP[01]: *frequency*> on**
1838 **<A.03.12.01E.ODP[02]: *systems or system components*>.**
- 1839 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**
- 1840 **Examine**
- 1841 [SELECT FROM: Assessment and monitoring policy; procedures addressing
1842 penetration testing; assessment plan; system security plan; penetration test rules of
1843 engagement; penetration test report; assessment report; assessment evidence;
1844 other relevant documents or records].
- 1845 **Interview**
- 1846 [SELECT FROM: Personnel with assessment responsibilities; personnel with
1847 information security responsibilities; system/network administrators].

1848 **Test**
1849 [SELECT FROM: Mechanisms supporting penetration testing].

1850 **REFERENCES**

1851 Source Assessment Procedures: [CA-08](#)

1852 **03.12.02E Independent Assessors**

1853 **ASSESSMENT OBJECTIVE**

1854 *Determine if:*

1855 **A.03.12.02E:** independent assessors or assessment teams are used to conduct
1856 security requirement assessments.

1857 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1858 **Examine**

1859 [SELECT FROM: Assessment and monitoring policy; procedures addressing
1860 assessments; previous assessment plan; previous assessment report; plan of action
1861 and milestones; system security plan; other relevant documents or records].

1862 **Interview**

1863 [SELECT FROM: Personnel with assessment responsibilities; personnel with
1864 information security responsibilities].

1865 **REFERENCES**

1866 Source Assessment Procedures: [CA-02\(01\)](#)

1867 **03.12.03E Risk Monitoring**

1868 **ASSESSMENT OBJECTIVE**

1869 *Determine if:*

1870 **A.03.12.03E[01]:** risk monitoring is an integral part of the continuous monitoring
1871 strategy.

1872 **A.03.12.03E[02]:** effectiveness monitoring is included in risk monitoring.

1873 **A.03.12.03E[03]:** compliance monitoring is included in risk monitoring.

1874 **A.03.12.03E[04]:** change monitoring is included in risk monitoring.

1875 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1876 **Examine**

1877 [SELECT FROM: Assessment and monitoring policy; organizational continuous

1878 monitoring strategy; system-level continuous monitoring strategy; procedures
1879 addressing continuous monitoring of system; assessment report; plan of action and
1880 milestones; system monitoring records; impact analyses; status reports; system
1881 security plan; other relevant documents or records].

1882 **Interview**

1883 [SELECT FROM: Personnel with continuous monitoring responsibilities; personnel
1884 with information security responsibilities].

1885 **Test**

1886 [SELECT FROM: Mechanisms supporting risk monitoring].

1887 **REFERENCES**

1888 Source Assessment Procedures: [CA-07\(04\)](#)

1889 **03.12.04E Internal System Connections**

1890 **ASSESSMENT OBJECTIVE**

1891 *Determine if:*

1892 **A.03.12.04E.ODP[01]: system components or classes of components requiring**
1893 **internal connections to the system are defined.**

1894 **A.03.12.04E.ODP[02]: conditions requiring the termination of internal connections**
1895 **are defined.**

1896 **A.03.12.04E.ODP[03]: the frequency at which to review the continued need for**
1897 **each internal connection is defined.**

1898 **A.03.12.04E.a:** internal connections of **<A.03.12.04E.ODP[01]: system components**
1899 **or classes of components>** to the system are authorized.

1900 **A.03.12.04E.b[01]:** for each internal connection, the interface characteristics are
1901 documented.

1902 **A.03.12.04E.b[02]:** for each internal connection, the security requirements are
1903 documented.

1904 **A.03.12.04E.b[03]:** for each internal connection, the nature of the information
1905 communicated is documented.

1906 **A.03.12.04E.c:** internal system connections are terminated after
1907 **<A.03.12.04E.ODP[02]: conditions>**.

1908 **A.03.12.04E.d:** the continued need for each internal connection is reviewed
1909 **<A.03.12.04E.ODP[03]: frequency>**.

1910 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1911 **Examine**

1912 [SELECT FROM: Assessment and monitoring policy; access control policy; procedures
1913 addressing system connections; system and communications protection policy;
1914 system design documentation; system audit records; list of components or classes of
1915 components authorized as internal system connections; system security plan;
1916 system configuration settings and associated documentation; assessment report;
1917 other relevant documents or records].

1918 **Interview**

1919 [SELECT FROM: Personnel with responsibilities for developing, implementing, or
1920 authorizing internal system connections; personnel with information security and
1921 responsibilities].

1922 **Test**

1923 [SELECT FROM: Mechanisms supporting internal system connections].

1924 **REFERENCES**

1925 Source Assessment Procedures: [CA-09](#)

1926 **3.13. [System and Communications Protection](#)**

1927 **03.13.01E Heterogeneity**

1928 **ASSESSMENT OBJECTIVE**

1929 *Determine if:*

1930 **A.03.13.01E.ODP[01]: *system components requiring a diverse set of information***
1931 ***technologies to be employed in the implementation of the system are defined.***

1932 **A.03.13.01E:** a diverse set of information technologies is employed for
1933 **<A.03.13.01E.ODP[01]: *system components*>** in the implementation of the system.

1934 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1935 **Examine**

1936 [SELECT FROM: System and communications protection policy; system design
1937 documentation; system configuration settings and associated documentation; list of
1938 technologies deployed in the system; acquisition documentation; acquisition
1939 contracts for system components or services; system security plan; other relevant
1940 documents or records].

1941 **Interview**

1942 [SELECT FROM: System/network administrators; personnel with information security
1943 responsibilities; personnel with system acquisition, development, and
1944 implementation responsibilities].

1945 **Test**
1946 [SELECT FROM: Mechanisms supporting and/or implementing the use of a diverse
1947 set of information technologies].

1948 **REFERENCES**

1949 Source Assessment Procedures: [SC-29](#)

1950 **03.13.02E Randomness**

1951 **ASSESSMENT OBJECTIVE**

1952 *Determine if:*

1953 **A.03.13.02E.ODP[01]: *the techniques employed to introduce randomness into***
1954 ***organizational operations and assets are defined.***

1955 **A.03.13.02E: <A.03.13.02E.ODP[01]: *techniques*>** are employed to introduce
1956 randomness into organizational operations and assets.

1957 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1958 **Examine**

1959 [SELECT FROM: System and communications protection policy; procedures
1960 addressing concealment and misdirection techniques for the system; system design
1961 documentation; system configuration settings and associated documentation;
1962 system architecture; list of techniques to be used to introduce randomness into
1963 organizational operations and assets; system audit records; system security plan;
1964 other relevant documents or records].

1965 **Interview**

1966 [SELECT FROM: System/network administrators; personnel with the responsibility to
1967 implement concealment and misdirection techniques for systems; personnel with
1968 information security responsibilities].

1969 **Test**

1970 [SELECT FROM: Mechanisms supporting and/or implementing randomness as a
1971 concealment and misdirection technique].

1972 **REFERENCES**

1973 Source Assessment Procedures: [SC-30\(02\)](#)

1974 **03.13.03E Concealment and Misdirection**

1975 **ASSESSMENT OBJECTIVE**

1976 *Determine if:*

1977 **A.03.13.03E.ODP[01]: *the concealment and misdirection techniques employed to***
1978 ***mislead adversaries potentially targeting systems are defined.***

1979 **A.03.13.03E: <A.03.13.03E.ODP[01]: *concealment and misdirection techniques*>** are
1980 used to mislead adversaries.

1981 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

1982 **Examine**

1983 [SELECT FROM: System and communications protection policy; procedures
1984 addressing concealment and misdirection techniques for the system; system design
1985 documentation; system configuration settings and associated documentation;
1986 system architecture; list of concealment and misdirection techniques to be used for
1987 organizational systems; system audit records; system security plan; other relevant
1988 documents or records].

1989 **Interview**

1990 [SELECT FROM: System/network administrators; personnel with information security
1991 responsibilities; personnel with the responsibility to implement concealment and
1992 misdirection techniques for systems].

1993 **Test**

1994 [SELECT FROM: Mechanisms supporting and/or implementing concealment and
1995 misdirection techniques].

1996 **REFERENCES**

1997 Source Assessment Procedures: [SC-30](#)

1998 **03.13.04E Isolation of System Components**

1999 **ASSESSMENT OBJECTIVE**

2000 *Determine if:*

2001 **A.03.13.04E.ODP[01]: *system components to be isolated by boundary protection***
2002 ***mechanisms are defined.***

2003 **A.03.13.04E:** boundary protection mechanisms are employed to isolate
2004 **<A.03.13.04E.ODP[01]: *system components*>.**

2005 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2006 **Examine**

2007 [SELECT FROM: System and communications protection policy; procedures
2008 addressing boundary protection; system design documentation; system hardware
2009 and software; enterprise architecture documentation; system architecture; system
2010 configuration settings and associated documentation; system audit records; system
2011 security plan; other relevant documents or records].

2012 **Interview**

2013 [SELECT FROM: System/network administrators; personnel with information security
2014 responsibilities; personnel with boundary protection responsibilities].

2015 **Test**

2016 [SELECT FROM: Mechanisms supporting and/or implementing the capability to
2017 separate system components].

2018 **REFERENCES**

2019 Source Assessment Procedures: [SC-07\(21\)](#)

2020 **03.13.05E Change Processing and Storage Locations**

2021 **ASSESSMENT OBJECTIVE**

2022 *Determine if:*

2023 **A.03.13.05E.ODP[01]: *processing and/or storage locations to be changed are***
2024 ***defined.***

2025 **A.03.13.05E.ODP[02]: *one of the following PARAMETER VALUES is selected:***
2026 ***{<A.03.13.05E.ODP[03] time frequency>; at random time intervals}.***

2027 **A.03.13.05E.ODP[03]: *the time frequency at which to change the location of***
2028 ***processing and/or storage is defined (if selected).***

2029 **A.03.13.05E: *the location of <A.03.13.05E.ODP[01]: processing and/or storage> is***
2030 ***changed <A.03.13.05E.ODP[02]: SELECTED PARAMETER VALUE>.***

2031 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2032 **Examine**

2033 [SELECT FROM: System and communications protection policy; configuration
2034 management policy and procedures; procedures addressing concealment and
2035 misdirection techniques for the system; list of processing and/or storage locations to
2036 be changed at organizational time intervals; change control records; configuration
2037 management records; system audit records; system security plan; other relevant
2038 documents or records].

2039 **Interview**
2040 [SELECT FROM: System/network administrators; personnel with information security
2041 responsibilities; personnel with the responsibility to change processing and/or
2042 storage locations].

2043 **Test**
2044 [SELECT FROM: Mechanisms supporting and/or implementing changing processing
2045 and/or storage locations].

2046 **REFERENCES**
2047 Source Assessment Procedures: [SC-30\(03\)](#)

2048 **03.13.06E Platform-Independent Applications**

2049 **ASSESSMENT OBJECTIVE**

2050 *Determine if:*

2051 **A.03.13.06E.ODP[01]: *platform-independent applications to be included within***
2052 ***organizational systems are defined.***

2053 **A.03.13.06E: <A.03.13.06E.ODP[01]: *platform-independent applications*>** are
2054 implemented within organizational systems.

2055 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2056 **Examine**

2057 [SELECT FROM: System and communications protection policy; procedures
2058 addressing platform-independent applications; system design documentation;
2059 system configuration settings and associated documentation; list of platform-
2060 independent applications; system audit records; system security plan; other relevant
2061 documents or records].

2062 **Interview**

2063 [SELECT FROM: System/network administrators; personnel with information security
2064 responsibilities; system developers].

2065 **Test**

2066 [SELECT FROM: Mechanisms supporting and/or implementing platform-independent
2067 applications].

2068 **REFERENCES**

2069 Source Assessment Procedures: [SC-27](#)

2070 **03.13.07E Virtualization Techniques**

2071 **ASSESSMENT OBJECTIVE**

2072 *Determine if:*

2073 **A.03.13.07E.ODP[01]: the frequency at which to change the diversity of operating**
2074 **systems and applications deployed using virtualization techniques is defined.**

2075 **A.03.13.07E:** virtualization techniques are employed to support the deployment of a
2076 diverse range of operating systems and applications that are changed
2077 **<A.03.13.07E.ODP[01]: frequency>.**

2078 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2079 **Examine**

2080 [SELECT FROM: System and communications protection policy; configuration
2081 management policy and procedures; system design documentation; system
2082 configuration settings and associated documentation; system architecture; list of
2083 operating systems and applications deployed using virtualization techniques; change
2084 control records; configuration management records; system audit records; system
2085 security plan; other relevant documents or records].

2086 **Interview**

2087 [SELECT FROM: System/network administrators; personnel with information security
2088 responsibilities; personnel with responsibilities for implementing approved
2089 virtualization techniques to the system].

2090 **Test**

2091 [SELECT FROM: Mechanisms supporting and/or implementing the use of a diverse
2092 set of information technologies; mechanisms supporting and/or implementing
2093 virtualization techniques].

2094 **REFERENCES**

2095 Source Assessment Procedures: [SC-29\(01\)](#)

2096 **03.13.08E Decoys**

- 2097 **ASSESSMENT OBJECTIVE**
- 2098 *Determine if:*
- 2099 **A.03.13.08E[01]:** components within organizational systems specifically designed to
2100 be the target of malicious attacks are included to detect such attacks.
- 2101 **A.03.13.08E[02]:** components within organizational systems specifically designed to
2102 be the target of malicious attacks are included to deflect such attacks.
- 2103 **A.03.13.08E[03]:** components within organizational systems specifically designed to
2104 be the target of malicious attacks are included to analyze such attacks.

2105 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

- 2106 **Examine**
- 2107 [SELECT FROM: System and communications protection policy; procedures
2108 addressing the use of decoys; system design documentation; system configuration
2109 settings and associated documentation; system audit records; system security plan;
2110 other relevant documents or records].

- 2111 **Interview**
- 2112 [SELECT FROM: System/network administrators; personnel with information security
2113 responsibilities; system developers].

- 2114 **Test**
- 2115 [SELECT FROM: Mechanisms supporting and/or implementing decoys].

2116 **REFERENCES**

- 2117 Source Assessment Procedures: [SC-26](#)

2118 **03.13.09E Isolation of Security Tools, Mechanisms, and Support Components**

- 2119 **ASSESSMENT OBJECTIVE**
- 2120 *Determine if:*
- 2121 **A.03.13.09E.ODP[01]:** *information security tools, mechanisms, and support*
2122 *components to be isolated from other internal system components are defined.*
- 2123 **A.03.13.09E:** *<A.03.13.09E.ODP[01]: information security tools, mechanisms, and*
2124 *support components>* are isolated from other internal system components by
2125 implementing physically separate subnetworks with managed interfaces to other
2126 components of the system.

2127 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

- 2128 **Examine**
- 2129 [SELECT FROM: System and communications protection policy; procedures

2130 addressing boundary protection; system design documentation; system hardware
2131 and software; system architecture; system configuration settings and associated
2132 documentation; list of security tools and support components to be isolated from
2133 other internal system components; system audit records; system security plan; other
2134 relevant documents or records].

2135 **Interview**

2136 [SELECT FROM: System/network administrators; personnel with information security
2137 responsibilities; personnel with boundary protection responsibilities].

2138 **Test**

2139 [SELECT FROM: Mechanisms supporting and/or implementing the isolation of
2140 information security tools, mechanisms, and support components].

2141 **REFERENCES**

2142 Source Assessment Procedures: [SC-07\(13\)](#)

2143 **03.13.10E Separate Subnetworks**

2144 **ASSESSMENT OBJECTIVE**

2145 *Determine if:*

2146 **A.03.13.10E:** separate network addresses are implemented to connect to systems in
2147 different security domains.

2148 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2149 **Examine**

2150 [SELECT FROM: System and communications protection policy; procedures
2151 addressing boundary protection; system design documentation; system hardware
2152 and software; system architecture; system configuration settings and associated
2153 documentation; system audit records; system security plan; other relevant
2154 documents or records].

2155 **Interview**

2156 [SELECT FROM: System/network administrators; personnel with information security
2157 responsibilities; system developers; personnel with boundary protection
2158 responsibilities].

2159 **Test**

2160 [SELECT FROM: Mechanisms supporting and/or implementing separate network
2161 addresses or different subnets].

2162 **REFERENCES**

2163 Source Assessment Procedures: [SC-07\(22\)](#)

2164 **03.13.11E Thin Nodes**

2165 **ASSESSMENT OBJECTIVE**

2166 *Determine if:*

2167 **A.03.13.11E.ODP[01]: system components to be implemented with minimal**
2168 **functionality and information storage are defined.**

2169 **A.03.13.11E[01]: minimal functionality for <A.03.13.11E.ODP[01]: system**
2170 **components> is employed.**

2171 **A.03.13.11E[02]: minimal information storage on <A.03.13.11E.ODP[01]: system**
2172 **components> is employed.**

2173 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2174 **Examine**

2175 [SELECT FROM: System and communications protection policy; procedures
2176 addressing use of thin nodes; system design documentation; system configuration
2177 settings and associated documentation; system audit records; system security plan;
2178 other relevant documents or records].

2179 **Interview**

2180 [SELECT FROM: System/network administrators; personnel with information security
2181 responsibilities].

2182 **Test**

2183 [SELECT FROM: Mechanisms supporting and/or implementing thin nodes].

2184 **REFERENCES**

2185 Source Assessment Procedures: [SC-25](#)

2186 **03.13.12E Denial-of-Service Protection**

2187 **ASSESSMENT OBJECTIVE**

2188 *Determine if:*

2189 **A.03.13.12E.ODP[01]: the types of denial-of-service events to be protected against**
2190 **or limited are defined.**

2191 **A.03.13.12E.ODP[02]: one of the following PARAMETER VALUES is selected:**
2192 **{protected against; limited}.**

2193 **A.03.13.12E.ODP[03]: the safeguards to prevent the denial-of-service objective by**
2194 **type of denial-of-service event are defined.**

2195 **A.03.13.12E.a: the effects of <A.03.13.12E.ODP[01]: types of denial-of-service**
2196 **events> are <A.03.13.12E.ODP[02]: SELECTED PARAMETER VALUE>.**

2197 **A.03.13.12E.b:** <**A.03.13.12E.ODP[03]: safeguards**> are employed to protect against
2198 or limit the effects of denial-of-service events.

2199 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2200 **Examine**

2201 [SELECT FROM: System and communications protection policy; procedures
2202 addressing denial-of-service protection; list of denial-of-service attacks requiring
2203 employment of security safeguards to protect against or limit effects of such attacks;
2204 system design documentation; list of security safeguards protecting against or
2205 limiting the effects of denial-of-service attacks; system configuration settings and
2206 associated documentation; system audit records; system security plan; other
2207 relevant documents or records].

2208 **Interview**

2209 [SELECT FROM: System/network administrators; personnel with information security
2210 responsibilities; personnel with incident response responsibilities; system
2211 developers].

2212 **Test**

2213 [SELECT FROM: Mechanisms protecting against or limiting the effects of denial-of-
2214 service attacks].

2215 **REFERENCES**

2216 Source Assessment Procedure: [SC-05](#)

2217 **03.13.13E Port and Input/Output Device Access**

2218 **ASSESSMENT OBJECTIVE**

2219 *Determine if:*

2220 **A.03.13.13E.ODP[01]: connection ports or input/output devices to be disabled or**
2221 **removed are defined.**

2222 **A.03.13.13E.ODP[02]: one of the following PARAMETER VALUES is selected:**
2223 **{physically; logically}.**

2224 **A.03.13.13E.ODP[03]: systems or system components with connection ports or**
2225 **input/output devices to be disabled or removed are defined.**

2226 **A.03.13.13E:** <**A.03.13.13E.ODP[01]: connection ports or input/output devices**> are
2227 <**A.03.13.13E.ODP[02]: SELECTED PARAMETER VALUE**> disabled or removed on
2228 <**A.03.13.13E.ODP[03]: systems or system components**>.

2229 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2230 **Examine**

2231 [SELECT FROM: System and communications protection policy; access control policy
2232 and procedures; procedures addressing port and input/output device access; system
2233 design documentation; system architecture; system configuration settings and
2234 associated documentation; systems or system components; list of connection ports
2235 or input/output devices to be physically disabled or removed on systems or system
2236 components; system security plan; other relevant documents or records].

2237 **Interview**

2238 [SELECT FROM: System/network administrators; personnel with information security
2239 responsibilities; personnel installing, configuring, and/or maintaining the system].

2240 **Test**

2241 [SELECT FROM: Mechanisms supporting and/or implementing the disabling of
2242 connection ports or input/output devices].

2243 **REFERENCES**

2244 Source Assessment Procedure: [SC-41](#)

2245 **03.13.14E Detonation Chambers**

2246 **ASSESSMENT OBJECTIVE**

2247 *Determine if:*

2248 **A.03.13.14E.ODP[01]: *the system, system component, or location in which a***
2249 ***detonation chamber capability is to be employed is defined.***

2250 **A.03.13.14E:** a detonation chamber capability is employed within the
2251 **<A.03.13.14E.ODP[01]: *system, system component, or location*>.**

2252 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2253 **Examine**

2254 [SELECT FROM: System and communications protection policy; procedures
2255 addressing detonation chambers; system configuration settings and associated
2256 documentation; system audit records; system design documentation; system
2257 security plan; other relevant documents or records].

2258 **Interview**

2259 [SELECT FROM: system/network administrators; personnel with information security
2260 responsibilities; personnel installing, configuring, and/or maintaining the system].

2261 **Test**

2262 [SELECT FROM: Mechanisms supporting and/or implementing the detonation
2263 chamber capability].

2264 **REFERENCES**

2265 Source Assessment Procedures: [SC-44](#)

2266 **03.13.15E Separate Subnets to Isolate System Components and Functions**

2267 **ASSESSMENT OBJECTIVE**

2268 *Determine if:*

2269 **A.03.13.15E.ODP[01]: one of the following PARAMETER VALUES is selected:**
2270 ***{physically; logically}.***

2271 **A.03.13.15E.ODP[02]: critical system components and functions to be isolated are**
2272 ***defined.***

2273 **A.03.13.15E:** subnetworks are separated <**A.03.13.15E.ODP[01]: SELECTED**
2274 ***PARAMETER VALUE***> to isolate <**A.03.13.15E.ODP[02]: critical system components**
2275 ***and functions***>.

2276 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2277 **Examine**

2278 [SELECT FROM: System and communications protection policy; procedures
2279 addressing boundary protection; system design documentation; system hardware
2280 and software; system architecture; system configuration settings and associated
2281 documentation; criticality analysis; system audit records; system security plan; other
2282 relevant documents or records].

2283 **Interview**

2284 [SELECT FROM: System/network administrators; organizational personnel with
2285 information security responsibilities; system developer; organizational personnel
2286 with boundary protection responsibilities].

2287 **Test**

2288 [SELECT FROM: Mechanisms separating critical system components and functions].

2289 **REFERENCES**

2290 Source Assessment Procedures: [SC-07\(29\)](#)

2291 **03.13.16E System Partitioning**

2292 **ASSESSMENT OBJECTIVE**

2293 *Determine if:*

2294 **A.03.13.16E.ODP[01]: system components to reside in separate physical or logical**
2295 ***domains or environments based on circumstances for the physical or logical***
2296 ***separation of components are defined.***

- 2297 **A.03.13.16E.ODP[02]: one of the following PARAMETER VALUES is selected:**
2298 ***{physical; logical}*.**
- 2299 **A.03.13.16E.ODP[03]: circumstances for the physical or logical separation of**
2300 ***components are defined.***
- 2301 **A.03.13.16E:** the system is partitioned into **<A.03.13.16E.ODP[01]: system**
2302 ***components*>** residing in separate **<A.03.13.16E.ODP[02]: SELECTED PARAMETER**
2303 ***VALUE*>** domains or environments based on **<A.03.13.16E.ODP[03]: circumstances>.**

2304 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2305 **Examine**

2306 [SELECT FROM: System and communications protection policy; procedures
2307 addressing system partitioning; system design documentation; system configuration
2308 settings and associated documentation; system architecture; list of system physical
2309 domains (or environments); system facility diagrams; system network diagrams;
2310 system security plan; other relevant documents or records].

2311 **Interview**

2312 [SELECT FROM: System/network administrators; organizational personnel with
2313 information security responsibilities; organizational personnel installing, configuring,
2314 and/or maintaining the system; system developers/integrators].

2315 **Test**

2316 [SELECT FROM: Mechanisms supporting and/or implementing the physical
2317 separation of system components].

2318 **REFERENCES**

2319 Source Assessment Procedures: [SC-32](#)

2320 **3.14. [System and Information Integrity](#)**

2321 **03.14.01E Software, Firmware, and Information Integrity**

2322 **ASSESSMENT OBJECTIVE**

2323 *Determine if:*

2324 **A.03.14.01E.ODP[01]: software requiring integrity verification tools to be used to**
2325 ***detect unauthorized changes is defined.***

2326 **A.03.14.01E.ODP[02]: firmware requiring integrity verification tools to be used to**
2327 ***detect unauthorized changes is defined.***

2328 **A.03.14.01E.ODP[03]: information requiring integrity verification tools to be used**
2329 ***to detect unauthorized changes is defined.***

2330 **A.03.14.01E.ODP[04]: actions to be taken when unauthorized changes to software**

- 2331 ***are detected are defined.***
- 2332 **A.03.14.01E.ODP[05]: *actions to be taken when unauthorized changes to firmware***
2333 ***are detected are defined.***
- 2334 **A.03.14.01E.ODP[06]: *actions to be taken when unauthorized changes to***
2335 ***information are detected are defined.***
- 2336 **A.03.14.01E.a[01]: integrity verification tools are employed to detect unauthorized**
2337 **changes to <A.03.14.01E.ODP[01]: *software*>.**
- 2338 **A.03.14.01E.a[02]: integrity verification tools are employed to detect unauthorized**
2339 **changes to <A.03.14.01E.ODP[02]: *firmware*>.**
- 2340 **A.03.14.01E.a[03]: integrity verification tools are employed to detect unauthorized**
2341 **changes to <A.03.14.01E.ODP[03]: *information*>.**
- 2342 **A.03.14.01E.b[01]: <A.03.14.01E.ODP[04]: *actions*> are taken when unauthorized**
2343 **changes to software are detected.**
- 2344 **A.03.14.01E.b[02]: <A.03.14.01E.ODP[05]: *actions*> are taken when unauthorized**
2345 **changes to firmware are detected.**
- 2346 **A.03.14.01E.b[03]: <A.03.14.01E.ODP[06]: *actions*> are taken when unauthorized**
2347 **changes to information are detected.**

2348 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2349 **Examine**

2350 [SELECT FROM: System and information integrity policy; system and information
2351 integrity procedures; procedures addressing software, firmware, and information
2352 integrity; system configuration settings and associated documentation; integrity
2353 verification tools and associated documentation; records generated or triggered by
2354 system design documentation; integrity verification tools regarding unauthorized
2355 software, firmware, and information changes; system audit records; system security
2356 plan; other relevant documents or records].

2357 **Interview**

2358 [SELECT FROM: Personnel responsible for software, firmware, and/or information
2359 integrity; personnel with information security responsibilities; system/network
2360 administrators].

2361 **Test**

2362 [SELECT FROM: Software, firmware, and information integrity verification tools].

2363 **REFERENCES**

2364 Source Assessment Procedure: [SI-07](#)

2365 **03.14.02E Withdrawn**

2366 Addressed by 03.14.06 (SP 800-171).

2367 **03.14.03E Withdrawn**

2368 Addressed by 03.15.01E, 03.13.16E, 03.12.01 (SP 800-171), 03.13.01 (SP 800-171),
2369 and 03.16.01 (SP 800-171).

2370 **03.14.04E Refresh From Trusted Sources**

2371 **ASSESSMENT OBJECTIVE**

2372 *Determine if:*

2373 **A.03.14.04E.ODP[01]: *trusted sources to obtain software and data for system***
2374 ***component and service refreshes are defined.***

2375 **A.03.13.14E:** the software and data used during system component and service
2376 refreshes are obtained from **<A.03.14.04E.ODP[01]: *trusted sources*>**.

2377 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2378 **Examine**

2379 [SELECT FROM: System and information integrity policy; system and information
2380 integrity procedures; system design documentation; procedures addressing non-
2381 persistence for system components; system configuration settings and associated
2382 documentation; system audit records; system security plan; other relevant
2383 documents or records].

2384 **Interview**

2385 [SELECT FROM: Personnel responsible for obtaining component and service
2386 refreshes from trusted sources; personnel with information security responsibilities].

2387 **Test**

2388 [SELECT FROM: Processes for defining and obtaining component and service
2389 refreshes from trusted sources; automated mechanisms supporting and/or
2390 implementing component and service refreshes].

2391 **REFERENCES**

2392 Source Assessment Procedures: [SI-14\(01\)](#)

2393 **03.14.05E Non-Persistent Information**

2394 **ASSESSMENT OBJECTIVE**

2395 *Determine if:*

2396 **A.03.14.05E.ODP[01]: one of the following PARAMETER VALUES is selected:**
2397 **{refresh <A.03.14.05E.ODP[02] information> <A.03.14.05E.ODP[03] frequency>;**
2398 **generate <A.03.14.05E.ODP[04] information> on demand}.**

2399 **A.03.14.05E.ODP[02]: the information to be refreshed is defined (if selected).**

2400 **A.03.14.05E.ODP[03]: the frequency at which to refresh information is defined (if**
2401 **selected).**

2402 **A.03.14.05E.ODP[04]: the information to be generated on demand is defined (if**
2403 **selected).**

2404 **A.03.14.05E.a: <A.03.14.05E.ODP[01]: SELECTED PARAMETER VALUE> is**
2405 **performed.**

2406 **A.03.14.05E.b:** information is deleted when no longer needed.

2407 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2408 **Examine**

2409 [SELECT FROM: System and information integrity policy; system and information
2410 integrity procedures; system security plan; procedures addressing non-persistence
2411 for system components; system design documentation; system configuration
2412 settings and associated documentation; system audit records; other relevant
2413 documents or records].

2414 **Interview**

2415 [SELECT FROM: Personnel responsible for ensuring that information is and remains
2416 non-persistent; personnel with information security responsibilities].

2417 **Test**

2418 [SELECT FROM: Processes for ensuring that information is and remains non-
2419 persistent; automated mechanisms supporting and/or implementing component
2420 and service refreshes].

2421 **REFERENCES**

2422 Source Assessment Procedure: [SI-14\(02\)](#)

2423 **03.14.06E Withdrawn**

2424 Addressed by 03.11.02E and 03.11.09E.

2425 **03.14.07E Withdrawn**

2426 Addressed by 03.14.08E, 03.14.10E, 03.14.14E, , 03.17.03E, and 03.16.01 (SP 800-
2427 171).

2428 **03.14.08E Integrity Checks**

2429 **ASSESSMENT OBJECTIVE**

2430 *Determine if:*

2431 **A.03.14.08E.ODP[01]: software on which an integrity check is to be performed is**
2432 **defined.**

2433 **A.03.14.08E.ODP[02]: one or more of the following PARAMETER VALUES is/are**
2434 **selected: {at startup; at <A.03.14.08E.ODP[03] transitional states or security-**
2435 **relevant events>; <A.03.14.08E.ODP[04] frequency>}.**

2436 **A.03.14.08E.ODP[03]: transitional states or security-relevant events requiring**
2437 **integrity checks (on software) are defined (if selected).**

2438 **A.03.14.08E.ODP[04]: the frequency at which to perform an integrity check (on**
2439 **software) is defined (if selected).**

2440 **A.03.14.08E.ODP[05]: firmware on which an integrity check is to be performed is**
2441 **defined.**

2442 **A.03.14.08E.ODP[06]: one or more of the following PARAMETER VALUES is/are**
2443 **selected: {at startup; at <A.03.14.08E.ODP[07] transitional states or security-**
2444 **relevant events>; <A.03.14.08E.ODP[08] frequency>}.**

2445 **A.03.14.08E.ODP[07]: transitional states or security-relevant events requiring**
2446 **integrity checks (on firmware) are defined (if selected).**

2447 **A.03.14.08E.ODP[08]: the frequency at which to perform an integrity check (on**
2448 **firmware) is defined (if selected).**

2449 **A.03.14.08E.ODP[09]: information on which an integrity check is to be performed is**
2450 **defined.**

2451 **A.03.14.08E.ODP[10]: one or more of the following PARAMETER VALUES is/are**
2452 **selected: {at startup; at <A.03.14.08E.ODP[11] transitional states or security-**
2453 **relevant events>; <A.03.14.08E.ODP[12] frequency>}.**

2454 **A.03.14.08E.ODP[11]: transitional states or security-relevant events requiring**
2455 **integrity checks (of information) are defined (if selected).**

2456 **A.03.14.08E.ODP[12]: the frequency at which to perform an integrity check (of**
2457 **information) is defined (if selected).**

2458 **A.03.14.08E[01]: an integrity check of <A.03.14.08E.ODP[01]: software> is**
2459 **performed <A.03.14.05E.ODP[02]: SELECTED PARAMETER VALUE(S)>.**

2460 **A.03.14.08E[02]**: an integrity check of <**A.03.14.08E.ODP[05]: firmware**> is
2461 performed <**A.03.14.08E.ODP[06]: SELECTED PARAMETER VALUE(S)**>.

2462 **A.03.14.08E[03]**: an integrity check of <**A.03.14.08E.ODP[09]: information**> is
2463 performed <**A.03.14.08E.ODP[10]: SELECTED PARAMETER VALUE(S)**>.

2464 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2465 **Examine**

2466 [SELECT FROM: System and information integrity policy; system and information
2467 integrity procedures; procedures addressing software, firmware, and information
2468 integrity testing; system design documentation; system configuration settings and
2469 associated documentation; system security plan; integrity verification tools and
2470 associated documentation; records of integrity scans; other relevant documents or
2471 records].

2472 **Interview**

2473 [SELECT FROM: Personnel responsible for software, firmware, and/or information
2474 integrity; personnel with information security responsibilities; system/network
2475 administrators; system developers].

2476 **Test**

2477 [SELECT FROM: Software, firmware, and information integrity verification tools].

2478 **REFERENCES**

2479 Source Assessment Procedure: [SI-07\(01\)](#)

2480 **03.14.09E Cryptographic Protection**

2481 **ASSESSMENT OBJECTIVE**

2482 *Determine if:*

2483 **A.03.14.09E[01]**: cryptographic mechanisms are implemented to detect
2484 unauthorized changes to software.

2485 **A.03.14.09E[02]**: cryptographic mechanisms are implemented to detect
2486 unauthorized changes to firmware.

2487 **A.03.14.09E[03]**: cryptographic mechanisms are implemented to detect
2488 unauthorized changes to information.

2489 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2490 **Examine**

2491 [SELECT FROM: System and information integrity policy; system and information
2492 integrity procedures; procedures addressing software, firmware, and information
2493 integrity; system design documentation; system configuration settings and

2494 associated documentation; system audit records; system security plan;
2495 cryptographic mechanisms and associated documentation; records of detected
2496 unauthorized changes to software, firmware, and information; other relevant
2497 documents or records].

2498 **Interview**

2499 [SELECT FROM: Personnel responsible for software, firmware, and/or information
2500 integrity; personnel with information security responsibilities; system/network
2501 administrators; system developers].

2502 **Test**

2503 [SELECT FROM: Software, firmware, and information integrity verification tools;
2504 cryptographic mechanisms implementing software, firmware, and information
2505 integrity].

2506 **REFERENCES**

2507 Source Assessment Procedures: [SI-07\(06\)](#)

2508 **03.14.10E Protection of Boot Firmware**

2509 **ASSESSMENT OBJECTIVE**

2510 *Determine if:*

2511 **A.03.14.10E.ODP[01]: mechanisms to be implemented to protect the integrity of**
2512 **boot firmware in system components are defined.**

2513 **A.03.14.10E.ODP[02]: system components requiring mechanisms to protect the**
2514 **integrity of boot firmware are defined.**

2515 **A.03.14.10E: <A.03.14.10E.ODP[01]: mechanisms>** are implemented to protect the
2516 integrity of boot firmware in **<A.03.14.10E.ODP[02]: system components>**.

2517 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2518 **Examine**

2519 [SELECT FROM: System and information integrity policy; system and information
2520 integrity procedures; procedures addressing software, firmware, and information
2521 integrity; system design documentation; system configuration settings and
2522 associated documentation; system security plan; integrity verification tools and
2523 associated documentation; records of integrity verification scans; system audit
2524 records; other relevant documents or records].

2525 **Interview**

2526 [SELECT FROM: Personnel responsible for software, firmware, and/or information
2527 integrity; personnel with information security responsibilities; system/network
2528 administrators; system developer].

- 2529 **Test**
- 2530 [SELECT FROM: Software, firmware, and information integrity verification tools;
2531 mechanisms supporting and/or implementing protection of the integrity of boot
2532 firmware; safeguards implementing protection of the integrity of boot firmware].
- 2533 **REFERENCES**
- 2534 Source Assessment Procedures: [SI-07\(10\)](#)
- 2535 **03.14.11E Integration of Detection and Response**
- 2536 **ASSESSMENT OBJECTIVE**
- 2537 *Determine if:*
- 2538 **A.03.14.11E.ODP[01]: security-relevant changes to the system are defined.**
- 2539 **A.03.14.11E:** the detection of <**A.03.14.11E.ODP[01]: changes**> are incorporated
2540 into the organizational incident response capability.
- 2541 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**
- 2542 **Examine**
- 2543 [SELECT FROM: System and information integrity policy; system and information
2544 integrity procedures; procedures addressing software, firmware, and information
2545 integrity; procedures addressing incident response; system design documentation;
2546 system configuration settings and associated documentation; incident response
2547 records; audit records; system security plan; other relevant documents or records].
- 2548 **Interview**
- 2549 [SELECT FROM: Personnel responsible for software, firmware, and/or information
2550 integrity; personnel with information security responsibilities; personnel with
2551 incident response responsibilities].
- 2552 **Test**
- 2553 [SELECT FROM: Processes for incorporating the detection of unauthorized security-
2554 relevant changes into the incident response capability; mechanisms supporting
2555 and/or implementing the incorporation of detection of unauthorized security-
2556 relevant changes into the incident response capability; software, firmware, and
2557 information integrity verification tools].
- 2558 **REFERENCES**
- 2559 Source Assessment Procedures: [SI-07\(07\)](#)

2560 **03.14.12E Information Input Validation**

2561 **ASSESSMENT OBJECTIVE**

2562 *Determine if:*

2563 **A.03.14.12E.ODP[01]: information inputs to the system requiring validity checks**
2564 **are defined.**

2565 **A.03.14.12E:** the validity of the **<A.03.14.12E.ODP[01]: information inputs>** is
2566 checked.

2567 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2568 **Examine**

2569 [SELECT FROM: System and information integrity policy; system and information
2570 integrity procedures; access control policy and procedures; separation of duties
2571 policy and procedures; procedures addressing information input validation;
2572 documentation for automated tools and applications to verify the validity of
2573 information; list of information inputs requiring validity checks; system design
2574 documentation; system configuration settings and associated documentation;
2575 system audit records; system security plan; other relevant documents or records].

2576 **Interview**

2577 [SELECT FROM: Personnel responsible for information input validation; personnel
2578 with information security responsibilities; system/network administrators; system
2579 developers].

2580 **Test**

2581 [SELECT FROM: Mechanisms supporting and/or implementing validity checks on
2582 information inputs].

2583 **REFERENCES**

2584 Source Assessment Procedures: [SI-10](#)

2585 **03.14.13E Error Handling**

2586 **ASSESSMENT OBJECTIVE**

2587 *Determine if:*

2588 **A.03.14.13E.ODP[01]: personnel or roles to whom error messages are to be**
2589 **revealed are defined.**

2590 **A.03.14.13E.a:** error messages that provide the information necessary for corrective
2591 actions are generated without revealing information that could be exploited.

2592 **A.03.14.13E.b:** error messages are revealed only to **<A.03.14.13E.ODP[01]:**
2593 **personnel or roles>.**

2594 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2595 **Examine**

2596 [SELECT FROM: System and information integrity policy; system and information
2597 integrity procedures; procedures addressing system error handling; system design
2598 documentation; system configuration settings and associated documentation;
2599 documentation providing the structure and content of error messages; system audit
2600 records; system security plan; other relevant documents or records].

2601 **Interview**

2602 [SELECT FROM: Personnel responsible for information input validation; personnel
2603 with information security responsibilities; system/network administrators; system
2604 developers].

2605 **Test**

2606 [SELECT FROM: Processes for error handling; automated mechanisms supporting
2607 and/or implementing error handling; automated mechanisms supporting and/or
2608 implementing the management of error messages].

2609 **REFERENCES**

2610 Source Assessment Procedure: [SI-11](#)

2611 **03.14.14E Memory Protection**

2612 **ASSESSMENT OBJECTIVE**

2613 *Determine if:*

2614 **A.03.14.14E.ODP[01]: *safeguards to be implemented to protect the system***
2615 ***memory from unauthorized code execution are defined.***

2616 **A.03.14.14E: <A.03.14.14E.ODP[01]: *safeguards*>** are implemented to protect the
2617 system memory from unauthorized code execution.

2618 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2619 **Examine**

2620 [SELECT FROM: System and information integrity policy; system and information
2621 integrity procedures; procedures addressing memory protection for the system;
2622 system design documentation; system configuration settings and associated
2623 documentation; list of security safeguards protecting system memory from
2624 unauthorized code execution; system audit records; system security plan; other
2625 relevant documents or records].

- 2626 **Interview**
- 2627 [SELECT FROM: Personnel responsible for memory protection; personnel with
2628 information security responsibilities; system/network administrators; system
2629 developers].
- 2630 **Test**
- 2631 [SELECT FROM: Automated mechanisms supporting and/or implementing safeguards
2632 to protect the system memory from unauthorized code execution].
- 2633 **REFERENCES**
- 2634 Source Assessment Procedure: [SI-16](#)

2635 **03.14.15E Non-Persistent System Components and Services**

2636 **ASSESSMENT OBJECTIVE**

2637 *Determine if:*

2638 **A.03.14.15E.ODP[01]: non-persistent system components and services to be**
2639 **implemented are defined.**

2640 **A.03.14.15E.ODP[02]: one or more of the following PARAMETER VALUES is/are**
2641 **selected: {upon end of session of use; <A.03.14.15E.ODP[03] frequency>}.**

2642 **A.03.14.15E.ODP[03]: the frequency at which to terminate non-persistent**
2643 **components and services that are initiated in a known state is defined (if selected).**

2644 **A.03.14.15E.a: <A.03.14.15E.ODP[01]: non-persistent system components and**
2645 **services> that are initiated in a known state are implemented.**

2646 **A.03.14.15E.b: <A.03.14.15E.ODP[01]: non-persistent system components and**
2647 **services> that are initiated from a known state are implemented.**

2648 **A.03.14.15E.c: <A.03.14.13E.ODP[01]: non-persistent system components and**
2649 **services> are terminated <A.03.14.15E.ODP[02]: SELECTED PARAMETER VALUE(S)>.**

2650 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2651 **Examine**

2652 [SELECT FROM: System and information integrity policy; system and information
2653 integrity procedures; system design documentation; procedures addressing non-
2654 persistence for system components; system security plan; system configuration
2655 settings and associated documentation; system audit records; other relevant
2656 documents or records].

2657 **Interview**

2658 [SELECT FROM: Personnel responsible for non-persistence; personnel with
2659 information security responsibilities; system/network administrators; system

2660 developers].

2661 **Test**

2662 [SELECT FROM: Automated mechanisms supporting and/or implementing the
2663 initiation and termination of non-persistent components].

2664 **REFERENCES**

2665 Source Assessment Procedure: [SI-14](#)

2666 **03.14.16E Tainting**

2667 **ASSESSMENT OBJECTIVE**

2668 *Determine if:*

2669 **A.03.14.16E.ODP[01]: systems or system components with data or capabilities to**
2670 **be embedded are defined.**

2671 **A.03.14.16E:** data or capabilities are embedded in **<A.03.14.16E.ODP[01]: systems**
2672 **or system components>** to determine if CUI has been exfiltrated or improperly
2673 removed from the organization.

2674 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2675 **Examine**

2676 [SELECT FROM: System and information integrity policy; system and information
2677 integrity procedures; procedures addressing software and information integrity;
2678 system design documentation; system configuration settings and associated
2679 documentation; policy and procedures addressing the systems security engineering
2680 technique of deception; system security plan; other relevant documents or records].

2681 **Interview**

2682 [SELECT FROM: Personnel responsible for detecting tainted data; personnel with
2683 systems security engineering responsibilities; personnel with information security
2684 responsibilities].

2685 **Test**

2686 [SELECT FROM: Automated mechanisms for post-breach detection; decoys, traps,
2687 lures, and methods for deceiving adversaries; detection and notification
2688 mechanisms].

2689 **REFERENCES**

2690 Source Assessment Procedure: [SI-20](#)

2691 **03.14.17E System-Generated Alerts**

2692 **ASSESSMENT OBJECTIVE**

2693 *Determine if:*

2694 **A.03.14.17E.ODP[01]: *personnel or roles to be alerted when indications of***
2695 ***compromise are defined.***

2696 **A.03.14.17E.ODP[02]: *compromise indicators are defined.***

2697 **A.03.14.17E: <A.03.14.17E.ODP[01]: *personnel or roles*> are alerted when system-**
2698 **generated <A.03.14.17E.ODP[02]: *indicators of compromise*> occur.**

2699 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2700 **Examine**

2701 [SELECT FROM: System and information integrity policy; system and information
2702 integrity procedures; system security plan; system audit records; procedures
2703 addressing system monitoring tools and techniques; system monitoring tools and
2704 techniques documentation; list of personnel selected to receive alerts; system
2705 configuration settings and associated documentation; documentation of alerts
2706 generated based on compromise indicators; other relevant documents or records].

2707 **Interview**

2708 [SELECT FROM: Personnel with information security responsibilities; system
2709 developers; personnel installing, configuring, and/or maintaining the system;
2710 personnel responsible for monitoring the system; personnel on the system alert
2711 notification list; personnel responsible for the intrusion detection system;
2712 system/network administrators].

2713 **Test**

2714 [SELECT FROM: Processes for intrusion detection and system monitoring;
2715 mechanisms supporting and/or implementing intrusion detection and system
2716 monitoring capabilities; mechanisms supporting and/or implementing alerts for
2717 compromise indicators].

2718 **REFERENCES**

2719 Source Assessment Procedure: [SI-04\(05\)](#)

2720 **03.14.18E Automated Organization-Generated Alerts**

2721 **ASSESSMENT OBJECTIVE**

2722 *Determine if:*

2723 **A.03.14.18E.ODP[01]: *personnel or roles to be alerted when indications of***
2724 ***inappropriate or unusual activities with security implications occur are defined.***

2725 **A.03.14.18E.ODP[02]: *automated mechanisms used to alert personnel or roles are***
2726 ***defined.***

2727 **A.03.14.18E.ODP[03]: *activities that trigger alerts to personnel or roles are***
2728 ***defined.***

2729 **A.03.14.18E: <A.03.14.18E.ODP[01]: *personnel or roles*> are alerted using**
2730 **<A.03.14.18E.ODP[02]: *automated mechanisms*> when <A.03.14.18E.ODP[03]:**
2731 ***activities*> indicate inappropriate or unusual activities with security implications.**

2732 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2733 **Examine**

2734 [SELECT FROM: System and information integrity policy; system and information
2735 integrity procedures; system security plan; list of inappropriate or unusual activities
2736 with security implications that trigger alerts; suspicious activity reports; system
2737 monitoring tools and techniques documentation; system design documentation;
2738 procedures addressing system monitoring tools and techniques; alerts provided to
2739 security personnel; system configuration settings and associated documentation;
2740 system monitoring logs or records; system audit records; other relevant documents
2741 or records].

2742 **Interview**

2743 [SELECT FROM: Personnel with information security responsibilities; system
2744 developers; personnel installing, configuring, and/or maintaining the system;
2745 personnel responsible for monitoring the system; personnel responsible for the
2746 intrusion detection system; system/network administrators].

2747 **Test**

2748 [SELECT FROM: Processes for intrusion detection and system monitoring; automated
2749 mechanisms supporting and/or implementing intrusion detection and system
2750 monitoring capabilities; automated mechanisms supporting and/or implementing
2751 automated alerts to security personnel].

2752 **REFERENCES**

2753 Source Assessment Procedure: [SI-04\(12\)](#)

2754 **3.15. [Planning](#)**

2755 **03.15.01E Security Architecture**

2756 **ASSESSMENT OBJECTIVE**

2757 *Determine if:*

2758 **A.03.15.01E.ODP[01]: *the frequency for reviewing and updating the security***
2759 ***architecture to reflect changes in the enterprise architecture is defined.***

2760 **A.03.15.01E.a.01:** a security architecture for the system that describes the
2761 requirements and approach to be taken for protecting the confidentiality, integrity,
2762 and availability of CUI is developed.

2763 **A.03.15.01E.a.02:** a security architecture for the system that describes how the
2764 security architecture is integrated into and supports the enterprise architecture is
2765 developed.

2766 **A.03.15.01E.a.03:** a security architecture for the system that describes any
2767 assumptions about and dependencies on external systems and services is
2768 developed.

2769 **A.03.15.01E.b:** the security architecture is reviewed and updated
2770 **<A.03.15.01E.ODP[01]: *frequency*>** to reflect changes in the enterprise architecture.

2771 **A.03.15.01E.c:** planned security architecture changes are reflected in system
2772 security plans, concept of operations, criticality analyses, organizational procedures,
2773 procurements, and acquisitions.

2774 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2775 **Examine**

2776 [SELECT FROM: Security planning policy; procedures addressing information security
2777 architecture development; procedures addressing information security architecture
2778 reviews and updates; enterprise architecture documentation; information security
2779 architecture documentation; system security plan; security CONOPS for the system;
2780 records of information security architecture reviews and updates; other relevant
2781 documents or records].

2782 **Interview**

2783 [SELECT FROM: Personnel with security planning and plan implementation
2784 responsibilities; personnel with information security responsibilities; personnel with
2785 information security architecture development responsibilities].

2786 **Test**

2787 [SELECT FROM: Mechanisms supporting and/or implementing the development,
2788 review, and update of the information security architecture; processes for
2789 developing, reviewing, and updating the information security architecture].

2790 **REFERENCES**

2791 Source Assessment Procedures: [PL-08](#)

2792 **03.15.02E Defense In Depth**

2793 **ASSESSMENT OBJECTIVE**

2794 *Determine if:*

2795 **A.03.15.02E.ODP[01]: security requirements to be allocated to architectural layers**
2796 **and locations are defined.**

2797 **A.03.15.02E.ODP[02]: architectural layers and locations are defined.**

2798 **A.03.15.02E.a:** the security architecture for the system is designed using a defense-
2799 in-depth approach.

2800 **A.03.15.02E.b:** *<A.03.15.02E.ODP[01]: security requirements>* are allocated to
2801 *<A.03.15.02E.ODP[02]: architectural layers and locations>*.

2802 **A.03.15.02E.c:** the security requirements allocated to the architectural layers and
2803 locations are coordinated and mutually reinforcing.

2804 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2805 **Examine**

2806 [SELECT FROM: Security planning policy; procedures addressing information security
2807 architecture development; enterprise architecture documentation; information
2808 security architecture documentation; system security plan; security CONOPS for the
2809 system; other relevant documents or records].

2810 **Interview**

2811 [SELECT FROM: Personnel with information security responsibilities; personnel with
2812 information security architecture development responsibilities; personnel with
2813 security planning and plan implementation responsibilities].

2814 **Test**

2815 [SELECT FROM: Processes for designing the information security architecture;
2816 mechanisms supporting and/or implementing the design of the information security
2817 architecture].

2818 **REFERENCES**

2819 Source Assessment Procedures: [PL-08\(01\)](#)

2820 **03.15.03E Supplier Diversity**

2821 **ASSESSMENT OBJECTIVE**

2822 *Determine if:*

2823 **A.03.15.03E.ODP[01]: *safeguards to be allocated to architectural layers and***
2824 ***locations are defined.***

2825 **A.03.15.03E.ODP[02]: *architectural layers and locations are defined.***

2826 **A.03.15.03E: <A.03.15.03E.ODP[01]: *safeguards*> that are allocated to**
2827 **<A.03.15.03E.ODP[02]: *architectural layers and locations*> are obtained from**
2828 **different suppliers.**

2829 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2830 **Examine**

2831 [SELECT FROM: Security planning policy; procedures addressing information security
2832 architecture development; enterprise architecture documentation; information
2833 security architecture documentation; system security plan; security CONOPS for the
2834 system; IT acquisitions policy; other relevant documents or records].

2835 **Interview**

2836 [SELECT FROM: Personnel with acquisition responsibilities personnel with
2837 information security responsibilities; personnel with security planning and plan
2838 implementation responsibilities; personnel with information security architecture
2839 development responsibilities].

2840 **Test**

2841 [SELECT FROM: Processes for obtaining information security safeguards from
2842 different suppliers].

2843 **REFERENCES**

2844 Source Assessment Procedures: [PL-08\(02\)](#)

2845 **3.16. [System and Services Acquisition](#)**

2846 **03.16.01E Specialization**

2847 **ASSESSMENT OBJECTIVE**

2848 *Determine if:*

2849 **A.03.16.01E.ODP[01]: *one or more of the following PARAMETER VALUES is/are***
2850 ***selected: {design; modification; augmentation; reconfiguration}.***

2851 **A.03.16.01E.ODP[02]: systems or system components supporting mission-essential**
2852 **services or functions are defined.**

2853 **A.03.16.01E: <A.03.16.01E.ODP[01]: SELECTED PARAMETER VALUE(S)>** is/are
2854 employed to **<A.03.16.01E.ODP[02]: systems or system components>** supporting
2855 mission-essential services or functions to increase the trustworthiness in those
2856 systems or components.

2857 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2858 **Examine**

2859 [SELECT FROM: System and services acquisition policy; procedures addressing design
2860 modification, augmentation, or reconfiguration of systems or system components;
2861 documented evidence of design modification, augmentation, or reconfiguration;
2862 system security plan; supply chain risk management plan; other relevant documents
2863 or records].

2864 **Interview**

2865 [SELECT FROM: Personnel with system and service acquisition responsibilities;
2866 personnel with information security responsibilities; personnel with security
2867 architecture responsibilities; personnel with configuration management
2868 responsibilities].

2869 **Test**

2870 [SELECT FROM: Processes for the modification, design, augmentation, or
2871 reconfiguration of systems or system components; mechanisms supporting and/or
2872 implementing design modification, augmentation, or reconfiguration of systems or
2873 system components].

2874 **REFERENCES**

2875 Source Assessment Procedure: [SA-23](#)

2876 **3.17. Supply Chain Risk Management**

2877 **03.17.01E Notification Agreements**

2878 **ASSESSMENT OBJECTIVE**

2879 *Determine if:*

2880 **A.03.17.01E.ODP[01]: one or more of the following PARAMETER VALUES is/are**
2881 **selected: {notification of supply chain compromises; results of assessments or**
2882 **audits; provision of <A.03.17.01E.ODP[02]: information>}**.

2883 **A.03.17.01E.ODP[02]: information for which agreements and procedures are to be**
2884 **established is defined (if selected).**

2885 **A.03.17.01E:** agreements and procedures are established with entities involved in
2886 the supply chain for the system, system components, or system service for
2887 **<A.03.17.01E.ODP[01]: SELECTED PARAMETER VALUE(S)>.**

2888 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2889 **Examine**

2890 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
2891 risk management plan; system and services acquisition policy; acquisition contracts
2892 for the system, system component, or system service; procedures addressing supply
2893 chain protection; acquisition documentation; service-level agreements; system
2894 security plan; inter-organizational agreements and procedures; other relevant
2895 documents or records].

2896 **Interview**

2897 [SELECT FROM: Personnel with system and service acquisition responsibilities;
2898 personnel with information security responsibilities; personnel with supply chain risk
2899 management responsibilities].

2900 **Test**

2901 [SELECT FROM: Processes for establishing inter-organizational agreements and
2902 procedures with supply chain entities].

2903 **REFERENCES**

2904 Source Assessment Procedure: [SR-08](#)

2905 **03.17.02E Inspection of Systems or Components**

2906 **ASSESSMENT OBJECTIVE**

2907 *Determine if:*

2908 **A.03.17.02E.ODP[01]: systems or system components that require inspection are**
2909 **defined.**

2910 **A.03.17.02E.ODP[02]: one or more of the following PARAMETER VALUES is/are**
2911 **selected: {at random; <A.03.17.02E.ODP[03]: frequency>; upon**
2912 **<A.03.17.02E.ODP[04]: indications of the need for inspection>}**.

2913 **A.03.17.02E.ODP[03]: the frequency at which to inspect systems or system**
2914 **components is defined (if selected).**

2915 **A.03.17.02E.ODP[04]: indications of the need for an inspection of systems or**
2916 **system components are defined (if selected).**

2917 **A.03.17.02E: <A.03.17.02E.ODP[01]: systems or system components>** are inspected
2918 **<A.03.17.02E.ODP[02]: SELECTED PARAMETER VALUE(S)>** to detect tampering.

2919 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2920 **Examine**

2921 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
2922 risk management plan; system and services acquisition policy; records of random
2923 inspections; inspection reports or results; assessment reports or results; acquisition
2924 documentation; acquisition contracts for the system, system component, or system
2925 service; inter-organizational agreements and procedures; system security plan;
2926 service-level agreements; other relevant documents or records].

2927 **Interview**

2928 [SELECT FROM: Personnel with system and services acquisition responsibilities;
2929 personnel with information security responsibilities; personnel with supply chain risk
2930 management responsibilities].

2931 **Test**

2932 [SELECT FROM: Processes for establishing inter-organizational agreements and
2933 procedures with supply chain entities; processes to inspect for tampering].

2934 **REFERENCES**

2935 Source Assessment Procedure: [SR-10](#)

2936 **03.17.03E Component Authenticity**

2937 **ASSESSMENT OBJECTIVE**

2938 *Determine if:*

2939 **A.03.17.03E.ODP[01]: one or more of the following PARAMETER VALUES is/are**
2940 **selected: {source of counterfeit component; <A.03.17.03E.ODP[02]: external**
2941 **reporting organizations>; <A.03.17.03E.ODP[03]: personnel or roles>}.**

2942 **A.03.17.03E.ODP[02]: external reporting organizations to whom counterfeit**
2943 **system components are to be reported are defined (if selected).**

2944 **A.03.17.03E.ODP[03]: personnel or roles to whom counterfeit system components**
2945 **are to be reported are defined (if selected).**

2946 **A.03.17.03E.a[01]:** an anti-counterfeit policy is developed and implemented.

2947 **A.03.17.03E.a[02]:** anti-counterfeit procedures are developed and implemented.

2948 **A.03.17.03E.a[03]:** the anti-counterfeit policy and procedures include the means to
2949 detect counterfeit components entering the system.

2950 **A.03.17.03E.a[04]**: the anti-counterfeit policy and procedures include the means to
2951 prevent counterfeit components from entering the system.

2952 **A.03.17.03E.b**: counterfeit system components are reported to
2953 **<A.03.17.03E.ODP[01]: SELECTED PARAMETER VALUE(S)>**.

2954 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2955 **Examine**

2956 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
2957 risk management plan; system and services acquisition policy; anti-counterfeit plan;
2958 anti-counterfeit policy and procedures; media disposal policy; media protection
2959 policy; incident response policy; reports notifying developers, manufacturers,
2960 vendors, contractors, and/or external reporting organizations of counterfeit system
2961 components; acquisition documentation; service-level agreements; acquisition
2962 contracts for the system, system component, or system service; inter-organizational
2963 agreements and procedures; records of reported counterfeit system components;
2964 system security plan; other relevant documents or records].

2965 **Interview**

2966 [SELECT FROM: Personnel with system and service acquisition responsibilities;
2967 personnel with information security responsibilities; personnel with supply chain risk
2968 management responsibilities; personnel with responsibilities for anti-counterfeit
2969 policies, procedures, and reporting].

2970 **Test**

2971 [SELECT FROM: Processes for counterfeit prevention, detection, and reporting;
2972 mechanisms supporting and/or implementing anti-counterfeit detection,
2973 prevention, and reporting].

2974 **REFERENCES**

2975 Source Assessment Procedure: [SR-11](#)

2976 **03.17.04E Provenance**

2977 **ASSESSMENT OBJECTIVE**

2978 *Determine if:*

2979 **A.03.17.04E.ODP[01]: *systems, system components, and associated CUI that***
2980 ***require valid provenance are defined.***

2981 **A.03.17.04E[01]: valid provenance is documented *for <A.03.17.04E.ODP[01]:***
2982 ***systems, system components, and associated CUI>*.**

2983 **A.03.17.04E[02]: valid provenance is monitored *for <A.03.17.04E.ODP[01]: systems,***
2984 ***system components, and associated CUI>*.**

2985 **A.03.17.04E[03]:** valid provenance is maintained for **<A.03.17.04E.ODP[01]:**
2986 **systems, system components, and associated CUI>**.

2987

2988 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

2989 **Examine**

2990 [SELECT FROM: Supply chain risk management policy; supply chain risk management
2991 procedures; supply chain risk management plan; documentation of critical systems,
2992 critical system components, and associated data; documentation showing the
2993 history of ownership, custody, and location of and changes to critical systems or
2994 critical system components; system architecture; inter-organizational agreements
2995 and procedures; contracts; system security plan; other relevant documents or
2996 records].

2997 **Interview**

2998 [SELECT FROM: Organizational personnel with acquisition responsibilities;
2999 organizational personnel with information security responsibilities; organizational
3000 personnel with supply chain risk management responsibilities].

3001 **Test**

3002 [SELECT FROM: Organizational processes for identifying the provenance of critical
3003 systems and critical system components; mechanisms used to document, monitor,
3004 or maintain provenance].

3005 **REFERENCES**

3006 Source Assessment Procedure: [SR-04](#)

3007 **03.17.05E Supply Chain Integrity – Pedigree**

3008 **ASSESSMENT OBJECTIVE**

3009 *Determine if:*

3010 **A.03.17.05E.ODP[01]:** *safeguards employed to ensure the integrity of the system*
3011 *and system component are defined.*

3012 **A.03.17.05E.ODP[02]:** *an analysis method to be conducted to validate the internal*
3013 *composition and provenance of critical or mission-essential technologies, products,*
3014 *and services to ensure the integrity of the system and system component is*
3015 *defined.*

3016 **A.03.17.05E[01]:** **<A.03.17.05E.ODP[01]:** *safeguards***>** are employed to ensure the
3017 integrity of the system and system components.

3018 **A.03.17.05E[02]:** **<A.03.17.05E.ODP[02]:** *analysis method***>** is conducted to ensure
3019 the integrity of the system and system components.

3020 **POTENTIAL ASSESSMENT METHODS AND OBJECTS**

3021 **Examine**

3022 [SELECT FROM: Supply chain risk management policy and procedures; supply chain
3023 risk management plan; system and services acquisition policy; procedures
3024 addressing supply chain protection; bill of materials for critical systems or system
3025 components; acquisition documentation; software identification tags; manufacturer
3026 declarations of platform attributes (e.g., serial numbers, hardware component
3027 inventory) and measurements (e.g., firmware hashes) that are tightly bound to the
3028 hardware itself; system security plan; other relevant documents or records].

3029 **Interview**

3030 [[SELECT FROM: Organizational personnel with system and services acquisition
3031 responsibilities; organizational personnel with information security responsibilities;
3032 organizational personnel with supply chain risk management responsibilities].

3033 **Test**

3034 [SELECT FROM: Organizational processes for identifying pedigree information;
3035 organizational processes to determine and validate the integrity of the internal
3036 composition of critical systems and critical system components; mechanisms to
3037 determine and validate the integrity of the internal composition of critical systems
3038 and critical system components].

3039 **REFERENCES**

3040 Source Assessment Procedure: [SR-04\(04\)](#)

3041 **References**

- 3042 [1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available
3043 at <https://www.govinfo.gov/app/details/PLAW-113publ283>
- 3044 [2] Office of Management and Budget Memorandum Circular A-130, Managing Information as
3045 a Strategic Resource, July 2016. Available at [https://www.whitehouse.gov/wp-](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)
3046 [content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf](https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf)
- 3047 [3] Ross RS, Pillitteri VY (2024) Enhanced Security Requirements for Protecting Controlled
3048 Unclassified Information. (National Institute of Standards and Technology, Gaithersburg,
3049 MD), NIST Special Publication (SP) NIST SP 800-172r3 ipd.
3050 <https://doi.org/10.6028/NIST.SP.800-172r3.ipd>
- 3051 [4] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:
3052 Organization, Mission, and Information System View. (National Institute of Standards and
3053 Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39.
3054 <https://doi.org/10.6028/NIST.SP.800-39>
- 3055 [5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and
3056 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
3057 Special Publication (SP) NIST SP 800-53Ar5. <https://doi.org/10.6028/NIST.SP.800-53Ar5>
- 3058 [6] International Organization for Standardization/International Electrotechnical Commission
3059 15408-3:2017, Information technology — Security techniques — Evaluation criteria for IT
3060 security — Part 3: Security assurance requirements, April 2017. Available at
3061 <https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf>
- 3062 [7] National Institute of Standards and Technology (2019) Security Requirements for
3063 Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal
3064 Information Processing Standards Publication (FIPS) NIST FIPS 140-3.
3065 <https://doi.org/10.6028/NIST.FIPS.140-3>
- 3066 [8] Committee on National Security Systems (2022) Committee on National Security Systems
3067 (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS Instruction
3068 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- 3069 [9] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House, 2340
3070 Washington, DC), DCPD-201000942, November 4, 2010. Available at
3071 <https://www.govinfo.gov/app/details/DCPD-201000942>

3072	Appendix A. Acronyms
3073	CNSS
3074	Committee on National Security Systems
3075	CUI
3076	Controlled Unclassified Information
3077	FIPS
3078	Federal Information Processing Standards
3079	FISMA
3080	Federal Information Security Modernization Act
3081	FOIA
3082	Freedom of Information Act
3083	ITL
3084	Information Technology Laboratory
3085	GRC
3086	Governance, Risk, and Compliance
3087	NIST
3088	National Institute of Standards and Technology
3089	ODP
3090	Organization-Defined Parameter
3091	OMB
3092	Office of Management and Budget
3093	OSCAL
3094	Open Security Controls Assessment Language

3095 **Appendix B. Glossary**

3096 Appendix B provides definitions for the terminology used in SP 800-172A. The definitions are
3097 consistent with the definitions contained in the Committee on National Security Systems (CNSS)
3098 Glossary [8] unless otherwise noted.

3099 **agency**

3100 Any executive agency or department, military department, Federal Government corporation, Federal Government-
3101 controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any
3102 independent regulatory agency. [2]

3103 **assessment**

3104 See *security control assessment*.

3105 **assessor**

3106 See *security control assessor*.

3107 **controlled unclassified information**

3108 Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating
3109 controls, excluding information that is classified under Executive Order 13526, Classified National Security
3110 Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as
3111 amended. [9]

3112 **information**

3113 Any communication or representation of knowledge such as facts, data, or opinions in any medium or form,
3114 including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [2]

3115 **information system**

3116 A discrete set of information resources organized for the collection, processing, maintenance, use, sharing,
3117 dissemination, or disposition of information. [2]

3118 **nonfederal organization**

3119 An entity that owns, operates, or maintains a nonfederal system.

3120 **nonfederal system**

3121 A system that does not meet the criteria for a federal system.

3122 **risk**

3123 A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a
3124 function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and
3125 (ii) the likelihood of occurrence. [2]

3126 **security**

3127 A condition that results from the establishment and maintenance of protective measures that enable an
3128 organization to perform its mission or critical functions despite risks posed by threats to its use of systems.
3129 Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and
3130 correction that should form part of the organization's risk management approach. [8]

3131 **security assessment**

3132 See *security control assessment*.

3133 **security control**

3134 The safeguards or countermeasures prescribed for an information system or an organization to protect the
3135 confidentiality, integrity, and availability of the system and its information. [2]

3136 **security control assessment**

3137 The testing or evaluation of security controls to determine the extent to which the controls are implemented
3138 correctly, operating as intended, and producing the desired outcome with respect to meeting the security
3139 requirements for an information system or organization. [2]

3140 **system**

3141 See *information system*.

3142 **system security plan**

3143 A document that describes how an organization meets or plans to meet the security requirements for a system. In
3144 particular, the system security plan describes the system boundary, the environment in which the system
3145 operates, how the security requirements are satisfied, and the relationships with or connections to other systems.

3146 **Appendix C. Summary of Enhanced Security Requirements**

3147 Table 2 provides a consolidated list of the enhanced security requirements in SP 800-172 [3].

3148 **Table 2. Enhanced security requirements**

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Access Control	
03.01.01E	Dual Authorization
03.01.02E	Non-Organizationally Owned Systems Restricted Use
03.01.03E	Withdrawn
03.01.04E	Concurrent Session Control
03.01.05E	Remote Access Monitoring and Control
03.01.06E	Protection of Remote Access Mechanism Information
03.01.07E	Automated Audit Actions for Account Management
03.01.08E	Account Monitoring for Atypical Usage
03.01.09E	Attribute-Based Access Control
03.01.10E	Object Security Attributes
03.01.11E	Role-Based Access Control
03.01.12E	Physical or Logical Separation of CUI Flows
03.01.13E	Metadata
03.01.14E	Security Policy Filters
03.01.15E	Data Type Identifiers
03.01.16E	Decomposition Into Policy-Relevant Subcomponents
03.01.17E	Detection of Unsanctioned Information
Awareness and Training	
03.02.01E	Advanced Literacy and Awareness Training
03.02.02E	Literacy and Awareness Training Practical Exercises
03.02.03E	Literacy and Awareness Training Feedback
03.02.04E	Anti-Counterfeit Training
Audit and Accountability	
03.03.01E	Protection of Audit Record Storage in Separate Physical Systems or Components
03.03.02E	Real-Time Alerts for Audit Processing Failures
03.03.03E	Dual Authorization for Audit Information and Actions
03.03.04E	Integrated Analysis of Audit Records
Configuration Management	
03.04.01E	Withdrawn
03.04.02E	Automated Unauthorized Component Detection
03.04.03E	Automation Maintenance for System Component Inventory
03.04.04E	Automation Support for Baseline Configuration
03.04.05E	Dual Authorization for System Changes
03.04.06E	Retention of Previous Configurations
03.04.07E	Testing, Validation, and Documentation of Changes
03.04.08E	Centralized Repository

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Identification and Authentication	
03.05.01E	Cryptographic Bidirectional Authentication
03.05.02E	Password Managers
03.05.03E	Device Attestation
03.05.04E	No Embedded Unencrypted Static Authenticators
03.05.05E	Expiration of Cached Authenticators
03.05.06E	Identity Proofing
03.05.07E	Identity Providers and Authentication Servers
Incident Response	
03.06.01E	Security Operations Center
03.06.02E	Integrated Incident Response Team
03.06.03E	Behavior Analysis
03.06.04E	Automated Tracking, Data Collection, and Analysis for Incident Reporting
Maintenance	
03.07.01E	Software Updates and Patches for Maintenance Tools
Media Protection	
03.08.01E	Dual Authorization for Media Sanitization
03.08.02E	Dual Authorization for System Backup Deletion and Destruction
03.08.03E	Testing System Backups for Reliability and Integrity
03.08.04E	System Recovery and Reconstitution
Personnel Security	
03.09.01E	Withdrawn
03.09.02E	Withdrawn
03.09.03E	Access Agreements
03.09.04E	Citizenship Requirements
Physical Protection	
03.10.01E	Intrusion Alarms and Surveillance Equipment
03.10.02E	Delivery and Removal of System Components
Risk Assessment	
03.11.01E	Threat Awareness Program
03.11.02E	Threat Hunting
03.11.03E	Predictive Cyber Analytics
03.11.04E	Withdrawn
03.11.05E	Withdrawn
03.11.06E	Withdrawn
03.11.07E	Withdrawn
03.11.08E	Dynamic Threat Awareness
03.11.09E	Indicators of Compromise
03.11.10E	Criticality Analysis
03.11.11E	Discoverable Information
03.11.12E	Automated Means for Sharing Threat Intelligence

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
Security Assessment and Monitoring	
03.12.01E	Penetration Testing
03.12.02E	Independent Assessors
03.12.03E	Risk Monitoring
03.12.04E	Internal System Connections
System and Communications Protection	
03.13.01E	Heterogeneity
03.13.02E	Randomness
03.13.03E	Concealment and Misdirection
03.13.04E	Isolation of System Components
03.13.05E	Change Processing and Storage Locations
03.13.06E	Platform-Independent Applications
03.13.07E	Virtualization Techniques
03.13.08E	Decoys
03.13.09E	Isolation of Security Tool, Mechanism, and Support Components Isolation
03.13.10E	Separate Subnetworks
03.13.11E	Thin Nodes
03.13.12E	Denial-of-Service Protection
03.13.13E	Port and Input/Output Device Access
03.13.14E	Detonation Chambers
03.14.15E	Separate Subnets to Isolate System Components and Functions
03.14.16E	System Partitioning
System and Information Integrity	
03.14.01E	Software, Firmware, and Information Integrity
03.14.02E	Withdrawn
03.14.03E	Withdrawn
03.14.04E	Refresh from Trusted Sources
03.14.05E	Non-Persistent Information
03.14.06E	Withdrawn
03.14.07E	Withdrawn
03.14.08E	Integrity Checks
03.14.09E	Cryptographic Protection
03.14.10E	Protection of Boot Firmware
03.14.11E	Integration of Detection and Response
03.14.12E	Information Input Validation
03.14.13E	Error Handling
03.14.14E	Memory Protection
03.14.15E	Non-Persistent System Components and Services
03.14.16E	Tainting
03.14.17E	System-Generated Alerts
03.14.18E	Automated Organization-Generated Alerts
Planning	

REQUIREMENT NUMBER	ENHANCED SECURITY REQUIREMENT
03.15.01E	Security Architecture
03.15.02E	Defense In Depth
03.15.03E	Supplier Diversity
System and Services Acquisition	
03.16.01E	Specialization
Supply Chain Risk Management	
03.17.01E	Notification Agreements
03.17.02E	Inspection of Systems or Components
03.17.03E	Component Authenticity
03.17.04E	Provenance
03.17.05E	Supply Chain Integrity – Pedigree

3149

3150 **Appendix D. Security Requirement Assessments**

3151 This appendix provides an overview of the process for assessing the security requirements in SP
3152 800-172 [3]. The four-phase process is based on the methodology in SP 800-53A [5]⁵ and
3153 includes:

- 3154 1. Preparing for assessments
- 3155 2. Developing assessment plans
- 3156 3. Conducting assessments
- 3157 4. Analyzing, documenting, and reporting assessment results

3158 **D.1. Preparing for Assessments**

3159 Thorough preparation by the organization and assessors is an important aspect of conducting
3160 an effective assessment. Preparatory activities address a range of issues related to the cost,
3161 schedule, and conduct of the assessment. From an organizational perspective, preparing for an
3162 assessment includes the following activities:

- 3163 • Ensuring that appropriate policies that cover the assessment are in place and
3164 understood by affected organizational elements
- 3165 • Establishing the objective and scope of the assessment (i.e., the purpose of the
3166 assessment and what is being assessed)
- 3167 • Notifying appropriate organizational officials of the impending assessment and
3168 allocating the necessary resources to carry out the assessment
- 3169 • Establishing appropriate communication channels among organizational officials with an
3170 interest in the assessment
- 3171 • Establishing the time frame for completing the assessment and the key milestone
3172 decision points required by the organization
- 3173 • Identifying and selecting the assessors who will be responsible for conducting the
3174 assessment and considering issues of assessor independence
- 3175 • Providing artifacts to the assessors (e.g., policies, procedures, plans, specifications,
3176 designs, records, administrator/operator manuals, information exchange agreements,
3177 system documentation, previous assessment results, legal requirements)
- 3178 • Establishing a mechanism between the organization and the assessors to minimize
3179 ambiguities or misunderstandings about the security requirements, implementation
3180 issues, and deficiencies identified during the assessment

⁵ For additional detail and guidance, see SP 800-53A [5], Section 3.

- 3181 Assessors begin preparing for the assessment by:
- 3182 • Developing a general understanding of the organization’s operations and how the scope
3183 of the assessment supports those organizational operations
 - 3184 • Understanding the structure of the system (i.e., the system architecture) and the
3185 security requirements being assessed
 - 3186 • Meeting with organizational officials to ensure that there is a common understanding of
3187 the assessment objectives and the proposed rigor and scope of the assessment
 - 3188 • Obtaining the artifacts needed for the assessment (e.g., policies, procedures, plans,
3189 specifications, administrator/operator manuals, system documentation, information
3190 exchange agreements, designs, records, previous assessment results⁶)
 - 3191 • Establishing organizational points of contact to carry out the assessment

3192 Table 3 provides a summary of the purpose and expected outcomes of the *assessment*
3193 *preparation phase*.

3194 **Table 3. Summary of assessment preparation phase**

PURPOSE	Address a range of issues pertaining to the cost, schedule, scope, and conduct of the assessment.
OUTCOMES	<ul style="list-style-type: none"> • The objective, scope, and time frame of the assessment are determined. • Key organizational stakeholders are notified, and the necessary resources are allocated. • Assessors are identified and selected. • Artifacts are collected and provided to assessors. • Mechanisms to minimize ambiguities and misunderstandings about the security requirements, implementation issues, and weaknesses/deficiencies identified during the assessment are established. • The organization’s operations, structure, objective, scope, and time frame of assessment are understood by assessors.

3195 **D.2. Developing Assessment Plans**

3196 The assessment plan establishes the objectives for the security requirement assessment and a
3197 detailed roadmap of how to conduct the assessment based on the system security plan. The
3198 following steps are considered by assessors when developing an assessment plan:

- 3199 • Determine which security requirements are to be included in the assessment based on
3200 the contents of the system security plan and the purpose and scope of the assessment.
- 3201 • Select the appropriate assessment procedures.

⁶ Previous assessment results that may be reused for the current assessment include Inspector General reports, audits, vulnerability scans, physical security inspections, developmental testing and evaluation, vendor flaw remediation activities, and ISO 15408 [6] evaluations.

- 3202 • Tailor the selected assessment procedures (i.e., select appropriate POTENTIAL
3203 ASSESSMENT METHODS AND OBJECTS, and assign depth and coverage attribute
3204 values).⁷
- 3205 • Optimize the assessment procedures to reduce the duplication of effort (e.g., sequence
3206 and consolidate assessment procedures) and provide a cost-effective assessment
3207 solution.
- 3208 • Finalize the assessment plan, and obtain the necessary approvals to execute the plan.

3209 Table 4 provides a summary of the purpose and expected outcomes of the *assessment plan*
3210 *development phase*.

3211 **Table 4. Summary of assessment plan development phase**

PURPOSE	Establish the objectives for the security requirement assessment and a detailed roadmap of how to conduct the assessment based on the system security plan.
OUTCOMES	<ul style="list-style-type: none"> • Security requirements to be included in the assessment are determined. • Assessment procedures are selected and tailored. • Assessment procedures are optimized to reduce the duplication of effort. • The assessment plan is finalized, and organizational approvals are obtained.

3212 **D.3. Conducting Assessments**

3213 After the assessment plan is approved by the organization, the assessors execute the plan in
3214 accordance with the agreed-upon schedule. Assessment objectives are achieved by applying
3215 the designated assessment methods to selected assessment objects and compiling or producing
3216 the evidence necessary to make the determination associated with each assessment objective.
3217 Each determination statement contained within an assessment procedure executed by an
3218 assessor produces one of the following findings:

- 3219 • Satisfied
- 3220 or
- 3221 • Other than satisfied

3222 A finding of *satisfied* indicates that the assessment objective for the security requirement (or
3223 subset of the requirement) addressed by the determination statement has been met and
3224 produced an acceptable result. A finding of *other than satisfied* indicates that the assessment
3225 objective for the requirement has not been met and has produced an unacceptable result. A

⁷ In addition to selecting POTENTIAL ASSESSMENT METHODS AND OBJECTS, each assessment method (i.e., examine, interview, and test) is associated with depth and coverage attributes. The attribute values identify the rigor (depth) and scope (coverage) of the assessment procedures executed by the assessor. The depth and coverage attribute values are associated with the assurance requirements specified by the organization. SP 800-53A [5], Appendix D provides additional guidance on depth and coverage attributes.

3226 finding of *other than satisfied* may also indicate that the assessor was unable to obtain
3227 sufficient information to make the determination called for in the determination statement.

3228 Table 5 provides a summary of the purpose and expected outcomes of the *assessment*
3229 *execution phase*.

3230 **Table 5. Summary of assessment execution phase**

PURPOSE	Conduct the assessment in accordance with the assessment plan, and document the results in an assessment report.
OUTCOMES	<ul style="list-style-type: none"> • Security requirements are assessed in accordance with the assessment plan. • An assessment report that documents whether the security requirements have been satisfied is produced.

3231 **D.4. Analyzing, Documenting, and Reporting Assessment Results**

3232 The assessment report includes information from assessors in the form of findings that are
3233 necessary to determine whether the requirements in SP 800-172 [3] have been satisfied.⁸ The
3234 report conveys the results of the assessment to designated organizational officials. The report
3235 can also provide recommendations for correcting any deficiencies discovered during the
3236 assessment. Depending on the organization’s objective for the assessment, the assessment
3237 results can trigger a variety of risk response actions, including risk acceptance, risk mitigation,
3238 risk rejection, risk transfer, or risk sharing. The assessment results can also influence changes to
3239 the system security plan and plan of action and milestones.

3240 Table 6 provides a summary of the purpose and expected outcomes of the *assessment analysis,*
3241 *documentation, and reporting phase*.

3242 **Table 6. Summary of assessment analysis, documentation, and reporting phase**

PURPOSE	Analyze the risks that result from the weaknesses and deficiencies identified during the assessment, and determine an approach to respond to those risks in accordance with organizational priorities.
OUTCOMES	<ul style="list-style-type: none"> • Assessment findings are reviewed and analyzed. • Subsequent risk responses are initiated to manage risks. • The system security plan and plan of action and milestones are updated to reflect the results of the assessment and any subsequent risk response actions.

3243

⁸ SP 800-53A [5], Appendix E provides additional guidance on security assessment reports.

3244 **Appendix E. Organization-Defined Parameters**

3245 Table 7 lists the ODPs that are included in the assessment procedures in Sec. 3. The ODPs are
3246 listed sequentially by requirement family, beginning with the first requirement containing an
3247 ODP in the Access Control (AC) family and ending with the last requirement containing an ODP
3248 in the Supply Chain Risk Management (SR) family.

3249 **Table 7. Organization-defined parameters**

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.01E	A.03.01.01E.ODP[01]	<i>privileged commands and/or other actions requiring dual authorization are defined.</i>
03.01.02E	A.03.01.02E.ODP[01]	<i>restrictions on the use of non-organizationally owned systems or system components to process, store, or transmit CUI are defined.</i>
03.01.04E	A.03.01.04E.ODP[01]	<i>accounts and/or account types for which to limit the number of concurrent sessions is defined.</i>
03.01.04E	A.03.01.04E.ODP[02]	<i>the number of concurrent sessions to be allowed for each account and/or account type is defined.</i>
03.01.08E	A.03.01.08E.ODP[01]	<i>atypical usage for which to monitor system accounts is defined.</i>
03.01.08E	A.03.01.08E.ODP[02]	<i>personnel or roles to report atypical usage are defined.</i>
03.01.09E	A.03.01.09E.ODP[01]	<i>attributes to assume access permissions are defined.</i>
03.01.10E	A.03.01.10E.ODP[01]	<i>security attributes to be associated with information, source, and destination objects are defined.</i>
03.01.10E	A.03.01.10E.ODP[02]	<i>information objects to be associated with information security attributes are defined.</i>
03.01.10E	A.03.01.10E.ODP[03]	<i>source objects to be associated with information security attributes are defined.</i>
03.01.10E	A.03.01.10E.ODP[04]	<i>destination objects to be associated with information security attributes are defined.</i>
03.01.10E	A.03.01.10E.ODP[05]	<i>information flow control policies as a basis for the enforcement of flow control decisions are defined.</i>
03.01.11E	A.03.01.11E.ODP[01]	<i>roles and users authorized to assume such roles are defined.</i>
03.01.12E	A.03.01.12E.ODP[01]	<i>mechanisms and/or techniques to separate CUI flows are defined.</i>
03.01.13E	A.03.01.13E.ODP[01]	<i>metadata that requires flow control is defined.</i>
03.01.14E	A.03.01.14E.ODP[01]	<i>security policy filers are defined.</i>
03.01.14E	A.03.01.14E.ODP[02]	<i>information flows are defined.</i>
03.01.14E	A.03.01.14E.ODP[03]	<i>one or more of the following PARAMETER VALUES is/are selected: {Block; Strip; Modify; Quarantine} in response to a filter processing failure.</i>
03.01.14E	A.03.01.14E.ODP[04]	<i>security policy addressing a filter processing failure is defined.</i>
03.01.15E	A.03.01.15E.ODP[01]	<i>data type identifiers are defined.</i>
03.01.16E	A.03.01.16E.ODP[01]	<i>policy-relevant subcomponents into which to decompose information for submission to policy enforcement mechanisms are defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.01.17E	A.03.01.17E.ODP[01]	<i>unsanctioned information to be detected is defined.</i>
03.01.17E	A.03.01.17E.ODP[02]	<i>a security policy that prohibits the transfer of such information is defined.</i>
03.02.01E	A.03.02.01E.ODP[01]	<i>indicators of malicious code are defined.</i>
03.02.01E	A.03.02.01E.ODP[02]	<i>the frequency at which to update security literacy training content is defined.</i>
03.02.01E	A.03.02.01E.ODP[03]	<i>events which cause security literacy training content to be updated are defined.</i>
03.02.03E	A.03.02.03E.ODP[01]	<i>personnel to whom feedback on organizational training results will be provided are assigned.</i>
03.02.04E	A.03.02.04E.ODP[01]	<i>personnel or roles requiring training to detect counterfeit system components are defined.</i>
03.03.02E	A.03.03.02E.ODP[01]	<i>real-time period requiring alerts when audit failure events (defined in A.03.03.02E.ODP[03]) occur is defined.</i>
03.03.02E	A.03.03.02E.ODP[02]	<i>personnel, roles, and/or locations to be alerted in real time when audit failure events (defined in A.03.03.02E.ODP[03]) occur are defined.</i>
03.03.02E	A.03.03.02E.ODP[03]	<i>audit logging failure events requiring real-time alerts are defined.</i>
03.03.03E	A.03.03.03E.ODP[01]	<i>one or more of the following PARAMETER VALUES is/are selected: {movement; deletion}.</i>
03.03.03E	A.03.03.03E.ODP[02]	<i>audit information for which dual authorization is to be enforced is defined.</i>
03.03.04E	A.03.03.04E.ODP[01]	<i>one or more of the following PARAMETER VALUES is/are selected: {vulnerability scanning information; performance data; system monitoring information; <A.03.03.04E.ODP[02] data/information collected from other sources>}.</i>
03.03.04E	A.03.03.04E.ODP[02]	<i>data or information collected from other sources to be analyzed is defined (if selected).</i>
03.04.02E	A.03.04.02E.ODP[01]	<i>automated mechanisms used to detect the presence of unauthorized or misconfigured system components are defined.</i>
03.04.02E	A.03.04.02E.ODP[02]	<i>one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized or misconfigured system components; isolate unauthorized or misconfigured system components; notify <A.03.04.02E.ODP[03] personnel or roles>}.</i>
03.04.02E	A.03.04.02E.ODP[03]	<i>personnel or roles to be notified when unauthorized or misconfigured system components are detected are defined (if selected).</i>
03.04.03E	A.03.04.03E.ODP[01]	<i>automated mechanisms used to maintain the currency of the system component inventory are defined.</i>
03.04.03E	A.03.04.03E.ODP[02]	<i>automated mechanisms used to maintain the completeness of the system component inventory are defined.</i>
03.04.03E	A.03.04.03E.ODP[03]	<i>automated mechanisms used to maintain the accuracy of the system component inventory are defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.04.03E	A.03.04.03E.ODP[04]	<i>automated mechanisms used to maintain the availability of the system component inventory are defined.</i>
03.04.04E	A.03.04.04E.ODP[01]	<i>automated mechanisms used to maintain the currency of the baseline configuration of the system are defined.</i>
03.04.04E	A.03.04.04E.ODP[02]	<i>automated mechanisms used to maintain the completeness of the baseline configuration of the system are defined.</i>
03.04.04E	A.03.04.04E.ODP[03]	<i>automated mechanisms used to maintain the accuracy of the baseline configuration of the system are defined.</i>
03.04.04E	A.03.04.04E.ODP[04]	<i>automated mechanisms used to maintain the availability of the baseline configuration of the system are defined.</i>
03.04.05E	A.03.04.05E.ODP[01]	<i>system components requiring dual authorization for changes are defined.</i>
03.04.05E	A.03.04.05E.ODP[02]	<i>system-level information requiring dual authorization for changes is defined.</i>
03.04.06E	A.03.04.06E.ODP[01]	<i>the number of previous baseline configuration versions to be retained is defined.</i>
03.05.01E	A.03.05.01E.ODP[01]	<i>devices and/or types of devices requiring the use of cryptographically based bidirectional authentication to authenticate before establishing a system connection are defined.</i>
03.05.02E	A.03.05.02E.ODP[01]	<i>password managers employed for generating and managing passwords are defined.</i>
03.05.03E	A.03.05.03E.ODP[01]	<i>the configuration management process to be implemented to handle device identification and authentication based on attestation is defined.</i>
03.05.05E	A.03.05.05E.ODP[01]	<i>the time period after which the use of cached authenticators is prohibited is defined.</i>
03.05.07E	A.03.05.07E.ODP[01]	<i>an identification and authentication policy is defined.</i>
03.05.07E	A.03.05.07E.ODP[02]	<i>mechanisms supporting authentication and authorization decisions are defined.</i>
03.06.02E	A.03.06.02E.ODP[01]	<i>the time period within which an integrated incident response team can be deployed is defined.</i>
03.06.03E	A.03.06.03E.ODP[01]	<i>environments or resources that may contain or be related to anomalous or suspected adversarial behavior are defined.</i>
03.06.04E	A.03.06.04E.ODP[01]	<i>automated mechanisms used to track incidents are defined.</i>
03.06.04E	A.03.06.04E.ODP[02]	<i>automated mechanisms used to collect incident information are defined.</i>
03.06.04E	A.03.06.04E.ODP[03]	<i>automated mechanisms used to analyze incident information are defined.</i>
03.08.01E	A.03.08.01E.ODP[01]	<i>system media to be sanitized using dual authorization is defined.</i>
03.08.02E	A.03.08.02E.ODP[01]	<i>backup information for which to enforce dual authorization in order to delete or destroy is defined.</i>
03.08.03E	A.03.08.03E.ODP[01]	<i>the frequency at which to test backup information for media reliability is defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.08.03E	A.03.08.03E.ODP[02]	<i>the frequency at which to test backup information for information integrity is defined.</i>
03.08.04E	A.03.08.04E.ODP[01]	<i>a time period consistent with recovery time and recovery point objectives for the recovery of the system is determined.</i>
03.08.04E	A.03.08.04E.ODP[02]	<i>a time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined.</i>
03.09.03E	A.03.09.03E.ODP[01]	<i>the frequency at which to review and update access agreements is defined.</i>
03.09.03E	A.03.09.03E.ODP[02]	<i>the frequency at which to re-sign access agreements to maintain access systems processing, storing, or transmitting CUI is defined.</i>
03.09.04E	A.03.09.04E.ODP[01]	<i>Citizenship requirements to be met by individuals to access a system processing, storing, or transmitting CUI are defined.</i>
03.10.01E	A.03.10.01E.ODP[01]	<i>the time period for which to maintain visitor access records for the facility in which the system resides is defined.</i>
03.10.02E	A.03.10.02E.ODP[01]	<i>the types of system components to be authorized and controlled when entering the facility are defined.</i>
03.10.02E	A.03.10.02E.ODP[02]	<i>the types of system components to be authorized and controlled when exiting the facility are defined.</i>
03.11.02E	A.03.11.02E.ODP[01]	<i>the frequency at which to implement the threat-hunting capability is defined.</i>
03.11.03E	A.03.11.03E.ODP[01]	<i>advanced automation capabilities to predict and identify risks are defined.</i>
03.11.03E	A.03.11.03E.ODP[02]	<i>systems or system components in which advanced automation and analytics capabilities are to be employed are defined.</i>
03.11.03E	A.03.11.03E.ODP[03]	<i>advanced analytics capabilities to predict and identify risks are defined.</i>
03.11.08E	A.03.11.08E.ODP[01]	<i>the means to determine the current cyber threat environment on an ongoing basis are defined.</i>
03.11.09E	A.03.11.09E.ODP[01]	<i>sources that provide indicators of compromise are defined.</i>
03.11.09E	A.03.11.09E.ODP[02]	<i>personnel or roles to whom indicators of compromise are to be distributed are defined.</i>
03.11.10E	A.03.11.10E.ODP[01]	<i>systems, system components, or system services to be analyzed for criticality are defined.</i>
03.11.10E	A.03.11.10E.ODP[02]	<i>decision points in the system development life cycle when a criticality analysis is to be performed are defined.</i>
03.11.11E	A.03.11.11E.ODP[01]	<i>corrective actions to be taken if information about the system is discoverable are defined.</i>
03.12.01E	A.03.12.01E.ODP[01]	<i>the frequency at which to conduct penetration testing on systems or system components is defined.</i>
03.12.01E	A.03.12.01E.ODP[02]	<i>systems or system components on which penetration testing is to be conducted are defined.</i>
03.12.04E	A.03.12.04E.ODP[01]	<i>system components or classes of components requiring internal connections to the system are defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.12.04E	A.03.12.04E.ODP[02]	<i>conditions requiring the termination of internal connections are defined.</i>
03.12.04E	A.03.12.04E.ODP[03]	<i>the frequency at which to review the continued need for each internal connection is defined.</i>
03.13.01E	A.03.13.01E.ODP[01]	<i>system components requiring a diverse set of information technologies to be used in the implementation of the system are defined.</i>
03.13.02E	A.03.13.02E.ODP[01]	<i>the techniques employed to introduce randomness into organizational operations and assets are defined.</i>
03.13.03E	A.03.13.03E.ODP[01]	<i>the concealment and misdirection techniques used to confuse and mislead adversaries potentially targeting systems are defined.</i>
03.13.04E	A.03.13.04E.ODP[01]	<i>system components to be isolated by boundary protection mechanisms are defined.</i>
03.13.05E	A.03.13.05E.ODP[01]	<i>processing and/or storage locations to be changed are defined.</i>
03.13.05E	A.03.13.05E.ODP[02]	<i>one of the following PARAMETER VALUES is selected: {<A.03.13.05E.ODP[03] frequency>; at random time intervals}.</i>
03.13.05E	A.03.13.05E.ODP[03]	<i>the frequency at which to change the location of processing and/or storage is defined (if selected).</i>
03.13.06E	A.03.13.06E.ODP[01]	<i>platform-independent applications to be included within organizational systems are defined.</i>
03.13.07E	A.03.13.07E.ODP[01]	<i>the frequency at which to change the diversity of operating systems and applications deployed using virtualization techniques is defined.</i>
03.13.09E	A.03.13.09E.ODP[01]	<i>information security tools, mechanisms, and support components to be isolated from other internal system components are defined.</i>
03.13.11E	A.03.13.11E.ODP[01]	<i>system components to be implemented with minimal functionality and information storage are defined.</i>
03.13.12E	A.03.13.12E.ODP[01]	<i>the types of denial-of-service events to be protected against or limited are defined.</i>
03.13.12E	A.03.13.12E.ODP[02]	<i>one of the following PARAMETER VALUES is selected: {protected against; limited}.</i>
03.13.12E	A.03.13.12E.ODP[03]	<i>the safeguards to prevent the denial-of-service objective by type of denial-of-service event are defined.</i>
03.13.13E	A.03.13.13E.ODP[01]	<i>connection ports or input/output devices to be disabled or removed are defined.</i>
03.13.13E	A.03.13.13E.ODP[02]	<i>one of the following PARAMETER VALUES is selected: {physically; logically}.</i>
03.13.13E	A.03.13.13E.ODP[03]	<i>systems or system components with connection ports or input/output devices to be disabled or removed are defined.</i>
03.13.14E	A.03.13.14E.ODP[01]	<i>the system, system component, or location in which a detonation chamber capability is to be employed is defined.</i>
03.13.15E	A.03.13.15E.ODP[01]	<i>one of the following PARAMETER VALUES is selected: {physically; logically}.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.13.15E	A.03.13.15E.ODP[02]	<i>critical system components and functions to be isolated are defined.</i>
03.13.16E	A.03.13.16E.ODP[01]	<i>system components to reside in separate physical or logical domains or environments based on circumstances for the physical or logical separation of components are defined.</i>
03.13.16E	A.03.13.16E.ODP[02]	<i>one of the following PARAMETER VALUES is selected: {physical; logical}.</i>
03.13.16E	A.03.13.16E.ODP[03]	<i>circumstances for the physical or logical separation of components are defined.</i>
03.14.01E	A.03.14.01E.ODP[01]	<i>software requiring integrity verification tools to be used to detect unauthorized changes is defined.</i>
03.14.01E	A.03.14.01E.ODP[02]	<i>firmware requiring integrity verification tools to be used to detect unauthorized changes is defined.</i>
03.14.01E	A.03.14.01E.ODP[03]	<i>information requiring integrity verification tools to be used to detect unauthorized changes is defined.</i>
03.14.01E	A.03.14.01E.ODP[04]	<i>actions to be taken when unauthorized changes to software are detected are defined.</i>
03.14.01E	A.03.14.01E.ODP[05]	<i>actions to be taken when unauthorized changes to firmware are detected are defined.</i>
03.14.01E	A.03.14.01E.ODP[06]	<i>actions to be taken when unauthorized changes to information are detected are defined.</i>
03.14.04E	A.03.14.04E.ODP[01]	<i>trusted sources to obtain software and data for system component and service refreshes are defined.</i>
03.14.05E	A.03.14.05E.ODP[01]	<i>one of the following PARAMETER VALUES is selected: {refresh <A.03.14.05E_ODP[02] information> <A.03.14.05E_ODP[03] frequency>; generate <A.03.14.05E_ODP[04] information>}.</i>
03.14.05E	A.03.14.05E.ODP[02]	<i>the information to be refreshed is defined (if selected).</i>
03.14.05E	A.03.14.05E.ODP[03]	<i>the frequency at which to refresh information is defined (if selected).</i>
03.14.05E	A.03.14.05E.ODP[04]	<i>the information to be generated on demand is defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[01]	<i>software on which an integrity check is to be performed is defined.</i>
03.14.08E	A.03.14.08E.ODP[02]	<i>one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[03] transitional states or security-relevant events>; <A.03.14.08E.ODP[04] frequency>}.</i>
03.14.08E	A.03.14.08E.ODP[03]	<i>transitional states or security-relevant events requiring integrity checks (on software) are defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[04]	<i>the frequency at which to perform an integrity check (on software) is defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[05]	<i>firmware on which an integrity check is to be performed is defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.14.08E	A.03.14.08E.ODP[06]	<i>one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[07] transitional states or security-relevant events>; <A.03.14.08E.ODP[08] frequency>}.</i>
03.14.08E	A.03.14.08E.ODP[07]	<i>transitional states or security-relevant events requiring integrity checks (on firmware) are defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[08]	<i>the frequency at which to perform an integrity check (on firmware) is defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[09]	<i>information on which an integrity check is to be performed is defined.</i>
03.14.08E	A.03.14.08E.ODP[10]	<i>one or more of the following PARAMETER VALUES is/are selected: {at startup; at <A.03.14.08E.ODP[11] transitional states or security-relevant events>; <A.03.14.08E.ODP[12] frequency>}.</i>
03.14.08E	A.03.14.08E.ODP[11]	<i>transitional states or security-relevant events requiring integrity checks (of information) are defined (if selected).</i>
03.14.08E	A.03.14.08E.ODP[12]	<i>the frequency at which to perform an integrity check (of information) is defined (if selected).</i>
03.14.10E	A.03.14.10E.ODP[01]	<i>mechanisms to be implemented to protect the integrity of boot firmware in system components are defined.</i>
03.14.10E	A.03.14.10E.ODP[02]	<i>system components requiring mechanisms to protect the integrity of boot firmware are defined.</i>
03.14.11E	A.03.14.11E.ODP[01]	<i>security-relevant changes to the system are defined.</i>
03.14.12E	A.03.14.12E.ODP[01]	<i>information inputs to the system requiring validity checks are defined.</i>
03.14.13E	A.03.14.13E.ODP[01]	<i>personnel or roles to whom error messages are to be revealed are defined.</i>
03.14.14E	A.03.14.14E.ODP[01]	<i>safeguards to be implemented to protect the system memory from unauthorized code execution are defined.</i>
03.14.15E	A.03.14.15E.ODP[01]	<i>non-persistent system components and services to be implemented are defined.</i>
03.14.15E	A.03.14.15E.ODP[02]	<i>one or more of the following PARAMETER VALUES is/are selected: {upon end of session of use; <A.03.14.15E.ODP[03] frequency>}.</i>
03.14.15E	A.03.14.15E.ODP[03]	<i>the frequency at which to terminate non-persistent components and services that are initiated in a known state is defined (if selected).</i>
03.14.16E	A.03.14.16E.ODP[01]	<i>systems or system components with data or capabilities to be embedded are defined.</i>
03.14.17E	A.03.14.17E.ODP[01]	<i>personnel or roles to be alerted when indications of compromise or potential compromise occur are defined.</i>
03.14.17E	A.03.14.17E.ODP[02]	<i>compromise indicators are defined.</i>
03.14.18E	A.03.14.18E.ODP[01]	<i>personnel or roles to be alerted when indications of inappropriate or unusual activity with security implications occur are defined.</i>
03.14.18E	A.03.14.18E.ODP[02]	<i>automated mechanisms used to alert personnel or roles are defined.</i>
03.14.18E	A.03.14.18E.ODP[03]	<i>activities that trigger alerts to personnel or roles are defined.</i>

ENHANCED SECURITY REQUIREMENT	ORGANIZATION-DEFINED PARAMETER	
03.15.01E	A.03.15.01E.ODP[01]	<i>the frequency for reviewing and updating the security architecture to reflect changes in the enterprise architecture is defined.</i>
03.15.02E	A.03.15.02E.ODP[01]	<i>safeguards to be allocated to architectural layers and locations are defined.</i>
03.15.02E	A.03.15.02E.ODP[02]	<i>architectural layers and locations are defined.</i>
03.15.03E	A.03.15.03E.ODP[01]	<i>safeguards to be allocated to architectural layers and locations are defined.</i>
03.15.03E	A.03.15.03E.ODP[02]	<i>architectural layers and locations are defined.</i>
03.16.01E	A.03.16.01E.ODP[01]	<i>one or more of the following PARAMETER VALUES is/are selected: {design modification; augmentation; reconfiguration}.</i>
03.16.01E	A.03.16.01E.ODP[02]	<i>systems or system components supporting mission-essential services or functions are defined.</i>
03.17.01E	A.03.17.01E.ODP[01]	<i>one or more of the following PARAMETER VALUES is/are selected: {notification of supply chain compromises; results of assessments or audits; provision of <A.03.17.01E.ODP[02]: information>}.</i>
03.17.01E	A.03.17.01E.ODP[02]	<i>information for which agreements and procedures are to be established is defined (if selected).</i>
03.17.02E	A.03.17.02E.ODP[01]	<i>systems or system components that require inspection are defined.</i>
03.17.02E	A.03.17.02E.ODP[02]	<i>one or more of the following PARAMETER VALUES is/are selected: {at random; <A.03.17.02E.ODP[03]: frequency>; upon <A.03.17.02E.ODP[04]: indications of the need for inspection>}.</i>
03.17.02E	A.03.17.02E.ODP[03]	<i>the frequency at which to inspect systems or system components is defined (if selected).</i>
03.17.02E	A.03.17.02E.ODP[04]	<i>indications of the need for an inspection of systems or system components are defined (if selected).</i>
03.17.03E	A.03.17.03E.ODP[01]	<i>one or more of the following PARAMETER VALUES is/are selected: {source of counterfeit component; <A.03.17.03E.ODP[02]: external reporting organizations>; <A.03.17.03E.ODP[03]: personnel or roles>}.</i>
03.17.03E	A.03.17.03E.ODP[02]	<i>external reporting organizations to whom counterfeit system components are to be reported are defined (if selected).</i>
03.17.03E	A.03.17.03E.ODP[03]	<i>personnel or roles to whom counterfeit system components are to be reported are defined (if selected).</i>
03.17.04E	A.03.17.04E.ODP[01]	<i>systems, system components, and associated CUI that require valid provenance are defined.</i>
03.17.05E	A.03.17.05E.ODP[01]	<i>safeguards employed to ensure the integrity of the system and system component are defined.</i>
03.17.05E	A.03.17.05E.ODP[02]	<i>an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined.</i>

3251 **Appendix F. Change Log**

3252 This publication incorporates the following changes from the original edition (March 15, 2022):

- 3253 • The restructuring of the assessment procedure syntax to align with SP 800-53A [5]
- 3254 • The addition of assessment procedures for the new and revised enhanced security
3255 requirements in SP 800-172, Revision 3 [3]
- 3256 • The addition of a references section to provide source assessment procedures from SP
3257 800-53A [5]
- 3258 • A one-time change to the publication version number to align with SP 800-172, Revision
3259 3 [3]

3260