



**NIST Special Publication  
NIST SP 800-171Ar3 ipd**

# **Assessing 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.800-171Ar3.ipd>

**NIST Special Publication  
NIST SP 800-171Ar3 ipd**

# **Assessing 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.800-171Ar3.ipd>

November 2023



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

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

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

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

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

### **Authority**

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [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 (2023) Assessing Security Requirements for Controlled Unclassified Information and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171Ar3 ipd. <https://doi.org/10.6028/NIST.SP.800-171Ar3.ipd>

### **Author ORCID iDs**

Ron Ross: 0000-0002-1099-9757  
Victoria Pillitteri: 0000-0002-7446-7506

### **Public Comment Period**

November 9, 2023 – January 12, 2024

### **Submit Comments**

[800-171comments@list.nist.gov](mailto: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 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 and nonfederal organizations with assessment procedures and a  
6 methodology that can be employed to conduct assessments of the security requirements in NIST  
7 Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal*  
8 *Systems and Organizations*. The assessment procedures are flexible and can be customized to the  
9 needs of organizations and assessors. Security assessments can be conducted as independent,  
10 third-party assessments or as government-sponsored assessments. The assessments can also be  
11 applied with various degrees of rigor based on customer-defined depth and coverage attributes.  
12 The findings and evidence produced during the assessments can facilitate risk-based decisions by  
13 organizations related to the security requirements.

14 **Keywords**

15 assessment; assessment method; assessment object; assessment procedure; assurance; basic  
16 security requirement; controlled unclassified information; coverage; CUI registry; depth;  
17 Executive Order 13556; FISMA; NIST Special Publication 800-171; NIST Special Publication  
18 800-53A; nonfederal organization; nonfederal system; security assessment; security control.

19 **Reports on Computer Systems Technology**

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

30 **Audience**

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

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

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

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

47 **Note to Reviewers**

48 This update to NIST Special Publication (SP) 800-171A represents over one year of data  
49 collection, technical analysis, customer interaction, redesign, and development of the procedures  
50 for assessing the security requirements for Controlled Unclassified Information (CUI). Many  
51 trade-offs have been made to ensure that the assessment procedures have been stated clearly and  
52 concisely while also recognizing the specific needs of both federal and nonfederal organizations.  
53 The following significant changes have been made in the initial public draft (ipd) of NIST SP  
54 800-171A, Revision 3:

- 55 • The restructuring of the assessment procedure syntax to align with NIST SP 800-53A [5].
- 56 • The addition of a references section to provide source assessment procedures from NIST  
57 SP 800-53A [5].

58 There has also been a one-time change to the publication version number to align with NIST SP  
59 800-171, Revision 3 [3].

60 NIST is specifically interested in comments, feedback, and recommendations for the following  
61 topics:

- 62 • The alignment of the assessment procedures to NIST SP 800-53A [5].
- 63 • The use of organization-defined parameters (ODPs) in the assessment procedures.
- 64 • The ease-of-use of the assessment procedures in conducting assessments of the CUI  
65 security requirements.

66 Reviewers are encouraged to comment on all or parts of NIST SP 800-171A, Revision 3 ipd.  
67 NIST requests that all comments be submitted to [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov) by 11:59 p.m.  
68 Eastern Standard Time (EST) on **January 12, 2024**. Commenters are encouraged to use the  
69 comment template provided with the document announcement.

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

73 **Call for Patent Claims**

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

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

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

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

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

98 Such statements should be addressed to: [800-171comments@list.nist.gov](mailto:800-171comments@list.nist.gov)

99 **Table of Contents**

100 **1. Introduction**..... **1**

101 1.1. Purpose and Applicability ..... 1

102 1.2. Organization of This Publication ..... 1

103 **2. The Fundamentals**..... **3**

104 2.1. Assessment Procedures..... 3

105 2.2. Assurance Cases..... 5

106 **3. The Procedures**..... **7**

107 3.1. Access Control..... 7

108 3.1.1. Account Management..... 7

109 3.1.2. Access Enforcement..... 8

110 3.1.3. Information Flow Enforcement..... 9

111 3.1.4. Separation of Duties ..... 9

112 3.1.5. Least Privilege ..... 10

113 3.1.6. Least Privilege – Privileged Accounts..... 11

114 3.1.7. Least Privilege – Privileged Functions..... 11

115 3.1.8. Unsuccessful Logon Attempts ..... 12

116 3.1.9. System Use Notification..... 13

117 3.1.10. Device Lock ..... 13

118 3.1.11. Session Termination ..... 14

119 3.1.12. Remote Access..... 14

120 3.1.13. Withdrawn..... 15

121 3.1.14. Withdrawn..... 15

122 3.1.15. Withdrawn..... 15

123 3.1.16. Wireless Access ..... 16

124 3.1.17. Withdrawn..... 16

125 3.1.18. Access Control for Mobile Devices ..... 16

126 3.1.19. Withdrawn..... 17

127 3.1.20. Use of External Systems..... 17

128 3.1.21. Withdrawn..... 18

129 3.1.22. Publicly Accessible Content..... 18

130 3.2. Awareness and Training ..... 19

131 3.2.1. Literacy Training and Awareness..... 19

132 3.2.2. Role-Based Training ..... 20

133 3.2.3. Withdrawn..... 21

134 3.3. Audit and Accountability ..... 21



135	3.3.1. Event Logging .....	21
136	3.3.2. Audit Record Content .....	21
137	3.3.3. Audit Record Generation .....	22
138	3.3.4. Response to Audit Logging Process Failures .....	23
139	3.3.5. Audit Record Review, Analysis, and Reporting .....	23
140	3.3.6. Audit Record Reduction and Report Generation .....	24
141	3.3.7. Time Stamps.....	25
142	3.3.8. Protection of Audit Information.....	25
143	3.3.9. Withdrawn .....	26
144	3.4. Configuration Management .....	26
145	3.4.1. Baseline Configuration.....	26
146	3.4.2. Configuration Settings .....	27
147	3.4.3. Configuration Change Control .....	28
148	3.4.4. Impact Analyses .....	28
149	3.4.5. Access Restrictions for Change.....	29
150	3.4.6. Least Functionality .....	30
151	3.4.7. Withdrawn .....	31
152	3.4.8. Authorized Software – Allow by Exception .....	31
153	3.4.9. Withdrawn .....	32
154	3.4.10. System Component Inventory.....	32
155	3.4.11. Information Location .....	33
156	3.4.12. System and Component Configuration for High-Risk Areas.....	34
157	3.5. Identification and Authentication .....	34
158	3.5.1. User Identification, Authentication, and Re-Authentication.....	34
159	3.5.2. Device Identification and Authentication .....	35
160	3.5.3. Multi-Factor Authentication .....	36
161	3.5.4. Replay-Resistant Authentication.....	36
162	3.5.5. Identifier Management .....	37
163	3.5.6. Withdrawn .....	37
164	3.5.7. Password Management .....	37
165	3.5.8. Withdrawn .....	38
166	3.5.9. Withdrawn .....	38
167	3.5.10. Withdrawn .....	38
168	3.5.11. Authentication Feedback .....	39
169	3.5.12. Authenticator Management.....	39
170	3.6. Incident Response .....	40

171	3.6.1. Incident Response Plan and Handling.....	40
172	3.6.2. Incident Monitoring, Reporting, and Response Assistance .....	41
173	3.6.3. Incident Response Testing .....	42
174	3.6.4. Incident Response Training .....	42
175	3.7. Maintenance .....	43
176	3.7.1. Withdrawn .....	43
177	3.7.2. Withdrawn .....	43
178	3.7.3. Withdrawn .....	43
179	3.7.4. Maintenance Tools .....	43
180	3.7.5. Nonlocal Maintenance .....	44
181	3.7.6. Maintenance Personnel .....	45
182	3.8. Media Protection.....	46
183	3.8.1. Media Storage .....	46
184	3.8.2. Media Access .....	46
185	3.8.3. Media Sanitization .....	47
186	3.8.4. Media Marking .....	47
187	3.8.5. Media Transport.....	48
188	3.8.6. Withdrawn .....	49
189	3.8.7. Media Use.....	49
190	3.8.8. Withdrawn .....	49
191	3.8.9. System Backup – Cryptographic Protection .....	50
192	3.9. Personnel Security.....	50
193	3.9.1. Personnel Screening .....	50
194	3.9.2. Personnel Termination and Transfer .....	51
195	3.10. Physical Protection .....	52
196	3.10.1. Physical Access Authorizations .....	52
197	3.10.2. Monitoring Physical Access .....	53
198	3.10.3. Withdrawn .....	53
199	3.10.4. Withdrawn .....	53
200	3.10.5. Withdrawn .....	53
201	3.10.6. Alternate Work Site .....	53
202	3.10.7. Physical Access Control .....	54
203	3.10.8. Access Control for Transmission and Output Devices.....	55
204	3.11. Risk Assessment .....	56
205	3.11.1. Risk Assessment .....	56
206	3.11.2. Vulnerability Monitoring and Scanning.....	56

207	3.11.3. Withdrawn .....	57
208	3.12. Security Assessment and Monitoring .....	57
209	3.12.1. Security Assessment .....	57
210	3.12.2. Plan of Action and Milestones.....	58
211	3.12.3. Continuous Monitoring .....	59
212	3.12.4. Withdrawn .....	59
213	3.12.5. Information Exchange .....	59
214	3.13. System and Communications Protection.....	60
215	3.13.1. Boundary Protection .....	60
216	3.13.2. Withdrawn .....	61
217	3.13.3. Withdrawn .....	61
218	3.13.4. Information in Shared System Resources .....	61
219	3.13.5. Withdrawn .....	62
220	3.13.6. Network Communications – Deny by Default – Allow by Exception .....	62
221	3.13.7. Withdrawn .....	62
222	3.13.8. Transmission and Storage Confidentiality .....	62
223	3.13.9. Network Disconnect.....	63
224	3.13.10. Cryptographic Key Establishment and Management.....	64
225	3.13.11. Cryptographic Protection .....	64
226	3.13.12. Collaborative Computing Devices and Applications .....	65
227	3.13.13. Mobile Code.....	66
228	3.13.14. Withdrawn .....	66
229	3.13.15. Session Authenticity.....	66
230	3.13.16. Withdrawn .....	67
231	3.14. System and Information Integrity .....	67
232	3.14.1. Flaw Remediation .....	67
233	3.14.2. Malicious Code Protection .....	68
234	3.14.3. Security Alerts, Advisories, and Directives .....	69
235	3.14.4. Withdrawn .....	70
236	3.14.5. Withdrawn .....	70
237	3.14.6. System Monitoring .....	70
238	3.14.7. Withdrawn .....	70
239	3.14.8. Information Management and Retention.....	71
240	3.15. Planning.....	71
241	3.15.1. Policy and Procedures .....	71
242	3.15.2. System Security Plan.....	72

243	3.15.3. Rules of Behavior .....	73
244	3.16. System and Services Acquisition.....	74
245	3.16.1. Acquisition Process.....	74
246	3.16.2. Unsupported System Components .....	74
247	3.16.3. External System Services .....	75
248	3.17. Supply Chain Risk Management .....	76
249	3.17.1. Supply Chain Risk Management Plan .....	76
250	3.17.2. Acquisition Strategies, Tools, and Methods.....	77
251	3.17.3. Supply Chain Requirements and Processes .....	78
252	<b>References.....</b>	<b>79</b>
253	<b>Appendix A. Acronyms .....</b>	<b>80</b>
254	<b>Appendix B. Glossary .....</b>	<b>81</b>
255	<b>Appendix C. Change Log.....</b>	<b>83</b>
256		

257	<b>List of Tables</b>	
258	<b>Table 1.</b> Security requirement families .....	3
259	<b>Table 2.</b> Change Log .....	84
260		

261 **Acknowledgments**

262 The authors gratefully acknowledge and appreciate the significant contributions from individuals  
263 and organizations in the public and private sectors whose constructive comments improved the  
264 overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank  
265 the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura,  
266 Isabel Van Wyk, and Cristina Ritfeld – for their outstanding support in preparing this document  
267 for publication.

268 *Historical Contributions*

269 The authors wish to acknowledge the following individuals for their historic contributions to this  
270 publication: Jon Boyens, Devin Casey, Chris Enloe, Ned Goren, Gary Guissanie, Jody Jacobs,  
271 Jeff Marron, Vicki Michetti, Mark Riddle, Mary Thomas, Gary Stoneburner, Patricia Toth, and  
272 Patrick Viscuso.

## 273 **1. Introduction**

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

- 276 • Identifying potential problems or shortfalls in security and risk management programs;
- 277 • Identifying security weaknesses and deficiencies in systems and the environments in  
278 which those systems operate;
- 279 • Prioritizing risk mitigation decisions and activities;
- 280 • Confirming that identified security weaknesses and deficiencies in the system and  
281 environment of operation have been addressed; and
- 282 • Supporting continuous monitoring activities and providing information security  
283 situational awareness.

### 284 **1.1. Purpose and Applicability**

285 The purpose of this publication is to provide procedures for assessing the security requirements  
286 in NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information*  
287 *(CUI) in Nonfederal Systems and Organizations* [3]. Organizations can use the assessment  
288 procedures to generate evidence to support the assertion that the security requirements have been  
289 satisfied. The scope of the security assessments conducted using the procedures described in this  
290 publication are guided and informed by the system security plans for systems that process, store,  
291 or transmit CUI. The assessment procedures offer the flexibility to customize assessments based  
292 on organizational policies and requirements, known threat and vulnerability information, system  
293 and platform dependencies, operational considerations, and tolerance for risk.<sup>1</sup>

### 294 **1.2. Organization of This Publication**

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

- 296 • [Section 2](#) describes the fundamental concepts associated with assessments of security  
297 requirements, including assessment procedures, methods, objects, and assurance cases  
298 that can be created using evidence produced during assessments.
- 299 • [Section 3](#) provides assessment procedures for the security requirements in NIST SP 800-  
300 171, including assessment objectives and potential assessment methods and objects for  
301 each procedure.

302 The following sections provide additional information to support the protection of CUI in  
303 nonfederal systems and organizations:

- 304 • [References](#)
- 305 • [Appendix A](#): Acronyms

---

<sup>1</sup> 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 NIST SP 800-39 [4] for additional information on organizational risk management and risk tolerance.

- 306 • [Appendix B](#): Glossary
- 307 • [Appendix C](#): Change Log

308

---

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 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 sufficient to obtain the needed evidence to support any claims of compliance.

309

---



## 310 2. The Fundamentals

311 The process used by organizations and assessors to assess the security requirements in NIST SP  
312 800-171 includes (1) preparing for the assessment, (2) developing a security assessment plan, (3)  
313 conducting the assessment, and (4) documenting, analyzing, and reporting the assessment  
314 results.<sup>2</sup> The remainder of this section describes the structure and content of the procedures used  
315 to assess the security requirements and the importance of assurance cases in providing the  
316 evidence necessary to determine compliance with the requirements.

### 317 2.1. Assessment Procedures

318 The security requirements in NIST SP 800-171 are organized into 17 families, as illustrated in  
319 Table 1. The assessment procedures in [Section 3](#) are grouped by similar family designations to  
320 ensure the completeness and consistency of assessments. The procedures have been derived from  
321 the assessment procedures in NIST SP 800-53A [5].

322 **Table 1.** Security requirement families

<a href="#">Access Control</a>	<a href="#">Maintenance</a>	<a href="#">Security Assessment and Monitoring</a>
<a href="#">Awareness and Training</a>	<a href="#">Media Protection</a>	<a href="#">System and Communications Protection</a>
<a href="#">Audit and Accountability</a>	<a href="#">Personnel Security</a>	<a href="#">System and Information Integrity</a>
<a href="#">Configuration Management</a>	<a href="#">Physical Protection</a>	<a href="#">Planning</a>
<a href="#">Identification and Authentication</a>	<a href="#">Risk Assessment</a>	<a href="#">System and Services Acquisition</a>
<a href="#">Incident Response</a>		<a href="#">Supply Chain Risk Management</a>

323  
324 An assessment procedure consists of an assessment *objective* and a set of potential assessment  
325 *methods* and *objects* that can be used to conduct the assessment. Each potential assessment  
326 objective includes a determination statement related to the security requirement. If there is an  
327 organization-defined parameter (ODP) in the security requirement, then the assessment objective  
328 begins with a determination statement related to the definition of the ODP. The determination  
329 statements are linked to the content of the security requirements to help ensure traceability of the  
330 assessment results to the requirements.

331 Assessment objects identify the specific items being assessed and can include specifications,  
332 mechanisms, activities, and individuals. Specifications are the documented artifacts<sup>3</sup> (e.g., plans,  
333 policies, procedures, requirements, functional and assurance specifications, architectures, and  
334 design documentation) associated with a system. Mechanisms are the hardware, software, and  
335 firmware safeguards implemented within a system. Activities are the protection-related actions  
336 supporting a system that involve people (e.g., conducting system backup operations, exercising  
337 an incident response plan, and monitoring network traffic). Individuals are the people applying  
338 the specifications, mechanisms, or activities described above.

<sup>2</sup> NIST SP 800-53A [5] provides additional information on the assessment process and the individuals steps listed above.

<sup>3</sup> Artifacts may be in formats other than documents (e.g., databases, Governance, Risk, and Compliance [GRC] tools, or Open Security Controls Assessment Language [OSCAL])

339 Assessment methods define the nature and extent of the assessor’s actions and are used to  
340 facilitate understanding, achieve clarification, or obtain evidence. The potential assessment  
341 methods include *examine*, *interview*, and *test*. The examine method is the process of reviewing,  
342 studying, inspecting, observing, or analyzing assessment objects. The interview method is the  
343 process of holding discussions with individuals or groups about assessment objects. The test  
344 method is the process of exercising assessment objects (i.e., activities, mechanisms) under  
345 specified conditions to compare actual with expected behavior. Assessment methods include  
346 attributes of *depth* and *coverage*, which define the rigor, scope, and level of effort for the  
347 assessment as well as the degree of assurance that the security requirements have been satisfied.

348 The structure and content of a typical assessment procedure are provided in the example below:

### 349 3.1.8 Unsuccessful Logon Attempts

Security Requirement Name

350 **REQUIREMENT: 03.01.08**

#### 351 **ASSESSMENT OBJECTIVE**

352 *Determine if:*

353 **A.03.01.08.ODP[01]: the number of consecutive invalid logon**  
354 **attempts by a user allowed during a time period is defined.**

Multi-Part Determination Statement  
for Security Requirement and ODPs

355 **A.03.01.08.ODP[02]: the time period to which the number of**  
356 **consecutive invalid logon attempts by a user is limited is defined.**

357 **A.03.01.08:** the number of consecutive invalid logon attempts by a user during  
358 **<03.01.08.ODP[02]: time period>** is limited to **<A.03.01.08.ODP[01]: number>**.

#### 359 **ASSESSMENT METHODS AND OBJECTS**

##### 360 **Examine**

361 [SELECT FROM: access control policy and procedures; procedures for unsuccessful logon attempts;  
362 system design documentation; system audit records; system configuration settings; system security plan;  
363 other relevant documents or records]

##### 364 **Interview**

365 [SELECT FROM: personnel with information security responsibilities; system developers; system  
366 administrators]

##### 367 **Test**

368 [SELECT FROM: mechanisms implementing access control policy for unsuccessful logon attempts]

#### 369 **REFERENCES**

370 Source Assessment Procedure: [AC-07](#)

371 Determination statements have alphanumeric identifiers. Each determination statement begins  
372 with the letter “A” to indicate that it is part of an assessment procedure. The next sequence of  
373 numbers and/or letters (e.g., [03.01.01.e](#) or [03.01.01.f.02](#)) indicates the security requirement  
374 identifier from SP 800-171 (and the specific control item if it is a multi-part requirement) that is  
375 the target of the assessment. Organization-defined parameters are indicated by the letters “ODP.”  
376 If there are multiple ODPs in the determination statement, the ODP number is indicated in a  
377 square bracket (e.g., [A.03.01.08.ODP\[01\]](#)). Square brackets are also used to denote when an  
378 assessment procedure further decomposes a requirement into more granular determination  
379 statements (e.g., [A.03.01.12.a\[01\]](#), [A.03.01.12.a\[02\]](#), [A.03.01.12.a\[03\]](#)).

380 The application of an assessment procedure to a security requirement produces assessment  
381 results or *findings*. The findings are compiled and used as evidence to determine whether the  
382 security requirement has been *satisfied* or *other than satisfied*. A finding of satisfied indicates  
383 that the assessment objective has been met, producing a fully acceptable result. A finding of  
384 other than satisfied indicates that there are potential anomalies that may need to be addressed by  
385 the organization. A finding of other than satisfied may also indicate that the assessor was unable  
386 to obtain sufficient information to make the determination called for in the determination  
387 statement.

388 For assessment findings that are other than satisfied, organizations may define subcategories of  
389 findings to indicate the severity or criticality of the weaknesses or deficiencies discovered and  
390 the potential adverse effects of those weaknesses or deficiencies on the missions and/or business  
391 functions of the organization. Defining such subcategories can help to establish priorities for  
392 needed risk mitigation actions.

## 393 **2.2. Assurance Cases**

394 Building an effective assurance case to determine compliance with security requirements is a  
395 process that involves compiling evidence from a variety of sources and conducting different  
396 types of activities during an assessment. An *assurance case* is a body of evidence organized into  
397 an argument demonstrating that some claim about a system is true. For assessments conducted  
398 using the procedures in this publication, that claim is compliance with the security requirements  
399 in NIST SP 800-171. Assessors obtain evidence during security assessments to allow designated  
400 officials<sup>4</sup> to make objective determinations about compliance with the security requirements. The  
401 evidence needed to make such determinations can be obtained from various sources, including  
402 independent, third-party assessments or other types of assessments, depending on the needs of  
403 the organization establishing the requirements and the organization conducting the assessments.

404 For example, many technical security requirements are satisfied by security capabilities that are  
405 built into commercial information technology products and systems. Product assessments are  
406 typically conducted by independent, third-party testing organizations.<sup>5</sup> These assessments  
407 examine the security functions of products and established configuration settings. Assessments  
408 can also be conducted to demonstrate compliance with industry, national, or international  
409 security standards as well as developer and vendor claims. Since many information technology  
410 products are assessed by commercial testing organizations and then subsequently deployed in  
411 hundreds of thousands of systems, these types of assessments can be carried out at a greater level  
412 of depth and provide deeper insights into the security capabilities of the products.

413 The evidence needed to determine compliance comes from assessing the implementation of the  
414 safeguards and countermeasure selected to satisfy the security requirements. Assessors can build  
415 on previously developed materials that started with the specification of the information security

---

<sup>4</sup> A *designated official* is an official, either internal or external to a nonfederal organization, with the responsibility to determine organizational compliance with the security requirements.

<sup>5</sup> 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 Standard (FIPS) 140 [7].

416 needs of the organization and were further improved during the design, development, and  
417 implementation of the system. These materials provide the initial evidence for an assurance case.  
418 Assessments can be conducted by system developers, system integrators, auditors, system  
419 owners, or the security staffs of organizations. The assessors or assessment teams bring together  
420 available information about the system, such as the results of component product assessments.  
421 The assessors can conduct additional system-level assessments using the assessment methods  
422 and procedures contained in this publication and based on the implementation information  
423 provided by the nonfederal organization in its system security plan. Assessments can be used to  
424 compile and evaluate the evidence needed by organizations to help determine the effectiveness  
425 of the safeguards implemented to protect CUI, the actions needed to mitigate security risks to the  
426 organization, and compliance with the security requirements.

## 427 3. The Procedures

428 This section provides assessment procedures for the security requirements defined in NIST SP  
429 800-171. Organizations that conduct security requirement assessments can develop their security  
430 assessment plans by using the information provided in the assessment procedures and selecting  
431 the specific assessment methods and objects that meet the organization's needs. Organizations  
432 also have flexibility in defining the level of rigor and detail associated with the assessment based  
433 on the assurance requirements of the organization.

### 434 3.1. [Access Control](#)

#### 435 3.1.1. Account Management

436 **REQUIREMENT:** 03.01.01

#### 437 **ASSESSMENT OBJECTIVE**

438 *Determine if:*

439 **A.03.01.01.ODP[01]: time period for account inactivity before disabling is defined.**

440 **A.03.01.01.a[01]:** system account types allowed are defined.

441 **A.03.01.01.a[02]:** system account types prohibited are defined.

442 **A.03.01.01.b[01]:** system accounts are created in accordance with organizational policy,  
443 procedures, prerequisites, and criteria.

444 **A.03.01.01.b[02]:** system accounts are enabled in accordance with organizational policy,  
445 procedures, prerequisites, and criteria.

446 **A.03.01.01.b[03]:** system accounts are modified in accordance with organizational policy,  
447 procedures, prerequisites, and criteria.

448 **A.03.01.01.b[04]:** system accounts are disabled in accordance with organizational policy,  
449 procedures, prerequisites, and criteria.

450 **A.03.01.01.b[05]:** system accounts are removed in accordance with organizational policy,  
451 procedures, prerequisites, and criteria.

452 **A.03.01.01.c[01]:** authorized users of the system are specified.

453 **A.03.01.01.c[02]:** group and role membership are specified.

454 **A.03.01.01.c[03]:** access authorizations (i.e., privileges) are specified.

455 **A.03.01.01.d[01]:** access to the system is authorized based on a valid access authorization.

456 **A.03.01.01.d[02]:** access to the system is authorized based on intended system usage.

457 **A.03.01.01.e:** the use of system accounts is monitored.

458 **A.03.01.01.f.01:** system accounts are disabled when the accounts have expired.

459 **A.03.01.01.f.02:** system accounts are disabled when the accounts have been inactive for  
460 **<A.03.01.01.ODP[01] time period>**.

461 **A.03.01.01.f.03:** system accounts are disabled when the accounts are no longer associated with  
462 a user or individual.

463 **A.03.01.01.f.04:** system accounts are disabled when the accounts violate organizational policy.

464 **A.03.01.01.f.05:** system accounts are disabled when significant risks associated with individuals  
465 are discovered.

466 **A.03.01.01.g.01:** organizational personnel or roles are notified when accounts are no longer  
467 required.

468 **A.03.01.01.g.02:** organizational personnel or roles are notified when users are terminated or  
469 transferred.

470 **A.03.01.01.g.03:** organizational personnel or roles are notified when system usage or the need-  
471 to-know changes for an individual.

## 472 **ASSESSMENT METHODS AND OBJECTS**

### 473 **Examine**

474 [SELECT FROM: access control policy and procedures; personnel termination/transfer policies  
475 and procedures; procedures for account management; system design documentation; system  
476 configuration settings; list of active system accounts and the name of the individual associated  
477 with each account; notifications of recent transfers, separations, or terminations of employees; list  
478 of conditions for group and role membership; list of recently disabled system accounts and the  
479 name of the individual associated with each account; list of user activities that pose significant  
480 organizational risks; access authorization records; account management compliance reviews;  
481 system monitoring and audit records; system security plan; system-generated list of accounts  
482 removed; system-generated list of emergency accounts disabled; system-generated list of  
483 disabled accounts; other relevant documents and records]

### 484 **Interview**

485 [SELECT FROM: personnel with account management responsibilities; system administrators;  
486 personnel with information security responsibilities; system developers]

### 487 **Test**

488 [SELECT FROM: processes for account management on the system; mechanisms for  
489 implementing account management]

## 490 **REFERENCES**

491 Source Assessment Procedures: [AC-02](#), [AC-02\(03\)](#), [AC-02\(13\)](#)

## 492 **3.1.2. Access Enforcement**

493 **REQUIREMENT:** 03.01.02

### 494 **ASSESSMENT OBJECTIVE**

495 *Determine if:*

496 **A.03.01.02:** approved authorizations for logical access to CUI and system resources are  
497 enforced.

## 498 **ASSESSMENT METHODS AND OBJECTS**

### 499 **Examine**

500 [SELECT FROM: access control policy and procedures; procedures for access enforcement;  
501 system design documentation; system configuration settings; list of approved authorizations (i.e.,  
502 user privileges); system audit records; system security plan; other relevant documents or records]

503 **Interview**  
504 [SELECT FROM: personnel with access enforcement responsibilities; system administrators;  
505 personnel with information security responsibilities; system developers]

506 **Test**  
507 [SELECT FROM: mechanisms for implementing the access control policy]

508 **REFERENCES**  
509 Source Assessment Procedure: [AC-03](#)

### 510 **3.1.3. Information Flow Enforcement**

511 **REQUIREMENT:** 03.01.03

#### 512 **ASSESSMENT OBJECTIVE**

513 *Determine if:*

514 **A.03.01.03:** approved authorizations are enforced for controlling the flow of CUI within the system  
515 and between connected systems.

#### 516 **ASSESSMENT METHODS AND OBJECTS**

##### 517 **Examine**

518 [SELECT FROM: access control policy and procedures; information flow control policies;  
519 procedures for information flow enforcement; security architecture and design documentation;  
520 system configuration settings; system baseline configuration; system audit records; list of  
521 information flow authorizations; system security plan; other relevant documents or records]

##### 522 **Interview**

523 [SELECT FROM: system administrators; personnel with security architecture responsibilities;  
524 personnel with information security responsibilities; system developers]

##### 525 **Test**

526 [SELECT FROM: mechanisms for implementing the information flow enforcement policy]

#### 527 **REFERENCES**

528 Source Assessment Procedure: [AC-04](#)

### 529 **3.1.4. Separation of Duties**

530 **REQUIREMENT:** 03.01.04

#### 531 **ASSESSMENT OBJECTIVE**

532 *Determine if:*

533 **A.03.01.04.a:** duties of individuals requiring separation are identified.

534 **A.03.01.04.b:** system access authorizations to support separation of duties are defined.

535 **ASSESSMENT METHODS AND OBJECTS**

536 **Examine**

537 [SELECT FROM: access control policy and procedures; procedures for the separation of duties  
538 and the division of responsibilities; system configuration settings; system audit records; system  
539 access authorizations; list of divisions of responsibility and separation of duties; system security  
540 plan; other relevant documents or records]

541 **Interview**

542 [SELECT FROM: personnel with responsibilities for defining the separation of duties and the  
543 division of responsibilities; personnel with information security responsibilities; system  
544 administrators]

545 **Test**

546 [SELECT FROM: mechanisms for implementing the separation of duties policy]

547 **REFERENCES0**

548 Source Assessment Procedure: [AC-05](#)

549 **3.1.5. Least Privilege**

550 **REQUIREMENT:** 03.01.05

551 **ASSESSMENT OBJECTIVE**

552 *Determine if:*

553 **A.03.01.05.ODP[01]: security functions for authorized access are defined.**

554 **A.03.01.05.ODP[02]: security-relevant information for authorized access is defined.**

555 **A.03.01.05.a:** system access for users (or processes acting on behalf of users) is authorized only  
556 when necessary to accomplish assigned organizational tasks.

557 **A.03.01.05.b[01]:** access to **<A.03.01.05.ODP[01] security functions>** is authorized.

558 **A.03.01.05.b[02]:** access to **<A.03.01.05.ODP[01] security-relevant information>** is  
559 authorized.

560 **A.03.01.05.c:** the privileges assigned to roles or classes of users are periodically reviewed to  
561 validate the need for such privileges.

562 **A.03.01.05.d:** privileges are reassigned or removed, as necessary.

563 **ASSESSMENT METHODS AND OBJECTS**

564 **Examine**

565 [SELECT FROM: access control policy and procedures; procedures for least privilege; list of  
566 assigned access authorizations (i.e., privileges); system configuration settings; system audit  
567 records; list of security functions (deployed in hardware, software, and firmware); security-  
568 relevant information for which access must be explicitly authorized; list of system-generated roles  
569 or classes of users and assigned privileges; validation reviews of privileges assigned to roles or  
570 classes or users; records of privilege removals or reassignments for roles or classes of users;  
571 system design documentation; system security plan; other relevant documents or records]



572 **Interview**  
573 [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with  
574 information security responsibilities; system administrators]  
575 **Test**  
576 [SELECT FROM: mechanisms for implementing least privilege functions; mechanisms for  
577 implementing reviews of user privileges]  
578 **REFERENCES**  
579 Source Assessment Procedures: [AC-06](#), [AC-06\(01\)](#), [AC-06\(07\)](#), [AU-09\(04\)](#)

### 580 **3.1.6. Least Privilege – Privileged Accounts**

581 **REQUIREMENT:** 03.01.06

#### 582 **ASSESSMENT OBJECTIVE**

583 *Determine if:*

584 **A.03.01.06.ODP[01]: personnel or roles to which privileged accounts on the system are to**  
585 **be restricted are defined.**

586 **A.03.01.06.a:** privileged accounts on the system are restricted to **<A.03.01.06.ODP[01]:**  
587 **personnel or roles>.**

588 **A.03.01.06.b:** users (or roles) with privileged accounts are required to use non-privileged  
589 accounts when accessing nonsecurity functions or nonsecurity information.

#### 590 **ASSESSMENT METHODS AND OBJECTS**

##### 591 **Examine**

592 [SELECT FROM: access control policy and procedures; procedures for least privilege; list of  
593 system-generated privileged accounts; list of system administration personnel; system audit  
594 records; system configuration settings; system security plan; list of system-generated security  
595 functions or security-relevant information assigned to system accounts or roles; other relevant  
596 documents or records]

##### 597 **Interview**

598 [SELECT FROM: personnel with responsibilities for defining least privileges; personnel with  
599 information security responsibilities; system administrators]

##### 600 **Test**

601 [SELECT FROM: mechanisms for implementing least privilege functions]

#### 602 **REFERENCES**

603 Source Assessment Procedures: [AC-06\(02\)](#), [AC-06\(05\)](#)

### 604 **3.1.7. Least Privilege – Privileged Functions**

605 **REQUIREMENT:** 03.01.07

#### 606 **ASSESSMENT OBJECTIVE**

607 *Determine if:*

608 **A.03.01.07.a:** non-privileged users are prevented from executing privileged functions.

609 **A.03.01.07.b:** the execution of privileged functions is logged.

## 610 **ASSESSMENT METHODS AND OBJECTS**

### 611 **Examine**

612 [SELECT FROM: access control policy and procedures; procedures for least privilege; system  
613 design documentation; system configuration settings; system audit records; list of audited events;  
614 list of privileged functions to be audited and associated user account assignments; system  
615 security plan; other relevant documents or records]

### 616 **Interview**

617 [SELECT FROM: personnel with responsibilities for reviewing least privileges; personnel with  
618 information security responsibilities; system developers; system administrators]

### 619 **Test**

620 [SELECT FROM: mechanisms for auditing the execution of least privilege functions; mechanisms  
621 for implementing least privilege functions for non-privileged users]

## 622 **REFERENCES**

623 Source Assessment Procedures: [AC-06\(09\)](#), [AC-06\(10\)](#)

## 624 **3.1.8. Unsuccessful Logon Attempts**

625 **REQUIREMENT:** 03.01.08

### 626 **ASSESSMENT OBJECTIVE**

627 *Determine if:*

628 **A.03.01.08.ODP[01]:** *the number of consecutive invalid logon attempts by a user allowed*  
629 *during a time period is defined.*

630 **A.03.01.08.ODP[02]:** *the time period to which the number of consecutive invalid logon*  
631 *attempts by a user is limited is defined.*

632 **A.03.01.08:** the number of consecutive invalid logon attempts by a user during  
633 **<03.01.08.ODP[02]: time period>** is limited to **<A.03.01.08.ODP[01]: number>**.

## 634 **ASSESSMENT METHODS AND OBJECTS**

### 635 **Examine**

636 [SELECT FROM: access control policy and procedures; procedures for unsuccessful logon  
637 attempts; system design documentation; system audit records; system configuration settings;  
638 system security plan; other relevant documents or records]

### 639 **Interview**

640 [SELECT FROM: personnel with information security responsibilities; system developers; system  
641 administrators]

### 642 **Test**

643 [SELECT FROM: mechanisms for implementing the access control policy for unsuccessful logon  
644 attempts]

645           **REFERENCES**

646           Source Assessment Procedure: [AC-07](#)

647   **3.1.9. System Use Notification**

648           **REQUIREMENT:** 03.01.09

649           **ASSESSMENT OBJECTIVE**

650           *Determine if:*

651           **A.03.01.09:** a system use notification message with privacy and security notices consistent with  
652           applicable CUI rules is displayed before granting access to the system.

653           **ASSESSMENT METHODS AND OBJECTS**

654           **Examine**

655           [SELECT FROM: access control policy and procedures; privacy and security policies, procedures  
656           for system use notification; documented approval of system use notification messages; system  
657           audit records; user acknowledgements of system use notification messages; system design  
658           documentation; system configuration settings; system use notification messages; system security  
659           plan; other relevant documents or records]

660           **Interview**

661           [SELECT FROM: personnel with information security responsibilities; legal counsel; system  
662           developers; system administrators]

663           **Test**

664           [SELECT FROM: mechanisms for implementing system use notifications]

665           **REFERENCES**

666           Source Assessment Procedure: [AC-08](#)

667   **3.1.10. Device Lock**

668           **REQUIREMENT:** 03.01.10

669           **ASSESSMENT OBJECTIVE**

670           *Determine if:*

671           **A.03.01.10.ODP[01]:** *one or more of the following parameter values is/are selected:*  
672           *{initiating a device lock after <A.03.01.10.ODP[02] time period> of inactivity; requiring the*  
673           *user to initiate a device lock before leaving the system unattended}.*

674           **A.03.01.10.ODP[02]:** *time period of inactivity after which a device lock is initiated is*  
675           *defined (if selected).*

676           **A.03.01.10.a:** access to the system is prevented by **<A.03.01.10.ODP[01]: selected parameter**  
677           **value(s)>**.

678           **A.03.01.10.b:** the device lock is retained until the user reestablishes access using established  
679           identification and authentication procedures.

680           **A.03.01.10.c:** information previously visible on the display is concealed via device lock with a  
681           publicly viewable image.

682 **ASSESSMENT METHODS AND OBJECTS**

683 **Examine**

684 [SELECT FROM: access control policy and procedures; procedures for session lock and  
685 identification and authentication; system design documentation; system configuration settings;  
686 display screen with session lock activated; system security plan; other relevant documents or  
687 records]

688 **Interview**

689 [SELECT FROM: personnel with information security responsibilities; system developers;  
690 system administrators]

691 **Test**

692 [SELECT FROM: mechanisms for implementing the access control policy for session lock;  
693 session lock mechanisms]

694 **REFERENCES**

695 Source Assessment Procedures: [AC-11](#), [AC-11\(01\)](#)

696 **3.1.11. Session Termination**

697 **REQUIREMENT:** 03.01.11

698 **ASSESSMENT OBJECTIVE**

699 *Determine if:*

700 **A.03.01.11.ODP[01]: conditions or trigger events that require session disconnect are**  
701 **defined.**

702 **A.03.01.11:** a user session is automatically terminated after **<A.03.01.11.ODP[01]: conditions**  
703 **or trigger events>.**

704 **ASSESSMENT METHODS AND OBJECTS**

705 **Examine**

706 [SELECT FROM: access control policy and procedures; procedures for session termination;  
707 system design documentation; system configuration settings; list of conditions or trigger events  
708 requiring session disconnect; system audit records; system security plan; other relevant  
709 documents or records]

710 **Interview**

711 [SELECT FROM: personnel with information security responsibilities; system developers;  
712 system administrators]

713 **Test**

714 [SELECT FROM: automated mechanisms for implementing user session termination]

715 **REFERENCES**

716 Source Assessment Procedure: [AC-12](#)

717 **3.1.12. Remote Access**

718 **REQUIREMENT:** 03.01.12

719 **ASSESSMENT OBJECTIVE**

720 *Determine if:*

721 **A.03.01.12.a[01]:** types of allowable remote system access are defined.

722 **A.03.01.12.a[02]:** usage restrictions are established for each type of allowable remote system  
723 access.

724 **A.03.01.12.a[03]:** configuration requirements are established for each type of allowable remote  
725 system access.

726 **A.03.01.12.a[04]:** connection requirements are established for each type of allowable remote  
727 system access.

728 **A.03.01.12.b:** each type of remote system access is authorized prior to establishing such  
729 connections.

730 **A.03.01.12.c:** remote access to the system is routed through managed access control points.

731 **A.03.01.12.d[1]:** remote execution of privileged commands is authorized.

732 **A.03.01.12.d[2]:** remote access to security-relevant information is authorized.

733 **ASSESSMENT METHODS AND OBJECTS**

734 **Examine**

735 [SELECT FROM: access control policy and procedures; procedures for remote system access;  
736 remote system access configuration and connection requirements; configuration management  
737 plan; system configuration settings; remote access authorizations; system audit records; system  
738 design documentation; procedures for remote access to the system; system monitoring records;  
739 list of managed network access control points; system security plan; other relevant documents  
740 or records]

741 **Interview**

742 [SELECT FROM: personnel with responsibilities for managing remote access connections;  
743 personnel with information security responsibilities; system administrators]

744 **Test**

745 [SELECT FROM: mechanisms for monitoring and controlling remote access methods;  
746 mechanisms for routing remote accesses through managed access control points; remote  
747 access management capability for the system]

748 **REFERENCES**

749 Source Assessment Procedures: [AC-17](#), [AC-17\(03\)](#), [AC-17\(04\)](#)

750 **3.1.13. Withdrawn**

751 Incorporated into [03.01.12](#).

752 **3.1.14. Withdrawn**

753 Incorporated into [03.01.12](#).

754 **3.1.15. Withdrawn**

755 Incorporated into [03.01.12](#).

756 **3.1.16. Wireless Access**

757 **REQUIREMENT:** 03.01.16

758 **ASSESSMENT OBJECTIVE**

759 *Determine if:*

760 **A.03.01.16.a[01]:** each type of wireless access to the system is defined.

761 **A.03.01.16.a[02]:** usage restrictions are established for each type of wireless access to the  
762 system.

763 **A.03.01.16.a[03]:** configuration requirements are established for each type of wireless access  
764 to the system.

765 **A.03.01.16.a[04]:** connection requirements are established for each type of wireless access to  
766 the system.

767 **A.03.01.16.b:** each type of wireless access to the system is authorized prior to establishing  
768 such connections.

769 **A.03.01.16.c:** wireless networking capabilities not intended for use are disabled prior to  
770 issuance and deployment.

771 **ASSESSMENT METHODS AND OBJECTS**

772 **Examine**

773 [SELECT FROM: access control policy and procedures; procedures for wireless system access;  
774 wireless system access configuration and connection requirements; configuration management  
775 plan; system configuration settings; wireless access authorizations; system audit records;  
776 system design documentation; system security plan; other relevant documents or records]

777 **Interview**

778 [SELECT FROM: personnel with responsibilities for managing wireless access connections;  
779 personnel with information security responsibilities; system developers; system administrators]

780 **Test**

781 [SELECT FROM: wireless access management capability for the system; mechanisms for  
782 implementing wireless access protections to the system; mechanisms for managing the  
783 disabling of wireless networking capabilities]

784 **REFERENCES**

785 Source Assessment Procedures: [AC-18](#), [AC-18\(03\)](#)

786 **3.1.17. Withdrawn**

787 Incorporated into [03.01.16](#).

788 **3.1.18. Access Control for Mobile Devices**

789 **REQUIREMENT:** 03.01.18

790 **ASSESSMENT OBJECTIVE**

791 *Determine if:*

- 792 **A.03.01.18.a[01]**: usage restrictions are established for mobile devices.  
793 **A.03.01.18.a[02]**: configuration requirements are established for mobile devices.  
794 **A.03.01.18.a[03]**: connection requirements are established for mobile devices.  
795 **A.03.01.18.b**: the connection of mobile devices to the system is authorized.  
796 **A.03.01.18.c**: full-device or container-based encryption is implemented to protect the  
797 confidentiality of CUI on mobile devices.

## 798 **ASSESSMENT METHODS AND OBJECTS**

### 799 **Examine**

800 [SELECT FROM: access control policy and procedures; procedures for mobile device access  
801 control; system design documentation; configuration management plan; system configuration  
802 settings; authorizations for mobile device connections to organizational systems; system audit  
803 records; encryption mechanisms and associated configuration documentation; system security  
804 plan; other relevant documents or records]

### 805 **Interview**

806 [SELECT FROM: personnel with access control responsibilities for mobile devices; personnel  
807 using mobile devices to access organizational systems; personnel with information security  
808 responsibilities; system administrators]

### 809 **Test**

810 [SELECT FROM: access control capability for mobile device connections to organizational  
811 systems; encryption mechanisms for protecting the confidentiality of CUI on mobile devices;  
812 configurations of mobile devices]

## 813 **REFERENCES**

814 Source Assessment Procedures: [AC-19](#), [AC-19\(05\)](#)

### 815 **3.1.19. Withdrawn**

816 Incorporated into [03.01.18](#).

### 817 **3.1.20. Use of External Systems**

818 **REQUIREMENT:** 03.01.20

#### 819 **ASSESSMENT OBJECTIVE**

820 *Determine if:*

821 **A.03.01.20.ODP[01]: terms and conditions to be satisfied on external systems prior to**  
822 **allowing the use of or access to those systems by authorized individuals are defined.**

823 **A.03.01.20.ODP[02]: security requirements to be satisfied on external systems prior to**  
824 **allowing the use of or access to those systems by authorized individuals are defined.**

825 **A.03.01.20.a:** the use of external systems is prohibited unless the systems are specifically  
826 authorized.

827 **A.03.01.20.b[01]:** the following terms and conditions to be satisfied on external systems prior to  
828 allowing the use of or access to those systems by authorized individuals are established:  
829 **<A.03.01.20.ODP[01]: terms and conditions>.**

830 **A.03.01.20.b[02]**: the following security requirements to be satisfied on external systems prior  
831 to allowing the use of or access to those systems by authorized individuals are established:  
832 **<A.03.01.20.ODP[02]: security requirements>**.

833 **A.03.01.20.c.01**: authorized individuals are permitted to use an external system to access the  
834 organizational system or to process, store, or transmit CUI only after verification of the  
835 implementation of security requirements on the external system as specified in the  
836 organization's security plans.

837 **A.03.01.20.c.02**: authorized individuals are permitted to use an external system to access the  
838 organizational system or to process, store, or transmit CUI only after the retention of approved  
839 system connection or processing agreements with the organizational entity hosting the external  
840 system.

841 **A.03.01.20.d**: the use of organization-controlled portable storage devices by authorized  
842 individuals on external systems is restricted.

## 843 **ASSESSMENT METHODS AND OBJECTS**

### 844 **Examine**

845 [SELECT FROM: access control policy and procedures; procedures for the use of external  
846 systems; terms and conditions for the use of external systems; external systems security  
847 requirements; list of types of applications accessible from external systems; system  
848 configuration settings; system security plan; other relevant documents or records]

### 849 **Interview**

850 [SELECT FROM: personnel with responsibilities for defining terms, conditions, and security  
851 requirements for the use of external systems; personnel with information security  
852 responsibilities; system administrators]

### 853 **Test**

854 [SELECT FROM: mechanisms for implementing and/or enforcing terms, conditions, and  
855 security requirements for the use of external systems]

## 856 **REFERENCES**

857 Source Assessment Procedures: [AC-20](#), [AC-20\(01\)](#), [AC-20\(02\)](#)

### 858 **3.1.21. Withdrawn**

859 Incorporated into [03.01.20](#).

### 860 **3.1.22. Publicly Accessible Content**

861 **REQUIREMENT:** 03.01.22

#### 862 **ASSESSMENT OBJECTIVE**

863 *Determine if:*

864 **A.03.01.22.a**: authorized individuals are trained to ensure that publicly accessible information  
865 does not contain CUI.

866 **A.03.01.22.b[01]**: the content on publicly accessible systems is periodically reviewed for CUI.

867 **A.03.01.22.b[02]**: CUI is removed from publicly accessible systems if discovered.



868 **ASSESSMENT METHODS AND OBJECTS**

869 **Examine**

870 [SELECT FROM: access control policy and procedures; procedures for publicly accessible  
871 content; list of users authorized to post publicly accessible content on organizational systems;  
872 training materials and/or records; records of publicly accessible information reviews; records of  
873 response to CUI discovered on public websites; system audit logs; security awareness training  
874 records; system security plan; other relevant documents or records]

875 **Interview**

876 [SELECT FROM: personnel with responsibilities for managing publicly accessible information  
877 posted on organizational systems; personnel with information security responsibilities]

878 **Test**

879 [SELECT FROM: mechanisms for implementing the management of publicly accessible  
880 content]

881 **REFERENCES**

882 Source Assessment Procedure: [AC-22](#)

883 **3.2. [Awareness and Training](#)**

884 **3.2.1. Literacy Training and Awareness**

885 **REQUIREMENT:** 03.02.01

886 **ASSESSMENT OBJECTIVE**

887 *Determine if:*

888 **A.03.02.01.ODP[01]: events that require role-based security training are defined.**

889 **A.03.02.01.a.01[01]:** security literacy training is provided to system users as part of initial training  
890 for new users.

891 **A.03.02.01.a.01[02]:** security literacy training is provided to system users periodically after initial  
892 training.

893 **A.03.02.01.a.02:** security literacy training is provided to system users when required by system  
894 changes or following **<A.03.02.01.ODP[01] events>**.

895 **A.03.02.01.a.03[01]:** security literacy training on recognizing indicators of insider threat is  
896 provided.

897 **A.03.02.01.a.03[02]:** security literacy training on reporting indicators of insider threat is provided.

898 **A.03.02.01.a.03[03]:** security literacy training on recognizing indicators of social engineering is  
899 provided.

900 **A.03.02.01.a.03[04]:** security literacy training on reporting indicators of social engineering is  
901 provided.

902 **A.03.02.01.a.03[05]:** security literacy training on recognizing indicators of social mining is  
903 provided.

904 **A.03.02.01.a.03[06]:** security literacy training on reporting indicators of social mining is provided.

905 **A.03.02.01.b[01]:** security literacy training content is updated periodically.

906 **A.03.02.01.b[02]:** security literacy training content is updated following **<A.03.02.01.ODP[01]**  
907 **events>**.

## 908 **ASSESSMENT METHODS AND OBJECTS**

### 909 **Examine**

910 [SELECT FROM: security literacy training and awareness policy and procedures; procedures for  
911 security literacy training and awareness implementation; codes of federal regulations; security  
912 literacy and awareness training curriculum; security literacy and awareness training materials;  
913 training records; system security plan; other relevant documents or records]

### 914 **Interview**

915 [SELECT FROM: personnel with responsibilities for security literacy training and awareness;  
916 personnel comprising the general system user community; personnel with information security  
917 responsibilities]

### 918 **Test**

919 [SELECT FROM: mechanisms for managing information security literacy training and awareness]

## 920 **REFERENCES**

921 Source Assessment Procedures: [AT-02](#), [AT-02\(02\)](#), [AT-02\(03\)](#)

## 922 **3.2.2. Role-Based Training**

923 **REQUIREMENT:** 03.02.02

### 924 **ASSESSMENT OBJECTIVE**

925 *Determine if:*

926 **A.03.02.02.ODP[01]:** *events that require role-based security training are defined.*

927 **A.03.02.02.a.01[01]:** role-based security training is provided to organizational personnel before  
928 authorizing access to the system or CUI.

929 **A.03.02.02.a.01[02]:** role-based security training is provided to organizational personnel before  
930 performing assigned duties.

931 **A.03.02.02.a.01[03]:** role-based security training is provided to organizational personnel  
932 periodically after initial access.

933 **A.03.02.02.a.02:** role-based security training is provided to organizational personnel when  
934 required by system changes or following **<A.03.02.02.ODP[01] events>**.

935 **A.03.02.02.b[01]:** role-based training content is updated periodically.

936 **A.03.02.02.b[02]:** role-based training content is updated following **<A.03.02.02.ODP[01]**  
937 **events>**.

## 938 **ASSESSMENT METHODS AND OBJECTS**

### 939 **Examine**

940 [SELECT FROM: security awareness and training policy and procedures; procedures for security  
941 training implementation; codes of federal regulations; security training curriculum; security training  
942 materials; training records; system security plan; other relevant documents or records]

943 **Interview**  
944 [SELECT FROM: personnel with responsibilities for role-based security training; personnel with  
945 assigned system security roles and responsibilities]

946 **Test**  
947 [SELECT FROM: mechanisms for managing role-based security training and awareness]

948 **REFERENCES**

949 Source Assessment Procedure: [AT-03](#)

950 **3.2.3. Withdrawn**

951 Incorporated into [03.02.01](#).

952 **3.3. [Audit and Accountability](#)**

953 **3.3.1. Event Logging**

954 **REQUIREMENT:** 03.03.01

955 **ASSESSMENT OBJECTIVE**

956 *Determine if:*

957 **A.03.03.01.ODP[01]: the event types selected for logging within the system are defined.**

958 **A.03.03.01.a:** the following event types are specified for logging within the system:  
959 **<A.03.03.01.ODP[01] event types>.**

960 **A.03.03.01.b[01]:** the event types selected for logging are reviewed periodically.

961 **A.03.03.01.b[02]:** the event types selected for logging are updated periodically.

962 **ASSESSMENT METHODS AND OBJECTS**

963 **Examine**

964 [SELECT FROM: audit and accountability policy and procedures; procedures for auditable  
965 events; system design documentation; system configuration settings; system audit records;  
966 system auditable events; system security plan; other relevant documents or records]

967 **Interview**

968 [SELECT FROM: personnel with audit and accountability responsibilities; personnel with  
969 information security responsibilities; system administrators]

970 **Test**

971 [SELECT FROM: mechanisms for implementing system auditing]

972 **REFERENCES**

973 Source Assessment Procedure: [AU-02](#)

974 **3.3.2. Audit Record Content**

975 **REQUIREMENT:** 03.03.02

976 **ASSESSMENT OBJECTIVE**

977 *Determine if:*

978 **A.03.03.02.a.01:** audit records contain information that establishes what type of event occurred.

979 **A.03.03.02.a.02:** audit records contain information that establishes when the event occurred.

980 **A.03.03.02.a.03:** audit records contain information that establishes where the event occurred.

981 **A.03.03.02.a.04:** audit records contain information that establishes the source of the event.

982 **A.03.03.02.a.05:** audit records contain information that establishes the outcome of the event.

983 **A.03.03.02.a.06:** audit records contain information that establishes the identity of the individuals,  
984 subjects, objects, or entities associated with the event.

985 **A.03.03.02.b:** additional information for audit records is provided, as needed.

986 **ASSESSMENT METHODS AND OBJECTS**

987 **Examine**

988 [SELECT FROM: audit and accountability policy and procedures; procedures for the content of  
989 audit records; list of organization-defined auditable events; system design documentation; system  
990 configuration settings; system audit records; system incident reports; system security plan; other  
991 relevant documents or records]

992 **Interview**

993 [SELECT FROM: personnel with audit and accountability responsibilities; personnel with  
994 information security responsibilities; system developers; system administrators]

995 **Test**

996 [SELECT FROM: mechanisms for implementing system auditing of auditable events; system  
997 audit capability]

998 **REFERENCES**

999 Source Assessment Procedures: [AU-03](#), [AU-03\(01\)](#)

1000 **3.3.3. Audit Record Generation**

1001 **REQUIREMENT:** 03.03.03

1002 **ASSESSMENT OBJECTIVE**

1003 *Determine if:*

1004 **A.03.03.03.a:** audit records for the selected event types and audit record content specified in  
1005 3.3.1 and 3.3.2 are generated.

1006 **A.03.03.03.b:** audit records are retained for a time period consistent with records retention policy.

1007 **ASSESSMENT METHODS AND OBJECTS**

1008 **Examine**

1009 [SELECT FROM: audit and accountability policy and procedures; procedures for audit record  
1010 generation; system design documentation; list of auditable events; audit records; audit record  
1011 retention policy and procedures; organization-defined retention period for audit records; audit

1012 record archives; system configuration settings; system security plan; other relevant documents or  
1013 records]

1014 **Interview**

1015 [SELECT FROM: personnel with audit record generation responsibilities; personnel with audit  
1016 record retention responsibilities; personnel with information security responsibilities; system  
1017 developers; system administrators]

1018 **Test**

1019 [SELECT FROM: mechanisms for implementing the audit record generation capability]

1020 **REFERENCES**

1021 Source Assessment Procedures: [AU-11](#), [AU-12](#)

1022 **3.3.4. Response to Audit Logging Process Failures**

1023 **REQUIREMENT:** 03.03.04

1024 **ASSESSMENT OBJECTIVE**

1025 *Determine if:*

1026 **A.03.03.04.ODP[01]: time period for organizational personnel or roles receiving audit**  
1027 **logging process failure alerts is defined.**

1028 **A.03.03.04.ODP[02]: additional actions to be taken in the event of an audit logging process**  
1029 **failure are defined.**

1030 **A.03.03.04.a:** organizational personnel or roles are alerted in the event of an audit logging  
1031 process failure within **<A.03.03.04.ODP[01] time period>**.

1032 **A.03.03.04.b:** the following additional actions are taken in the event of an audit logging process  
1033 failure: **<A.03.03.04.ODP[02] additional actions>**.

1034 **ASSESSMENT METHODS AND OBJECTS**

1035 **Examine**

1036 [SELECT FROM: audit and accountability policy and procedures; procedures for responding to  
1037 audit processing failures; system design documentation; system configuration settings; list of  
1038 personnel to be notified in case of an audit processing failure; system audit records; system  
1039 security plan; other relevant documents or records]

1040 **Interview**

1041 [SELECT FROM: personnel with audit and accountability responsibilities; personnel with  
1042 information security responsibilities; system developers; system administrators]

1043 **Test**

1044 [SELECT FROM: mechanisms for implementing system response to audit processing failures]

1045 **REFERENCES**

1046 Source Assessment Procedure: [AU-05](#)

1047 **3.3.5. Audit Record Review, Analysis, and Reporting**

1048 **REQUIREMENT:** 03.03.05

1049 **ASSESSMENT OBJECTIVE**

1050 *Determine if:*

1051 **A.03.03.05.a:** system audit records are reviewed and analyzed periodically for indications and  
1052 potential impacts of inappropriate or unusual activity.

1053 **A.03.03.05.b:** findings are reported to organizational personnel or roles.

1054 **A.03.03.05.c:** audit records across different repositories are analyzed and correlated to gain  
1055 organization-wide situational awareness.

1056 **ASSESSMENT METHODS AND OBJECTS**

1057 **Examine**

1058 [SELECT FROM: audit and accountability policy and procedures; procedures for audit review,  
1059 analysis, and reporting; reports of audit findings; records of actions taken in response to reviews  
1060 and analyses of audit records; system design documentation; system audit records across  
1061 different repositories; system configuration settings; system security plan; other relevant  
1062 documents or records]

1063 **Interview**

1064 [SELECT FROM: personnel with audit review, analysis, and reporting responsibilities; personnel  
1065 with information security responsibilities]

1066 **Test**

1067 [SELECT FROM: mechanisms for supporting the analysis and correlation of audit records]

1068 **REFERENCES**

1069 Source Assessment Procedures: [AU-06](#), [AU-06\(03\)](#)

1070 **3.3.6. Audit Record Reduction and Report Generation**

1071 **REQUIREMENT:** 03.03.06

1072 **ASSESSMENT OBJECTIVE**

1073 *Determine if:*

1074 **A.03.03.05.a:** an audit record reduction and report generation capability that supports audit  
1075 record review, analysis, reporting requirements, and after-the-fact investigations of incidents is  
1076 implemented.

1077 **A.03.03.05.b:** the original content and time ordering of audit records are preserved.

1078 **ASSESSMENT METHODS AND OBJECTS**

1079 **Examine**

1080 [SELECT FROM: audit and accountability policy and procedures; procedures for audit reduction  
1081 and report generation; system design documentation; system configuration settings; system audit  
1082 records; audit reduction, review, analysis, and reporting tools; system security plan; other relevant  
1083 documents or records]

1084 **Interview**

1085 [SELECT FROM: personnel with audit reduction and report generation responsibilities; personnel  
1086 with information security responsibilities]

1087 **Test**  
1088 [SELECT FROM: audit reduction and report generation capability]

1089 **REFERENCES**

1090 Source Assessment Procedure: [AU-07](#)

1091 **3.3.7. Time Stamps**

1092 **REQUIREMENT:** 03.03.07

1093 **ASSESSMENT OBJECTIVE**

1094 *Determine if:*

1095 **A.03.03.07.ODP[01]: the granularity of time measurement for audit record time stamps is**  
1096 **defined.**

1097 **A.03.03.07.a:** internal system clocks are used to generate time stamps for audit records.

1098 **A.03.03.07.b[01]:** time stamps for audit records meet **<A.03.03.07.ODP[01] granularity of time**  
1099 **measurement>.**

1100 **A.03.03.07.b[02]:** time stamps for audit records use Coordinated Universal Time (UTC), have a  
1101 fixed local time offset from UTC, or include the local time offset as part of the time stamp are  
1102 recorded.

1103 **ASSESSMENT METHODS AND OBJECTS**

1104 **Examine**

1105 [SELECT FROM: audit and accountability policy and procedures; procedures for timestamp  
1106 generation; system design documentation; system configuration settings; system audit records;  
1107 system security plan; other relevant documents or records]

1108 **Interview**

1109 [SELECT FROM: personnel with information security responsibilities; system developers; system  
1110 administrators]

1111 **Test**

1112 [SELECT FROM: mechanisms for implementing timestamp generation]

1113 **REFERENCES**

1114 Source Assessment Procedure: [AU-08](#)

1115 **3.3.8. Protection of Audit Information**

1116 **REQUIREMENT:** 03.03.08

1117 **ASSESSMENT OBJECTIVE**

1118 *Determine if:*

1119 **A.03.03.08.a:** audit information and audit logging tools are protected from unauthorized access,  
1120 modification, and deletion.

1121 **A.03.03.08.b:** access to the management of audit logging functionality is authorized to only a  
1122 subset of privileged users or roles.

1123 **ASSESSMENT METHODS AND OBJECTS**

1124 **Examine**

1125 [SELECT FROM: audit and accountability policy and procedures; access control policy and  
1126 procedures; procedures for the protection of audit information; system configuration settings;  
1127 system audit records; audit tools; system-generated list of privileged users with access to the  
1128 management of audit functionality; access authorizations; access control list; system design  
1129 documentation; system security plan; other relevant documents or records]

1130 **Interview**

1131 [SELECT FROM: personnel with audit and accountability responsibilities; personnel with  
1132 information security responsibilities; system developers; system administrators]

1133 **Test**

1134 [SELECT FROM: mechanisms for implementing audit information protection; mechanisms for  
1135 managing access to audit functionality]

1136 **REFERENCES**

1137 Source Assessment Procedures: [AU-09](#), [AU-09\(04\)](#)

1138 **3.3.9. Withdrawn**

1139 Incorporated into [03.03.08](#).

1140 **3.4. [Configuration Management](#)**

1141 **3.4.1. Baseline Configuration**

1142 **REQUIREMENT:** 03.04.01

1143 **ASSESSMENT OBJECTIVE**

1144 *Determine if:*

1145 **A.03.04.01.a[01]:** a current baseline configuration of the system is developed.

1146 **A.03.04.01.a[02]:** a current baseline configuration of the system is maintained under  
1147 configuration control.

1148 **A.03.04.01.b[01]:** the baseline configuration of the system is reviewed periodically.

1149 **A.03.04.01.b[02]:** the baseline configuration of the system is reviewed when system components  
1150 are installed or modified.

1151 **A.03.04.01.b[03]:** the baseline configuration of the system is updated periodically.

1152 **A.03.04.01.b[04]:** the baseline configuration of the system is updated when system components  
1153 are installed or modified.

1154 **ASSESSMENT METHODS AND OBJECTS**

1155 **Examine**

1156 [SELECT FROM: configuration management policy and procedures; procedures for the baseline  
1157 system configuration; configuration management plan; enterprise architecture; system design



1158 documentation; system architecture; system configuration settings; system component inventory;  
1159 change control records; system security plan; other relevant documents or records]

1160 **Interview**

1161 [SELECT FROM: personnel with configuration management responsibilities; personnel with  
1162 information security responsibilities; system administrators]

1163 **Test**

1164 [SELECT FROM: processes for managing baseline configurations; mechanisms for supporting  
1165 configuration control of the baseline configuration]

1166 **REFERENCES**

1167 Source Assessment Procedure: [CM-02](#)

1168 **3.4.2. Configuration Settings**

1169 **REQUIREMENT:** 03.04.02

1170 **ASSESSMENT OBJECTIVE**

1171 *Determine if:*

1172 **A.03.04.02.ODP[01]: configuration settings for the system that reflect the most restrictive**  
1173 **mode consistent with operational requirements are defined.**

1174 **A.03.04.02.a[01]:** the following configuration settings for the system that reflect the most  
1175 restrictive mode consistent with operational requirements are established and documented:  
1176 **<A.03.04.02.ODP[01] configuration settings>.**

1177 **A.03.04.02.a[02]:** the following configuration settings for the system are implemented:  
1178 **<A.03.04.02.ODP[01] configuration settings>.**

1179 **A.03.04.02.b[01]:** any deviations from established configuration settings are identified and  
1180 documented.

1181 **A.03.04.02.b[02]:** any deviations from established configuration settings are approved.

1182 **ASSESSMENT METHODS AND OBJECTS**

1183 **Examine**

1184 [SELECT FROM: configuration management policy and procedures; procedures for system  
1185 configuration settings; configuration management plan; system design documentation; system  
1186 configuration settings; common secure configuration checklists; system component inventory;  
1187 evidence supporting approved deviations from established configuration settings; change control  
1188 records; system data processing and retention permissions; system audit records; system  
1189 security plan; other relevant documents or records]

1190 **Interview**

1191 [SELECT FROM: personnel with security configuration management responsibilities; personnel  
1192 with information security responsibilities; system administrators]

1193 **Test**

1194 [SELECT FROM: processes for managing configuration settings; mechanisms that implement,  
1195 monitor, and/or control system configuration settings; mechanisms that identify and/or document  
1196 deviations from established configuration settings]

1197           **REFERENCES**

1198           Source Assessment Procedure: [CM-06](#)

1199   **3.4.3. Configuration Change Control**

1200           **REQUIREMENT:** 03.04.03

1201           **ASSESSMENT OBJECTIVE**

1202           *Determine if:*

1203           **A.03.04.03.a:** the types of changes to the system that are configuration-controlled are defined.

1204           **A.03.04.03.b[01]:** proposed configuration-controlled changes to the system are reviewed.

1205           **A.03.04.03.b[02]:** proposed configuration-controlled changes to the system are approved or  
1206           disapproved with explicit consideration for security impacts.

1207           **A.03.04.03.c[01]:** approved configuration-controlled changes to the system are implemented.

1208           **A.03.04.03.c[02]:** approved configuration-controlled changes to the system are documented.

1209           **A.03.04.03.d[01]:** activities associated with configuration-controlled changes to the system are  
1210           monitored.

1211           **A.03.04.03.d[02]:** activities associated with configuration-controlled changes to the system are  
1212           reviewed.

1213           **ASSESSMENT METHODS AND OBJECTS**

1214           **Examine**

1215           [SELECT FROM: configuration management policy and procedures; procedures for system  
1216           configuration change control; configuration management plan; system architecture; configuration  
1217           settings; change control records; system audit records; change control audit and review reports;  
1218           agenda, minutes, and documentation from configuration change control oversight meetings;  
1219           system security plan; other relevant documents or records]

1220           **Interview**

1221           [SELECT FROM: personnel with configuration change control responsibilities; personnel with  
1222           information security responsibilities; members of change control board or similar; system  
1223           administrators]

1224           **Test**

1225           [SELECT FROM: processes for configuration change control; mechanisms that implement  
1226           configuration change control]

1227           **REFERENCES**

1228           Source Assessment Procedure: [CM-03](#)

1229   **3.4.4. Impact Analyses**

1230           **REQUIREMENT:** 03.04.04

1231           **ASSESSMENT OBJECTIVE**

1232           *Determine if:*

1233 **A.03.04.04:** changes to the system are analyzed for security impact prior to implementation.

1234 **ASSESSMENT METHODS AND OBJECTS**

1235 **Examine**

1236 [SELECT FROM: configuration management policy and procedures; procedures for security  
1237 impact analyses for system changes; configuration management plan; security impact analysis  
1238 documentation; system design documentation; analysis tools and outputs; change control  
1239 records; system audit records; system security plan; other relevant documents or records]

1240 **Interview**

1241 [SELECT FROM: personnel with security impact analysis responsibilities; personnel with  
1242 information security responsibilities; members of change control board; system developers;  
1243 system administrators]

1244 **Test**

1245 [SELECT FROM: processes for security impact analyses]

1246 **REFERENCES**

1247 Source Assessment Procedure: [CM-04](#)

1248 **3.4.5. Access Restrictions for Change**

1249 **REQUIREMENT:** 03.04.05

1250 **ASSESSMENT OBJECTIVE**

1251 *Determine if:*

1252 **A.03.04.05[01]:** physical access restrictions associated with changes to the system are defined  
1253 and documented.

1254 **A.03.04.05[02]:** physical access restrictions associated with changes to the system are  
1255 approved.

1256 **A.03.04.05[03]:** physical access restrictions associated with changes to the system are enforced.

1257 **A.03.04.05[04]:** logical access restrictions associated with changes to the system are defined  
1258 and documented.

1259 **A.03.04.05[05]:** logical access restrictions associated with changes to the system are approved.

1260 **A.03.04.05[06]:** logical access restrictions associated with changes to the system are enforced.

1261 **ASSESSMENT METHODS AND OBJECTS**

1262 **Examine**

1263 [SELECT FROM: configuration management policy and procedures; procedures for access  
1264 restrictions for system changes; configuration management plan; system design documentation;  
1265 system architecture; system configuration settings; logical access approvals; physical access  
1266 approvals; access credentials; change control records; system audit records; system security  
1267 plan; other relevant documents or records]

1268 **Interview**

1269 [SELECT FROM: personnel with logical access control responsibilities; personnel with physical  
1270 access control responsibilities; personnel with information security responsibilities; system  
1271 administrators]

1272           **Test**  
1273           [SELECT FROM: processes for managing access restrictions for system changes; mechanisms  
1274           for supporting, implementing, or enforcing access restrictions associated with system changes]

1275           **REFERENCES**

1276           Source Assessment Procedure: [CM-05](#)

1277   **3.4.6. Least Functionality**

1278           **REQUIREMENT:** 03.04.06

1279           **ASSESSMENT OBJECTIVE**

1280           *Determine if:*

1281           **A.03.04.06.ODP[01]: functions to be prohibited or restricted are defined.**

1282           **A.03.04.06.ODP[02]: ports to be prohibited or restricted are defined.**

1283           **A.03.04.06.ODP[03]: protocols to be prohibited or restricted are defined.**

1284           **A.03.04.06.ODP[04]: connections to be prohibited or restricted are defined.**

1285           **A.03.04.06.ODP[05]: services to be prohibited or restricted are defined.**

1286           **A.03.04.06.ODP[06]: functions deemed unnecessary or non-secure are defined.**

1287           **A.03.04.06.ODP[07]: ports deemed unnecessary or non-secure are defined.**

1288           **A.03.04.06.ODP[08]: protocols deemed unnecessary or non-secure are defined.**

1289           **A.03.04.06.ODP[09]: connections deemed unnecessary or non-secure are defined.**

1290           **A.03.04.06.ODP[10]: services deemed unnecessary or non-secure are defined.**

1291           **A.03.04.06.a:** the system is configured to provide only mission-essential capabilities.

1292           **A.03.04.06.b[01]:** the use of the following functions is prohibited or restricted:

1293           **<A.03.04.06.ODP[01]: functions>.**

1294           **A.03.04.06.b[02]:** the use of the following ports is prohibited or restricted: **<A.03.04.06.ODP[02]:**  
1295           **ports>.**

1296           **A.03.04.06.b[03]:** the use of the following protocols is prohibited or restricted:

1297           **<A.03.04.06.ODP[03]: protocols>.**

1298           **A.03.04.06.b[04]:** the use of the following connections is prohibited or restricted:

1299           **<A.03.04.06.ODP[04]: connections>.**

1300           **A.03.04.06.b[05]:** the use of the following services is prohibited or restricted:

1301           **<A.03.04.06.ODP[05]: services>.**

1302           **A.03.04.06.c:** the system is reviewed periodically to identify unnecessary or nonsecure functions,  
1303           ports, protocols, connections, and services.

1304           **A.03.04.06.d[01]:** the following unnecessary or nonsecure functions are disabled or removed:

1305           **<A.03.04.06.ODP[06]: functions>.**

1306           **A.03.04.06.d[02]:** the following unnecessary or nonsecure ports are disabled or removed:

1307           **<A.03.04.06.ODP[07]: ports>.**

1308           **A.03.04.06.d[03]:** the following unnecessary or nonsecure protocols are disabled or removed:

1309           **<A.03.04.06.ODP[08]: protocols>.**

1310 **A.03.04.06.d[04]:** the following unnecessary or nonsecure connections are disabled or removed:  
1311 **<A.03.04.06.ODP[09]: connections>**.

1312 **A.03.04.06.d[05]:** the following unnecessary or nonsecure services are disabled or removed:  
1313 **<A.03.04.06.ODP[10]: services>**.

## 1314 **ASSESSMENT METHODS AND OBJECTS**

### 1315 **Examine**

1316 [SELECT FROM: configuration management policy and procedures; procedures for least  
1317 functionality in the system; configuration management plan; system design documentation;  
1318 system configuration settings; system component inventory; common secure configuration  
1319 checklists; documented reviews of functions, ports, protocols, and services; change control  
1320 records; system audit records; system security plan; other relevant documents or records]

### 1321 **Interview**

1322 [SELECT FROM: personnel with configuration management responsibilities; personnel with  
1323 responsibilities for reviewing functions, ports, protocols, and services; personnel with information  
1324 security responsibilities; system developers; system administrators]

### 1325 **Test**

1326 [SELECT FROM: processes for prohibiting or restricting functions, ports, protocols, and services;  
1327 processes for reviewing or disabling functions, ports, protocols, and services; mechanisms for  
1328 implementing the review and disabling of functions, ports, protocols, and services; mechanisms  
1329 for implementing restrictions on or the prohibition of functions, ports, protocols, and services]

## 1330 **REFERENCES**

1331 Source Assessment Procedures: [CM-07](#), [CM-07\(01\)](#)

### 1332 **3.4.7. Withdrawn**

1333 Incorporated into [03.04.06](#).

### 1334 **3.4.8. Authorized Software – Allow by Exception**

1335 **REQUIREMENT:** 03.04.08

#### 1336 **ASSESSMENT OBJECTIVE**

1337 *Determine if:*

1338 **A.03.04.08.a:** software programs authorized to execute on the system are identified.

1339 **A.03.04.08.b:** a deny-all, allow-by-exception policy for the execution of software programs on the  
1340 system is implemented.

1341 **A.03.04.08.c[01]:** the list of authorized software programs is reviewed periodically.

1342 **A.03.04.08.c[02]:** the list of authorized software programs is updated periodically.

## 1343 **ASSESSMENT METHODS AND OBJECTS**

### 1344 **Examine**

1345 [SELECT FROM: configuration management policy and procedures; procedures for least  
1346 functionality in the system; configuration management plan; system design documentation;  
1347 system configuration settings; list of software programs authorized to execute on the system;

1348 system component inventory; common secure configuration checklists; review and update  
1349 records associated with list of authorized software programs; change control records; system  
1350 audit records; system security plan; other relevant documents or records]

1351 **Interview**

1352 [SELECT FROM: personnel with responsibilities for identifying software authorized to execute on  
1353 the system; personnel with information security responsibilities; system administrators]

1354 **Test**

1355 [SELECT FROM: processes for identifying, reviewing, and updating programs authorized to  
1356 execute on the system; processes for implementing authorized software policy; mechanisms for  
1357 supporting and/or implementing authorized software policy]

1358 **REFERENCES**

1359 Source Assessment Procedure: [CM-07\(05\)](#)

1360 **3.4.9. Withdrawn**

1361 Addressed by [03.01.05](#), [03.01.06](#), [03.01.07](#), and [03.04.08](#).

1362 **3.4.10. System Component Inventory**

1363 **REQUIREMENT:** 03.04.10

1364 **ASSESSMENT OBJECTIVE**

1365 *Determine if:*

1366 **A.03.04.10.a:** an inventory of system components is developed and documented.

1367 **A.03.04.10.b[01]:** the system component inventory is reviewed periodically.

1368 **A.03.04.10.b[02]:** the system component inventory is updated periodically.

1369 **A.03.04.10.c[01]:** the system component inventory is updated as part of component  
1370 installations.

1371 **A.03.04.10.c[02]:** the system component inventory is updated as part of component removals.

1372 **A.03.04.10.c[03]:** the system component inventory is updated as part of system updates.

1373 **ASSESSMENT METHODS AND OBJECTS**

1374 **Examine**

1375 [SELECT FROM: configuration management policy and procedures; procedures for system  
1376 component inventory; configuration management plan; system design documentation; system  
1377 component inventory; inventory reviews and update records; component installation records;  
1378 change control records; component removal records; system change records; system security  
1379 plan; other relevant documents or records]

1380 **Interview**

1381 [SELECT FROM: personnel with component inventory management responsibilities; personnel  
1382 with information security responsibilities; system administrators]

1383           **Test**

1384           [SELECT FROM: processes for managing the system component inventory; mechanisms for  
1385 supporting and/or implementing the system component inventory; processes for updating the  
1386 system component inventory; mechanisms for supporting and/or implementing the system  
1387 component inventory updates]

1388           **REFERENCES**

1389           Source Assessment Procedures: [CM-08](#), [CM-08\(01\)](#)

1390   **3.4.11. Information Location**

1391           **REQUIREMENT: 03.04.11**

1392           **ASSESSMENT OBJECTIVE**

1393           *Determine if:*

1394           **A.03.04.11.a[01]:** the location of CUI is identified and documented.

1395           **A.03.04.11.a[02]:** the system components on which CUI is processed are identified and  
1396 documented.

1397           **A.03.04.11.a[03]:** the system components on which CUI is stored are identified and  
1398 documented.

1399           **A.03.04.11.b[01]:** users who have access to the system and system components where CUI is  
1400 processed are identified and documented.

1401           **A.03.04.11.b[02]:** users who have access to the system and system components where CUI is  
1402 stored are identified and documented.

1403           **A.03.04.11.c[01]:** changes to the location (i.e., system or system components) where CUI is  
1404 processed are documented.

1405           **A.03.04.11.c[02]:** changes to the location (i.e., system or system components) where CUI is  
1406 stored are documented.

1407           **ASSESSMENT METHODS AND OBJECTS**

1408           **Examine**

1409           [SELECT FROM: configuration management policy and procedures; configuration management  
1410 plan; procedures for identification and documentation of information location; system; audit  
1411 records; architecture documentation; system design documentation; list of users with system  
1412 and system component access; change control records; system component inventory; system  
1413 security plan; other relevant documents or records]

1414           **Interview**

1415           [SELECT FROM: personnel with responsibilities for managing information location and user  
1416 access; personnel with responsibilities for operating, using, and/or maintaining the system;  
1417 personnel with information security responsibilities; system developers; system administrators]

1418           **Test**

1419           [SELECT FROM: processes governing information location; mechanisms for enforcing policies  
1420 and methods for governing information location]

1421           **REFERENCES**

1422           Source Assessment Procedure: [CM-12](#)

1423 **3.4.12. System and Component Configuration for High-Risk Areas**

1424 **REQUIREMENT:** 03.04.12

1425 **ASSESSMENT OBJECTIVE**

1426 *Determine if:*

1427 **A.03.04.12.ODP[01]: configurations for systems or system components to be issued to**  
1428 **individuals traveling to high-risk locations are defined.**

1429 **A.03.04.12.ODP[02]: the security requirements to be applied to the system or system**  
1430 **components when individuals return from travel are defined.**

1431 **A.03.04.12.a:** systems or system components with the following configurations are issued to  
1432 individuals traveling to high-risk locations: **<A.03.04.12.ODP[01]: configurations>**.

1433 **A.03.04.12.b:** the following security requirements are applied to the system or system  
1434 components when the individuals return from travel: **<A.03.04.12.ODP[02]: requirements>**.

1435 **ASSESSMENT METHODS AND OBJECTS**

1436 **Examine**

1437 [SELECT FROM: configuration management policy and procedures; configuration management  
1438 plan; procedures for the baseline configuration of the system; procedures for system component  
1439 installations and upgrades; system component inventory; system component installations or  
1440 upgrades and associated records; records of system baseline configuration reviews and  
1441 updates; system configuration settings; system architecture; change control records; system  
1442 security plan; other relevant documents or records]

1443 **Interview**

1444 [SELECT FROM: personnel with configuration management responsibilities; personnel with  
1445 information security responsibilities; system administrators]

1446 **Test**

1447 [SELECT FROM: processes for managing baseline configurations]

1448 **REFERENCES**

1449 Source Assessment Procedure: [CM-02\(07\)](#)

1450 **3.5. [Identification and Authentication](#)**

1451 **3.5.1. User Identification, Authentication, and Re-Authentication**

1452 **REQUIREMENT:** 03.05.01

1453 **ASSESSMENT OBJECTIVE**

1454 *Determine if:*

1455 **A.03.05.01.ODP[01]: circumstances or situations that require re-authentication are defined.**

1456 **A.03.05.01.a[01]:** system users are uniquely identified and authenticated.

1457 **A.03.05.01.a[02]:** the unique identification of authenticated system users is associated with  
1458 processes acting on behalf of those users.



1459 **A.03.05.01.b:** users are reauthenticated when **<A.03.05.01.ODP[01]: circumstances or**  
1460 **situations>**.

1461 **ASSESSMENT METHODS AND OBJECTS**

1462 **Examine**

1463 [SELECT FROM: identification and authentication policy and procedures; list of circumstances or  
1464 situations requiring re-authentication; system design documentation; system configuration  
1465 settings; system audit records; list of system accounts; system security plan; other relevant  
1466 documents or records]

1467 **Interview**

1468 [SELECT FROM: personnel with identification and authentication responsibilities; personnel with  
1469 system operations responsibilities; personnel with account management responsibilities; system  
1470 developers; personnel with information security responsibilities; system administrators]

1471 **Test**

1472 [SELECT FROM: processes for uniquely identifying and authenticating users; mechanisms for  
1473 supporting and/or implementing identification and authentication capabilities]

1474 **REFERENCES**

1475 Source Assessment Procedures: [IA-02](#), [IA-11](#)

1476 **3.5.2. Device Identification and Authentication**

1477 **REQUIREMENT:** 03.05.02

1478 **ASSESSMENT OBJECTIVE**

1479 *Determine if:*

1480 **A.03.05.02:** devices are uniquely identified and authenticated before establishing a system  
1481 connection.

1482 **ASSESSMENT METHODS AND OBJECTS**

1483 **Examine**

1484 [SELECT FROM: identification and authentication policy and procedures; procedures for device  
1485 identification and authentication; system design documentation; list of devices requiring unique  
1486 identification and authentication; device connection reports; system configuration settings; system  
1487 security plan; other relevant documents or records]

1488 **Interview**

1489 [SELECT FROM: personnel with responsibilities for device identification and authentication;  
1490 personnel with information security responsibilities; system developers; system administrators]

1491 **Test**

1492 [SELECT FROM: mechanisms for supporting and/or implementing device identification and  
1493 authentication capabilities]

1494 **REFERENCES**

1495 Source Assessment Procedure: [IA-03](#)

1496 **3.5.3. Multi-Factor Authentication**

1497 **REQUIREMENT:** 03.05.03

1498 **ASSESSMENT OBJECTIVE**

1499 *Determine if:*

1500 **A.03.05.03:** multi-factor authentication for access to system accounts is implemented.

1501 **ASSESSMENT METHODS AND OBJECTS**

1502 **Examine**

1503 [SELECT FROM: identification and authentication policy and procedures; system design  
1504 documentation; list of system accounts; system configuration settings; system audit records;  
1505 system security plan; other relevant documents or records]

1506 **Interview**

1507 [SELECT FROM: personnel with system operations responsibilities; personnel with account  
1508 management responsibilities; personnel with information security responsibilities; system  
1509 developers; system administrators]

1510 **Test**

1511 [SELECT FROM: mechanisms for supporting and/or implementing a multi-factor authentication  
1512 capability]

1513 **REFERENCES**

1514 Source Assessment Procedures: [IA-02\(01\)](#), [IA-02\(02\)](#)

1515 **3.5.4. Replay-Resistant Authentication**

1516 **REQUIREMENT:** 03.05.04

1517 **ASSESSMENT OBJECTIVE**

1518 *Determine if:*

1519 **A.03.05.04:** replay-resistant authentication mechanisms for access to system accounts are  
1520 implemented.

1521 **ASSESSMENT METHODS AND OBJECTS**

1522 **Examine**

1523 [SELECT FROM: identification and authentication policy and procedures; system design  
1524 documentation; system audit records; system configuration settings; list of privileged system  
1525 accounts; system security plan; other relevant documents or records]

1526 **Interview**

1527 [SELECT FROM: personnel with system operations responsibilities; personnel with account  
1528 management responsibilities; personnel with information security responsibilities; system  
1529 developers; system administrators]

1530 **Test**

1531 [SELECT FROM: mechanisms for supporting and/or implementing identification and  
1532 authentication capabilities; mechanisms for supporting and/or implementing replay-resistance]

1533           **REFERENCES**

1534           Source Assessment Procedure: [IA-02\(08\)](#)

1535   **3.5.5. Identifier Management**

1536           **REQUIREMENT:** 03.05.05

1537           **ASSESSMENT OBJECTIVE**

1538           *Determine if:*

1539           **A.03.05.05.ODP[01]: personnel or roles from whom authorization must be received to**  
1540           **assign an identifier are defined.**

1541           **A.03.05.05.ODP[02]: a time period for preventing the reuse of identifiers is defined.**

1542           **A.03.05.05.a:** authorization is received from **<A.03.05.05.ODP[01]: personnel or roles>** to  
1543           assign an individual, group, role, service, or device identifier.

1544           **A.03.05.05.b[01]:** an identifier that identifies an individual, group, role, service, or device is  
1545           selected.

1546           **A.03.05.05.b[02]:** an identifier that identifies an individual, group, role, service, or device is  
1547           assigned.

1548           **A.03.05.05.c:** the reuse of identifiers for **<A.03.05.05.ODP[02]: time period>** is prevented.

1549           **A.03.05.05.d:** the status of each individual is uniquely identified with an identifying characteristic.

1550           **ASSESSMENT METHODS AND OBJECTS**

1551           **Examine**

1552           [SELECT FROM: identification and authentication policy and procedures; procedures for identifier  
1553           management; procedures for account management; system design documentation; list of system  
1554           accounts; list of characteristics identifying individual status; system configuration settings; list of  
1555           identifiers generated from physical access control devices; system security plan; other relevant  
1556           documents or records]

1557           **Interview**

1558           [SELECT FROM: personnel with identifier management responsibilities; personnel with  
1559           information security responsibilities; system developers; system administrators]

1560           **Test**

1561           [SELECT FROM: mechanisms for supporting and/or implementing identifier management]

1562           **REFERENCES**

1563           Source Assessment Procedures: [IA-04](#), [IA-04\(04\)](#)

1564   **3.5.6. Withdrawn**

1565   **3.5.7. Password Management**

1566           **REQUIREMENT:** 03.05.07

1567 **ASSESSMENT OBJECTIVE**

1568 *Determine if:*

1569 **A.03.05.07.ODP[01]: password composition and complexity rules are defined.**

1570 **A.03.05.07.a[01]:** a list of commonly used, expected, or compromised passwords is maintained.

1571 **A.03.05.07.a[02]:** a list of commonly used, expected, or compromised passwords is updated  
1572 periodically.

1573 **A.03.05.07.a[03]:** a list of commonly used, expected, or compromised passwords is updated  
1574 when organizational passwords are suspected to have been compromised.

1575 **A.03.05.07.b:** passwords are verified not to be found on the list of commonly used, expected, or  
1576 compromised passwords when they are created or updated by users.

1577 **A.03.05.07.c:** passwords are only transmitted over cryptographically protected channels.

1578 **A.03.05.07.d:** passwords are stored in a cryptographically protected form.

1579 **A.03.05.07.e:** a new password is selected upon first use after account recovery.

1580 **A.03.05.07.f:** the following composition and complexity rules are enforced: **<A.03.05.07.ODP[01]:**  
1581 **rules>.**

1582 **ASSESSMENT METHODS AND OBJECTS**

1583 **Examine**

1584 [SELECT FROM: identification and authentication policy and procedures; password policy;  
1585 procedures for authenticator management; system design documentation; system configuration  
1586 settings; password configurations; system security plan; other relevant documents or records]

1587 **Interview**

1588 [SELECT FROM: personnel with authenticator management responsibilities; personnel with  
1589 information security responsibilities; system developers; system administrators]

1590 **Test**

1591 [SELECT FROM: mechanisms for supporting and/or implementing a password-based  
1592 authenticator management capability]

1593 **REFERENCES**

1594 Source Assessment Procedure: [IA-05\(01\)](#)

1595 **3.5.8.** Withdrawn

1596 **3.5.9.** Withdrawn

1597 Incorporated into [03.05.07](#).

1598 **3.5.10.** Withdrawn

1599 Incorporated into [03.05.07](#).

1600 **3.5.11. Authentication Feedback**

1601 **REQUIREMENT:** 03.05.11

1602 **ASSESSMENT OBJECTIVE**

1603 *Determine if:*

1604 **A.03.05.11:** feedback of authentication information during the authentication process is  
1605 obscured.

1606 **ASSESSMENT METHODS AND OBJECTS**

1607 **Examine**

1608 [SELECT FROM: identification and authentication policy and procedures; procedures for  
1609 authenticator feedback; system design documentation; system configuration settings; system  
1610 audit records; system security plan; other relevant documents or records]

1611 **Interview**

1612 [SELECT FROM: personnel with information security responsibilities; system developers;  
1613 system administrators]

1614 **Test**

1615 [SELECT FROM: mechanisms for supporting and/or implementing the obscuring of feedback of  
1616 authentication information during authentication]

1617 **REFERENCES**

1618 Source Assessment Procedure: [IA-06](#)

1619 **3.5.12. Authenticator Management**

1620 **REQUIREMENT:** 03.05.12

1621 **ASSESSMENT OBJECTIVE**

1622 *Determine if:*

1623 **A.03.05.12.ODP[01]:** *events that trigger the change or refreshment of authenticators are*  
1624 *defined.*

1625 **A.03.05.12.a:** the identity of the individual, group, role, service, or device receiving the  
1626 authenticator as part of the initial authenticator distribution is verified.

1627 **A.03.05.12.b:** initial authenticator content for any authenticators issued by the organization is  
1628 established.

1629 **A.03.05.12.c[01]:** administrative procedures for initial authenticator distribution are established  
1630 and implemented.

1631 **A.03.05.12.c[02]:** administrative procedures for lost, compromised, or damaged authenticators  
1632 are established and implemented.

1633 **A.03.05.12.c[03]:** administrative procedures for revoking authenticators are established and  
1634 implemented.

1635 **A.03.05.12.d:** default authenticators are changed at first use.

1636 **A.03.05.12.e:** authenticators are changed and refreshed periodically or when the following  
1637 events occur: **<A.03.05.12.ODP[01]: events>**.

1638 **A.03.05.12.f[01]:** authenticator content is protected from unauthorized disclosure.

1639 **A.03.05.12.f[01]:** authenticator content is protected from unauthorized modification.

## 1640 **ASSESSMENT METHODS AND OBJECTS**

### 1641 **Examine**

1642 [SELECT FROM: identification and authentication policy and procedures; procedures for  
1643 authenticator management; system configuration settings; list of system authenticator types;  
1644 system design documentation; system audit records; change control records associated with  
1645 managing system authenticators; system security plan; other relevant documents or records]

### 1646 **Interview**

1647 [SELECT FROM: personnel with authenticator management responsibilities; personnel with  
1648 information security responsibilities; system administrators]

### 1649 **Test**

1650 [SELECT FROM: mechanisms for supporting and/or implementing the authenticator  
1651 management capability]

## 1652 **REFERENCES**

1653 Source Assessment Procedure: [IA-05](#)

## 1654 **3.6. [Incident Response](#)**

### 1655 **3.6.1. Incident Response Plan and Handling**

1656 **REQUIREMENT:** 03.06.01

#### 1657 **ASSESSMENT OBJECTIVE**

1658 *Determine if:*

1659 **A.03.06.01.a:** an incident response plan that provides the organization with a roadmap for  
1660 implementing its incident response capability is developed.

1661 **A.03.06.01.b[01]:** an incident-handling capability for incidents that is consistent with the incident  
1662 response plan is implemented.

1663 **A.03.06.01.b[02]:** the incident handling capability for incidents includes preparation.

1664 **A.03.06.01.b[03]:** the incident handling capability for incidents includes detection and analysis.

1665 **A.03.06.01.b[04]:** the incident handling capability for incidents includes containment.

1666 **A.03.06.01.b[05]:** the incident handling capability for incidents includes eradication.

1667 **A.03.06.01.b[06]:** the incident handling capability for incidents includes recovery.

1668 **A.03.06.01.c:** the incident response plan is updated to address system and organizational  
1669 changes or problems encountered during plan implementation, execution, or testing.

## 1670 **ASSESSMENT METHODS AND OBJECTS**

### 1671 **Examine**

1672 [SELECT FROM: incident response policy and procedures; contingency planning policy and  
1673 procedures; procedures for incident handling; procedures for incident response planning; incident

1674 response plan; contingency plan; records of incident response plan reviews and approvals;  
1675 system security plan; other relevant documents or records]

1676 **Interview**

1677 [SELECT FROM: personnel with incident handling responsibilities; personnel with incident  
1678 response planning responsibilities; personnel with contingency planning responsibilities;  
1679 personnel with information security responsibilities]

1680 **Test**

1681 [SELECT FROM: incident handling capability for the organization; incident response plan]

1682 **REFERENCES**

1683 Source Assessment Procedures: [IR-04](#), [IR-08](#)

1684 **3.6.2. Incident Monitoring, Reporting, and Response Assistance**

1685 **REQUIREMENT:** 03.06.02

1686 **ASSESSMENT OBJECTIVE**

1687 *Determine if:*

1688 **A.03.06.02.ODP[01]:** *the time period to report suspected incidents to the organizational*  
1689 *incident response capability is defined.*

1690 **A.03.06.02.ODP[02]:** *authorities to whom incident information is to be reported are defined.*

1691 **A.03.06.02.a[01]:** system security incidents are tracked.

1692 **A.03.06.02.a[02]:** system security incidents are documented.

1693 **A.03.06.02.b:** suspected incidents are reported to the organizational incident response capability  
1694 within **<A.03.06.02.ODP[01]: time period>**.

1695 **A.03.06.02.c:** incident information is reported to **<A.03.06.02.ODP[02]: authorities>**.

1696 **A.03.06.02.d:** an incident response support resource that offers advice and assistance to users of  
1697 the system for the handling and reporting of incidents is provided.

1698 **ASSESSMENT METHODS AND OBJECTS**

1699 **Examine**

1700 [SELECT FROM: incident response policy and procedures; procedures for incident monitoring;  
1701 procedures for incident response assistance; incident response records and documentation;  
1702 incident response plan; system security plan; other relevant documents or records]

1703 **Interview**

1704 [SELECT FROM: personnel with incident monitoring responsibilities; personnel with incident  
1705 response assistance and support responsibilities; personnel with information security  
1706 responsibilities]

1707 **Test**

1708 [SELECT FROM: processes for incident reporting; incident monitoring capability; mechanisms for  
1709 supporting and/or implementing the tracking and documenting of system security incidents;  
1710 mechanisms for supporting and/or implementing incident reporting; mechanisms for supporting  
1711 and/or implementing incident response assistance; processes for incident response assistance]

1712           **REFERENCES**

1713           Source Assessment Procedures: [IR-05](#), [IR-06](#), [IR-07](#)

1714   **3.6.3. Incident Response Testing**

1715           **REQUIREMENT:** 03.06.03

1716           **ASSESSMENT OBJECTIVE**

1717           *Determine if:*

1718           **A.03.06.03:** the effectiveness of the incident response capability is tested periodically.

1719           **ASSESSMENT METHODS AND OBJECTS**

1720           **Examine**

1721           [SELECT FROM: incident response policy and procedures; contingency planning policy and  
1722           procedures; procedures for incident response testing; procedures for contingency plan testing;  
1723           incident response testing material; incident response test results; incident response test plan;  
1724           incident response plan; contingency plan; system security plan; other relevant documents or  
1725           records]

1726           **Interview**

1727           [SELECT FROM: personnel with incident response testing responsibilities; personnel with  
1728           information security responsibilities]

1729           **REFERENCES**

1730           Source Assessment Procedure: [IR-03](#)

1731   **3.6.4. Incident Response Training**

1732           **REQUIREMENT:** 03.06.04

1733           **ASSESSMENT OBJECTIVE**

1734           *Determine if:*

1735           **A.03.06.04.ODP[01]:** *a time period within which incident response training is to be*  
1736           *provided to system users is defined.*

1737           **A.03.06.04.ODP[02]:** *events that initiate a review of the incident response training content*  
1738           *are defined.*

1739           **A.03.06.04.a.01:** incident response training for system users consistent with assigned roles and  
1740           responsibilities is provided within **<A.03.06.04.ODP[01]: time period>** of assuming an incident  
1741           response role or responsibility or acquiring system access.

1742           **A.03.06.04.a.02:** incident response training for system users consistent with assigned roles and  
1743           responsibilities is provided when required by system changes.

1744           **A.03.06.04.a.03:** incident response training for system users consistent with assigned roles and  
1745           responsibilities is provided periodically after initial and event-driven training.

1746           **A.03.06.04.b[01]:** incident response training content is reviewed periodically.

1747           **A.03.06.04.b[02]:** incident response training content is reviewed following **<A.03.06.04.ODP[02]:**  
1748           **events>**.



1749 **A.03.06.04.b[03]**: incident response training content is updated periodically.

1750 **A.03.06.04.b[04]**: incident response training content is updated following **<A.03.06.04.ODP[02]:**  
1751 **events>**.

## 1752 **ASSESSMENT METHODS AND OBJECTS**

### 1753 **Examine**

1754 [SELECT FROM: incident response policy and procedures; procedures for incident response  
1755 training; incident response training curriculum; incident response training materials; incident  
1756 response plan; incident response training records; system security plan; other relevant  
1757 documents or records]

### 1758 **Interview**

1759 [SELECT FROM: personnel with incident response training and operational responsibilities;  
1760 personnel with information security responsibilities]

## 1761 **REFERENCES**

1762 Source Assessment Procedure: [IR-02](#)

## 1763 **3.7. [Maintenance](#)**

### 1764 **3.7.1. Withdrawn**

1765 Recategorized as NCO.

### 1766 **3.7.2. Withdrawn**

1767 Incorporated into [03.07.04](#) and [03.07.06](#).

### 1768 **3.7.3. Withdrawn**

1769 Incorporated into [03.08.03](#).

## 1770 **3.7.4. Maintenance Tools**

1771 **REQUIREMENT:** 03.07.04

### 1772 **ASSESSMENT OBJECTIVE**

1773 *Determine if:*

1774 **A.03.07.04.a[01]**: the use of system maintenance tools is approved.

1775 **A.03.07.04.a[02]**: the use of system maintenance tools is controlled.

1776 **A.03.07.04.a[03]**: the use of system maintenance tools is monitored.

1777 **A.03.07.04.b**: maintenance tools are inspected for improper or unauthorized modifications.

1778 **A.03.07.04.c**: media that contain diagnostic and test programs are checked for malicious code  
1779 before being used in the system.

1780 **A.03.07.04.d:** the removal of system maintenance equipment containing CUI is prevented by  
1781 verifying that there is no CUI on the equipment; sanitizing or destroying the equipment; or  
1782 retaining the equipment within the facility.

### 1783 **ASSESSMENT METHODS AND OBJECTS**

#### 1784 **Examine**

1785 [SELECT FROM: maintenance policy and procedures; procedures for system maintenance tools;  
1786 system maintenance tools; maintenance tool inspection records; equipment sanitization records;  
1787 media sanitization records; system security plan; other relevant documents or records]

#### 1788 **Interview**

1789 [SELECT FROM: personnel with system maintenance responsibilities; personnel responsible for  
1790 media sanitization; personnel with information security responsibilities]

#### 1791 **Test**

1792 [SELECT FROM: processes for approving, controlling, and monitoring maintenance tools;  
1793 mechanisms for supporting and/or implementing the approval, control, and/or monitoring of  
1794 maintenance tools; processes for preventing the unauthorized removal of information; processes  
1795 for inspecting media for malicious code; mechanisms for supporting media sanitization or the  
1796 destruction of equipment; mechanisms for supporting the verification of media sanitization;  
1797 processes for inspecting maintenance tools; mechanisms for supporting and/or implementing the  
1798 inspection of maintenance tools; mechanisms for supporting and/or implementing the inspection  
1799 of media used for maintenance]

### 1800 **REFERENCES**

1801 Source Assessment Procedures: [MA-03](#), [MA-03\(01\)](#), [MA-03\(02\)](#), [MA-03\(03\)](#)

## 1802 **3.7.5. Nonlocal Maintenance**

1803 **REQUIREMENT:** 03.07.05

### 1804 **ASSESSMENT OBJECTIVE**

1805 *Determine if:*

1806 **A.03.07.05.a[01]:** nonlocal maintenance and diagnostic activities are approved.

1807 **A.03.07.05.a[02]:** nonlocal maintenance and diagnostic activities are monitored.

1808 **A.03.07.05.b:** multi-factor authentication and replay resistance are implemented in the  
1809 establishment of nonlocal maintenance and diagnostic sessions.

1810 **A.03.07.05.c[01]:** session connections are terminated when nonlocal maintenance is completed.

1811 **A.03.07.05.c[02]:** network connections are terminated when nonlocal maintenance is completed.

### 1812 **ASSESSMENT METHODS AND OBJECTS**

#### 1813 **Examine**

1814 [SELECT FROM: maintenance policy and procedures; remote access policy and procedures;  
1815 procedures for nonlocal system maintenance; records of remote access; maintenance records;  
1816 diagnostic records; system design documentation; system configuration settings; system security  
1817 plan; other relevant documents or records]

1818 **Interview**  
1819 [SELECT FROM: personnel with system maintenance responsibilities; personnel with information  
1820 security responsibilities; system administrators]

1821 **Test**  
1822 [SELECT FROM: processes for managing nonlocal maintenance; mechanisms for implementing,  
1823 supporting, and/or managing nonlocal maintenance; mechanisms for implementing multi-factor  
1824 authentication and replay resistance; mechanisms for terminating nonlocal maintenance sessions  
1825 and network connections]

1826 **REFERENCES**

1827 Source Assessment Procedure: [MA-04](#)

1828 **3.7.6. Maintenance Personnel**

1829 **REQUIREMENT:** 03.07.06

1830 **ASSESSMENT OBJECTIVE**

1831 *Determine if:*

1832 **A.03.07.06.a:** a process for maintenance personnel authorization is established.

1833 **A.03.07.06.b:** a list of authorized maintenance organizations or personnel is maintained.

1834 **A.03.07.06.c:** verification is performed that non-escorted personnel who perform maintenance on  
1835 the system possess the required access authorizations.

1836 **A.03.07.06.d:** organizational personnel with required access authorizations and technical  
1837 competence are designated to supervise the maintenance activities of personnel who do not  
1838 possess the required access authorizations.

1839 **ASSESSMENT METHODS AND OBJECTS**

1840 **Examine**

1841 [SELECT FROM: maintenance policy and procedures; service provider contracts; service-level  
1842 agreements; list of authorized personnel; maintenance records; access control records; system  
1843 security plan; other relevant documents or records]

1844 **Interview**

1845 [SELECT FROM: personnel with system maintenance responsibilities; personnel with information  
1846 security responsibilities]

1847 **Test**

1848 [SELECT FROM: processes for authorizing and managing maintenance personnel; mechanisms  
1849 for supporting and/or implementing the authorization of maintenance personnel]

1850 **REFERENCES**

1851 Source Assessment Procedure: [MA-05](#)

1852 **3.8. [Media Protection](#)**

1853 **3.8.1. Media Storage**

1854 **REQUIREMENT:** 03.08.01

1855 **ASSESSMENT OBJECTIVE**

1856 *Determine if:*

1857 **A.03.08.01[01]:** system media that contain CUI are physically controlled until the media are  
1858 sanitized or destroyed using approved equipment, techniques, and procedures.

1859 **A.03.08.01[02]:** system media that contain CUI are securely stored until the media are sanitized  
1860 or destroyed using approved equipment, techniques, and procedures.

1861 **ASSESSMENT METHODS AND OBJECTS**

1862 **Examine**

1863 [SELECT FROM: physical protection policy and procedures; media protection policy and  
1864 procedures; procedures for media storage; access control policy and procedures; system media;  
1865 system security plan; other relevant documents or records]

1866 **Interview**

1867 [SELECT FROM: personnel with system media protection and storage responsibilities; personnel  
1868 with information security responsibilities]

1869 **Test**

1870 [SELECT FROM: processes for storing information media; mechanisms for supporting and/or  
1871 implementing secure media storage/media protection]

1872 **REFERENCES**

1873 Source Assessment Procedure: [MP-04](#)

1874 **3.8.2. Media Access**

1875 **REQUIREMENT:** 03.08.02

1876 **ASSESSMENT OBJECTIVE**

1877 *Determine if:*

1878 **A.03.08.02:** access to CUI on system media is restricted.

1879 **ASSESSMENT METHODS AND OBJECTS**

1880 **Examine**

1881 [SELECT FROM: physical protection policy and procedures; media protection policy and  
1882 procedures; procedures for media access restrictions; access control policy and procedures;  
1883 media storage facilities; access control records; system security plan; other relevant documents  
1884 or records]

1885 **Interview**

1886 [SELECT FROM: personnel with system media protection responsibilities; personnel with  
1887 information security responsibilities; system administrators]

1888 **Test**  
1889 [SELECT FROM: processes for restricting information on media; mechanisms supporting and/or  
1890 implementing media access restrictions]

1891 **REFERENCES**

1892 Source Assessment Procedure: [MP-02](#)

1893 **3.8.3. Media Sanitization**

1894 **REQUIREMENT:** 03.08.03

1895 **ASSESSMENT OBJECTIVE**

1896 *Determine if:*

1897 **A.03.08.03:** system media that contain CUI are sanitized prior to disposal, release out of  
1898 organizational control, or release for reuse.

1899 **ASSESSMENT METHODS AND OBJECTS**

1900 **Examine**

1901 [SELECT FROM: media protection policy and procedures; procedures for media sanitization and  
1902 disposal; applicable standards and policies that address media sanitization policy; system audit  
1903 records; media sanitization records; system design documentation; system configuration settings;  
1904 records retention and disposition policy; records retention and disposition procedures; system  
1905 security plan; other relevant documents or records]

1906 **Interview**

1907 [SELECT FROM: personnel with media sanitization responsibilities; personnel with records  
1908 retention and disposition responsibilities; personnel with information security responsibilities;  
1909 system administrators]

1910 **Test**

1911 [SELECT FROM: processes for media sanitization; mechanisms for supporting and/or  
1912 implementing media sanitization]

1913 **REFERENCES**

1914 Source Assessment Procedure: [MP-06](#)

1915 **3.8.4. Media Marking**

1916 **REQUIREMENT:** 03.08.04

1917 **ASSESSMENT OBJECTIVE**

1918 *Determine if:*

1919 **A.03.08.04[01]:** system media that contain CUI are marked to indicate distribution limitations.

1920 **A.03.08.04[02]:** system media that contain CUI are marked to indicate handling caveats.

1921 **A.03.08.04[03]:** system media that contain CUI are marked to indicate security markings.

- 1922           **ASSESSMENT METHODS AND OBJECTS**
- 1923           **Examine**
- 1924           [SELECT FROM: physical protection policy and procedures; media protection policy and  
1925           procedures; procedures for media marking; list of system media marking security attributes;  
1926           system security plan; other relevant documents or records]
- 1927           **Interview**
- 1928           [SELECT FROM: personnel with system media protection and marking responsibilities; personnel  
1929           with information security responsibilities]
- 1930           **Test**
- 1931           [SELECT FROM: processes for marking information media; mechanisms for supporting and/or  
1932           implementing media marking]
- 1933           **REFERENCES**
- 1934           Source Assessment Procedure: [MP-03](#)

1935   **3.8.5. Media Transport**

- 1936           **REQUIREMENT:** 03.08.05
- 1937           **ASSESSMENT OBJECTIVE**
- 1938           *Determine if:*
- 1939           **A.03.08.05.a[01]:** system media that contain CUI are protected during transport outside of  
1940           controlled areas.
- 1941           **A.03.08.05.a[02]:** system media that contain CUI are controlled during transport outside of  
1942           controlled areas.
- 1943           **A.03.08.05.b:** the accountability of system media that contain CUI is maintained during transport  
1944           outside of controlled areas.
- 1945           **A.03.08.05.c:** cryptographic mechanisms are implemented to prevent the unauthorized disclosure  
1946           of CUI stored on digital media during transport.

- 1947           **ASSESSMENT METHODS AND OBJECTS**
- 1948           **Examine**
- 1949           [SELECT FROM: physical protection policy and procedures; media protection policy and  
1950           procedures; procedures for media storage; access control policy and procedures; authorized  
1951           personnel list; system media; designated controlled areas; system and communications  
1952           protection policy and procedures; cryptographic mechanisms and configuration documentation;  
1953           procedures for the protection of information at rest; system design documentation; system  
1954           configuration settings; list of information at rest requiring confidentiality protections; system audit  
1955           records; system security plan; other relevant documents or records]
- 1956           **Interview**
- 1957           [SELECT FROM: personnel with system media protection and storage responsibilities; personnel  
1958           with information security responsibilities; system developers; system administrators]

1959	<b>Test</b>
1960	[SELECT FROM: processes for storing information media; mechanisms for supporting and/or
1961	implementing media storage/media protection; mechanisms for supporting and/or implementing
1962	confidentiality protections for information at rest]
1963	<b>REFERENCES</b>
1964	Source Assessment Procedures: <a href="#">MP-05</a> , <a href="#">SC-28</a> , <a href="#">SC-28(01)</a>
1965	<b>3.8.6. Withdrawn</b>
1966	Incorporated into <a href="#">03.08.05</a> .
1967	<b>3.8.7. Media Use</b>
1968	<b>REQUIREMENT:</b> 03.08.07
1969	<b>ASSESSMENT OBJECTIVE</b>
1970	<i>Determine if:</i>
1971	<b>A.03.08.07.ODP[01]: the types of system media with usage restrictions or that are</b>
1972	<b>prohibited from use are defined.</b>
1973	<b>A.03.08.07.a:</b> the use of the following types of system media is restricted or prohibited:
1974	<b>&lt;A.03.08.07.ODP[01]: types of system media&gt;.</b>
1975	<b>A.03.08.07.b:</b> the use of removable system media without an identifiable owner is prohibited.
1976	<b>ASSESSMENT METHODS AND OBJECTS</b>
1977	<b>Examine</b>
1978	[SELECT FROM: system media protection policy and procedures; system use policy; procedures
1979	for media usage restrictions; rules of behavior; system design documentation; audit records;
1980	system configuration settings; system security plan; other relevant documents or records]
1981	<b>Interview</b>
1982	[SELECT FROM: personnel with system media use responsibilities; personnel with information
1983	security responsibilities; system administrators]
1984	<b>Test</b>
1985	[SELECT FROM: processes for media use; mechanisms for restricting or prohibiting the use of
1986	system media on systems or system components]
1987	<b>REFERENCES</b>
1988	Source Assessment Procedure: <a href="#">MP-07</a>
1989	<b>3.8.8. Withdrawn</b>
1990	Incorporated into <a href="#">03.08.07</a> .

1991 **3.8.9. System Backup – Cryptographic Protection**

1992 **REQUIREMENT:** 03.08.09

1993 **ASSESSMENT OBJECTIVE**

1994 *Determine if:*

1995 **A.03.08.09:** cryptographic mechanisms are implemented to prevent the unauthorized disclosure  
1996 of CUI at backup storage locations.

1997 **ASSESSMENT METHODS AND OBJECTS**

1998 **Examine**

1999 [SELECT FROM: contingency planning policy and procedures; procedures for system backup;  
2000 contingency plan; system design documentation; system configuration settings; system security  
2001 plan; other relevant documents or records]

2002 **Interview**

2003 [SELECT FROM: personnel with system backup responsibilities; personnel with information  
2004 security responsibilities]

2005 **Test**

2006 [SELECT FROM: mechanisms for supporting and/or implementing the cryptographic protection of  
2007 backup information]

2008 **REFERENCES**

2009 Source Assessment Procedure: [CP-09\(08\)](#)

2010 **3.9. [Personnel Security](#)**

2011 **3.9.1. Personnel Screening**

2012 **REQUIREMENT:** 03.09.01

2013 **ASSESSMENT OBJECTIVE**

2014 *Determine if:*

2015 **A.03.09.01.ODP[01]:** *the conditions that require the rescreening of individuals are defined.*

2016 **A.03.09.01.a:** individuals are screened prior to authorizing access to the system.

2017 **A.03.09.01.b:** individuals are rescreened in accordance with the following conditions:

2018 **<A.03.09.01.ODP[01]: conditions>.**

2019 **ASSESSMENT METHODS AND OBJECTS**

2020 **Examine**

2021 [SELECT FROM: personnel security policy and procedures; procedures for personnel screening;  
2022 records of screened personnel; system security plan; other relevant documents or records]

2023 **Interview**

2024 [SELECT FROM: personnel with personnel security responsibilities; personnel with information  
2025 security responsibilities]



2026 **Test**  
2027 [SELECT FROM: processes for personnel screening]

2028 **REFERENCES**

2029 Source Assessment Procedure: [PS-03](#)

2030 **3.9.2. Personnel Termination and Transfer**

2031 **REQUIREMENT:** 03.09.02

2032 **ASSESSMENT OBJECTIVE**

2033 *Determine if:*

2034 **A.03.09.02.ODP[01]:** *the time period within which to disable system access is defined.*

2035 **A.03.09.02.ODP[02]:** *the time period within which transfer or reassignment actions must*  
2036 *occur following an individual transfer or reassignment is defined.*

2037 **A.03.09.02.ODP[03]:** *the transfer or reassignment actions to be initiated following transfer*  
2038 *or reassignment are defined.*

2039 **A.03.09.02.a.01:** upon the termination of individual employment, system access is disabled within  
2040 **<A.03.09.02.ODP[01]: time period>.**

2041 **A.03.09.02.a.02:** upon the termination of individual employment, authenticators and credentials  
2042 associated with the individual are terminated or revoked.

2043 **A.03.09.02.a.03:** upon the termination of individual employment, security-related system property  
2044 is retrieved.

2045 **A.03.09.02.b.01:** upon individual reassignment or transfer to other positions in the organization,  
2046 the ongoing operational need for current logical and physical access authorizations to the system  
2047 and facility are reviewed and confirmed.

2048 **A.03.09.02.b.02:** upon individual reassignment or transfer to other positions in the organization,  
2049 the following transfer or reassignment actions are initiated within **<A.03.09.02.ODP[02]: time**  
2050 **period>: <A.03.09.02.ODP[03]: transfer or reassignment actions>.**

2051 **A.03.09.02.b.03:** upon individual reassignment or transfer to other positions in the organization,  
2052 access authorization is modified to correspond with any changes in operational need.

2053 **ASSESSMENT METHODS AND OBJECTS**

2054 **Examine**

2055 [SELECT FROM: personnel security policy and procedures; procedures for personnel  
2056 termination; records of personnel transfer actions; procedures for personnel transfer; list of  
2057 system and facility access authorizations; records of personnel termination actions; records of  
2058 terminated or revoked authenticators or credentials; list of system accounts; records of exit  
2059 interviews; system security plan; other relevant documents or records]

2060 **Interview**

2061 [SELECT FROM: personnel with personnel security responsibilities; personnel with account  
2062 management responsibilities; personnel with information security responsibilities; system  
2063 administrators]

2064           **Test**  
2065           [SELECT FROM: processes for personnel termination; processes for personnel transfer;  
2066           mechanisms for supporting and/or implementing personnel transfer notifications; mechanisms for  
2067           supporting and/or implementing personnel termination notifications; mechanisms for disabling  
2068           system access and revoking authenticators]

2069           **REFERENCES**

2070           Source Assessment Procedures: [PS-04](#), [PS-05](#)

2071   **3.10. [Physical Protection](#)**

2072   **3.10.1. Physical Access Authorizations**

2073           **REQUIREMENT:** 03.10.01

2074           **ASSESSMENT OBJECTIVE**

2075           *Determine if:*

2076           **A.03.10.01.a[01]:** a list of individuals with authorized access to the physical location where the  
2077           system resides is developed.

2078           **A.03.10.01.a[02]:** a list of individuals with authorized access to the physical location where the  
2079           system resides is approved.

2080           **A.03.10.01.a[03]:** a list of individuals with authorized access to the physical location where the  
2081           system resides is maintained.

2082           **A.03.10.01.b:** authorization credentials are issued for facility access.

2083           **A.03.10.01.c:** the physical access list is reviewed periodically.

2084           **A.03.10.01.d:** individuals from the physical access list are removed when access is no longer  
2085           required.

2086           **ASSESSMENT METHODS AND OBJECTS**

2087           **Examine**

2088           [SELECT FROM: physical protection policy and procedures; procedures for physical access  
2089           authorizations; authorized personnel access list; physical access list reviews; physical access  
2090           termination records; authorization credentials; system security plan; other relevant documents  
2091           or records]

2092           **Interview**

2093           [SELECT FROM: personnel with physical access authorization responsibilities; personnel with  
2094           physical access to the facility where the system resides; personnel with information security  
2095           responsibilities]

2096           **Test**

2097           [SELECT FROM: processes for physical access authorizations; mechanisms for supporting  
2098           and/or implementing physical access authorizations]

2099           **REFERENCES**

2100           Source Assessment Procedure: [PE-02](#)

2101 **3.10.2. Monitoring Physical Access**

2102 **REQUIREMENT:** 03.10.02

2103 **ASSESSMENT OBJECTIVE**

2104 *Determine if:*

2105 **A.03.10.02.a[01]:** physical access to the location where the system resides is monitored to  
2106 detect physical security incidents.

2107 **A.03.10.02.a[02]:** physical access to the location where the system resides is monitored to  
2108 respond to physical security incidents.

2109 **A.03.10.02.b:** physical access logs are reviewed periodically.

2110 **ASSESSMENT METHODS AND OBJECTS**

2111 **Examine**

2112 [SELECT FROM: physical protection policy and procedures; procedures for physical access  
2113 monitoring; physical access logs or records; physical access monitoring records; physical  
2114 access log reviews; system security plan; other relevant documents or records]

2115 **Interview**

2116 [SELECT FROM: personnel with physical access monitoring responsibilities; personnel with  
2117 incident response responsibilities; personnel with information security responsibilities]

2118 **Test**

2119 [SELECT FROM: processes for monitoring physical access; mechanisms supporting and/or  
2120 implementing physical access monitoring; mechanisms supporting and/or implementing the  
2121 review of physical access logs]

2122 **REFERENCES**

2123 Source Assessment Procedure: [PE-06](#)

2124 **3.10.3. Withdrawn**

2125 Incorporated into [03.10.07](#).

2126 **3.10.4. Withdrawn**

2127 Incorporated into [03.10.07](#).

2128 **3.10.5. Withdrawn**

2129 Incorporated into [03.10.07](#).

2130 **3.10.6. Alternate Work Site**

2131 **REQUIREMENT:** 03.10.06

2132 **ASSESSMENT OBJECTIVE**

2133 *Determine if:*

2134 **A.03.10.06.ODP[01]: the security requirements to be employed at alternate work sites are**  
2135 **defined.**

2136 **A.03.10.06.a:** alternate work sites allowed for use by employees are defined.

2137 **A.03.10.06.b:** the following security requirements are employed at alternate work sites:  
2138 **<A.03.10.06.ODP[01]: security requirements>.**

## 2139 **ASSESSMENT METHODS AND OBJECTS**

### 2140 **Examine**

2141 [SELECT FROM: physical protection policy and procedures; procedures for alternate work sites  
2142 for personnel; list of security requirements for alternate work sites; assessments of security  
2143 requirements at alternate work sites; system security plan; other relevant documents or records]

### 2144 **Interview**

2145 [SELECT FROM: personnel approving the use of alternate work sites; personnel using alternate  
2146 work sites; personnel assessing security requirements at alternate work sites; personnel with  
2147 information security responsibilities]

### 2148 **Test**

2149 [SELECT FROM: processes for security at alternate work sites; mechanisms for supporting  
2150 alternate work sites; security requirements employed at alternate work sites; means of  
2151 communication between personnel at alternate work sites and security personnel]

## 2152 **REFERENCES**

2153 Source Assessment Procedure: [PE-17](#)

## 2154 **3.10.7. Physical Access Control**

2155 **REQUIREMENT:** 03.10.07

### 2156 **ASSESSMENT OBJECTIVE**

2157 *Determine if:*

2158 **A.03.10.07.ODP[01]: the circumstances requiring visitor escorts and control of visitor**  
2159 **activity are defined.**

2160 **A.03.10.07.a.01:** physical access is controlled at the location where the system resides by  
2161 verifying individual physical access authorizations before granting access.

2162 **A.03.10.07.a.02:** physical access is controlled at the location where the system resides by  
2163 controlling ingress and egress with physical access control systems/devices or guards.

2164 **A.03.10.07.b:** physical access audit logs for entry or exit points are maintained.

2165 **A.03.10.07.c[01]:** visitors are escorted.

2166 **A.03.10.07.c[02]:** visitor activity is controlled under the following circumstances:  
2167 **<A.03.10.07.ODP[01]: circumstances>.**

2168 **A.03.10.07.d[01]:** keys are secured.

2169 **A.03.10.07.d[02]:** combinations are secured.

2170 **A.03.10.07.d[03]:** other physical access devices are secured.

2171 **ASSESSMENT METHODS AND OBJECTS**

2172 **Examine**

2173 [SELECT FROM: physical protection policy and procedures; procedures for physical access  
2174 control; physical access control logs or records; inventory records of physical access control  
2175 devices; system entry and exit points; records of key and lock combination changes; storage  
2176 locations for physical access control devices; physical access control devices; list of security  
2177 safeguards controlling access to designated publicly accessible areas within facility; system  
2178 security plan; other relevant documents or records]

2179 **Interview**

2180 [SELECT FROM: personnel with physical access control responsibilities; personnel with  
2181 information security responsibilities]

2182 **Test**

2183 [SELECT FROM: processes for physical access control; mechanisms for supporting and/or  
2184 implementing physical access control; physical access control devices]

2185 **REFERENCES**

2186 Source Assessment Procedure: [PE-03](#)

2187 **3.10.8. Access Control for Transmission and Output Devices**

2188 **REQUIREMENT:** 03.10.08

2189 **ASSESSMENT OBJECTIVE**

2190 *Determine if:*

2191 **A.03.10.08.a:** physical access to system distribution and transmission lines in organizational  
2192 facilities is controlled.

2193 **A.03.10.08.b:** physical access to output devices is controlled to prevent unauthorized  
2194 individuals from obtaining access to CUI.

2195 **ASSESSMENT METHODS AND OBJECTS**

2196 **Examine**

2197 [SELECT FROM: physical protection policy and procedures; procedures for access control for  
2198 transmission mediums; system design documentation; facility communications and wiring  
2199 diagrams; list of physical security safeguards applied to system distribution and transmission  
2200 lines; procedures for access control for display medium; facility layout of system components;  
2201 actual displays from system components; list of output devices and associated outputs that  
2202 require physical access controls; physical access control logs or records for areas containing  
2203 output devices and related outputs; system security plan; other relevant documents or records]

2204 **Interview**

2205 [SELECT FROM: personnel with physical access control responsibilities; personnel with  
2206 information security responsibilities]

2207 **Test**

2208 [SELECT FROM: processes for access control for distribution and transmission lines;  
2209 mechanisms for supporting and/or implementing access control for distribution and transmission  
2210 lines; processes for access control to output devices; mechanisms for supporting and/or  
2211 implementing access control for output devices]

2212           **REFERENCES**

2213           Source Assessment Procedures: [PE-04](#), [PE-05](#)

2214   **3.11. [Risk Assessment](#)**

2215   **3.11.1. Risk Assessment**

2216           **REQUIREMENT:** 03.11.01

2217           **ASSESSMENT OBJECTIVE**

2218           *Determine if:*

2219           **A.03.11.01.a:** the risk (including supply chain risk) of unauthorized disclosure resulting from the  
2220           processing, storage, or transmission of CUI is assessed.

2221           **A.03.11.01.b:** risk assessments are updated periodically.

2222           **ASSESSMENT METHODS AND OBJECTS**

2223           **Examine**

2224           [SELECT FROM: risk assessment policy and procedures; security planning policy and  
2225           procedures; procedures for organizational assessments of risk; risk assessment; risk  
2226           assessment results; risk assessment reviews; risk assessment updates; SCRM policy and  
2227           procedures; inventory of critical systems, system components, and system services; procedures  
2228           for organizational assessments of supply chain risk; acquisition policy; SCRM plan; system  
2229           security plan; other relevant documents or records]

2230           **Interview**

2231           [SELECT FROM: personnel with risk assessment responsibilities; personnel with SCRM  
2232           responsibilities; personnel with security responsibilities]

2233           **Test**

2234           [SELECT FROM: processes for organizational risk assessments; mechanisms for supporting  
2235           and/or conducting, documenting, reviewing, disseminating, and updating risk assessments;  
2236           mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and  
2237           updating supply chain risk assessments]

2238           **REFERENCES**

2239           Source Assessment Procedures: [RA-03](#), [RA-03\(01\)](#), [SR-06](#)

2240   **3.11.2. Vulnerability Monitoring and Scanning**

2241           **REQUIREMENT:** 03.11.02

2242           **ASSESSMENT OBJECTIVE**

2243           *Determine if:*

2244           **A.03.11.02.ODP[01]: response times to remediate system vulnerabilities are defined.**

2245           **A.03.11.02.a[01]:** the system is monitored for vulnerabilities periodically.

2246           **A.03.11.02.a[02]:** the system is monitored for vulnerabilities when new vulnerabilities that affect  
2247           the system are identified.

- 2248 **A.03.11.02.a[03]**: the system is scanned for vulnerabilities periodically.
- 2249 **A.03.11.02.a[04]**: the system is scanned for vulnerabilities when new vulnerabilities that affect  
2250 the system are identified.
- 2251 **A.03.11.02.b**: system vulnerabilities are remediated **<A.03.11.02.ODP[01]: response times>**.
- 2252 **A.03.11.02.c[01]**: system vulnerabilities to be scanned are updated periodically.
- 2253 **A.03.11.02.c[02]**: system vulnerabilities to be scanned are updated when new vulnerabilities  
2254 are identified.
- 2255 **A.03.11.02.c[03]**: system vulnerabilities to be scanned are updated when new vulnerabilities  
2256 are reported.

## 2257 **ASSESSMENT METHODS AND OBJECTS**

### 2258 **Examine**

2259 [SELECT FROM: risk assessment policy and procedures; procedures for vulnerability scanning;  
2260 patch and vulnerability management records; vulnerability scanning tools and configuration  
2261 documentation; vulnerability scanning results; risk assessment; risk assessment report; system  
2262 security plan; other relevant documents or records]

### 2263 **Interview**

2264 [SELECT FROM: personnel with risk assessment and vulnerability scanning responsibilities;  
2265 personnel with vulnerability scan analysis responsibilities; personnel with vulnerability  
2266 remediation responsibilities; personnel with information security responsibilities; system  
2267 administrators]

### 2268 **Test**

2269 [SELECT FROM: processes for vulnerability scanning, analysis, and remediation; mechanisms  
2270 for supporting and/or implementing vulnerability scanning, analysis, and remediation]

## 2271 **REFERENCES**

2272 Source Assessment Procedures: [RA-05](#), [RA-05\(02\)](#)

### 2273 **3.11.3. Withdrawn**

2274 Incorporated into [03.11.02](#).

## 2275 **3.12. [Security Assessment and Monitoring](#)**

### 2276 **3.12.1. Security Assessment**

2277 **REQUIREMENT:** 03.12.01

### 2278 **ASSESSMENT OBJECTIVE**

2279 *Determine if:*

2280 **A.03.12.01**: the security requirements for the system and its environment of operation are  
2281 assessed periodically to determine if the requirements have been satisfied.

2282 **ASSESSMENT METHODS AND OBJECTS**

2283 **Examine**

2284 [SELECT FROM: security assessment and monitoring policy and procedures; procedures for  
2285 security assessment planning; security assessment plan; security assessment report; system  
2286 security plan; other relevant documents or records]

2287 **Interview**

2288 [SELECT FROM: personnel with security assessment responsibilities; personnel with  
2289 information security responsibilities]

2290 **Test**

2291 [SELECT FROM: mechanisms supporting security assessments, processes for security  
2292 assessment plan development and/or security assessment reporting]

2293 **REFERENCES**

2294 Source Assessment Procedure: [CA-02](#)

2295 **3.12.2. Plan of Action and Milestones**

2296 **REQUIREMENT:** 03.12.02

2297 **ASSESSMENT OBJECTIVE**

2298 *Determine if:*

2299 **A.03.12.02.a.01:** a plan of action and milestones for the system is developed to document the  
2300 planned remediation actions for correcting weaknesses or deficiencies noted during security  
2301 assessments.

2302 **A.03.12.02.a.02:** a plan of action and milestones for the system is developed to reduce or  
2303 eliminate known system vulnerabilities.

2304 **A.03.12.02.b[01]:** the existing plan of action and milestones is updated periodically based on  
2305 the findings from security assessments.

2306 **A.03.12.02.b[02]:** the existing plan of action and milestones is updated periodically based on  
2307 the findings from independent audits or reviews.

2308 **A.03.12.02.b[03]:** the existing plan of action and milestones is updated periodically based on  
2309 the findings from continuous monitoring activities.

2310 **ASSESSMENT METHODS AND OBJECTS**

2311 **Examine**

2312 [SELECT FROM: security assessment and monitoring policy and procedures; procedures for  
2313 plans of action and milestones; security assessment plan; security assessment report; security  
2314 assessment evidence; plan of action and milestones; system security plan; other relevant  
2315 documents or records]

2316 **Interview**

2317 [SELECT FROM: personnel with plans of action and milestones development and  
2318 implementation responsibilities; personnel with information security responsibilities]

2319 **Test**

2320 [SELECT FROM: mechanisms for developing, implementing, and maintaining plans of action  
2321 and milestones]



2322           **REFERENCES**

2323           Source Assessment Procedure: [CA-05](#)

2324   **3.12.3. Continuous Monitoring**

2325           **REQUIREMENT:** 03.12.03

2326           **ASSESSMENT OBJECTIVE**

2327           *Determine if:*

2328           **A.03.12.03[01]:** a system-level continuous monitoring strategy is developed and implemented.

2329           **A.03.12.03[02]:** ongoing monitoring is included in the continuous monitoring strategy.

2330           **A.03.12.03[03]:** security assessments are included the continuous monitoring strategy.

2331           **ASSESSMENT METHODS AND OBJECTS**

2332           **Examine**

2333           [SELECT FROM: security assessment and monitoring policy and procedures; organizational  
2334           continuous monitoring strategy; system-level continuous monitoring strategy; procedures for  
2335           continuous monitoring of the system; procedures for configuration management; security  
2336           assessment report; plan of action and milestones; system monitoring records; configuration  
2337           management records; impact analyses; status reports; system security plan; other relevant  
2338           documents or records]

2339           **Interview**

2340           [SELECT FROM: personnel with continuous monitoring responsibilities; personnel with  
2341           information security responsibilities; system administrators]

2342           **Test**

2343           [SELECT FROM: mechanisms for implementing continuous monitoring; mechanisms supporting  
2344           response actions for assessment and monitoring results; mechanisms for supporting security  
2345           status reporting]

2346           **REFERENCES**

2347           Source Assessment Procedure: [CA-07](#)

2348   **3.12.4. Withdrawn**

2349           Incorporated into [03.15.02](#).

2350   **3.12.5. Information Exchange**

2351           **REQUIREMENT:** 03.12.05

2352           **ASSESSMENT OBJECTIVE**

2353           *Determine if:*

2354           **A.03.12.05.ODP[01]:** *one or more of the following parameter values is/are selected:*  
2355           *{interconnection security agreements; information exchange security agreements;*

2356 **memoranda of understanding or agreement; service-level agreements; user agreements;**  
2357 **non-disclosure agreements}.**

2358 **A.03.12.05.a:** the exchange of CUI between the system and other systems is approved and  
2359 managed using **<A.03.12.05.ODP[01]: selected parameter value(s)>**.

2360 **A.03.12.05.b[01]:** interface characteristics are documented as part of the exchange  
2361 agreements.

2362 **A.03.12.05.b[02]:** security requirements are documented as part of the exchange agreements.

2363 **A.03.12.05.b[03]:** responsibilities for each system are documented as part of the exchange  
2364 agreements.

2365 **A.03.12.05.c[01]:** exchange agreements are reviewed periodically.

2366 **A.03.12.05.c[02]:** exchange agreements are updated periodically.

## 2367 **ASSESSMENT METHODS AND OBJECTS**

### 2368 **Examine**

2369 [SELECT FROM: access control policy and procedures; procedures for system connections;  
2370 system and communications protection policy and procedures; system interconnection security  
2371 agreements; information exchange security agreements; service-level agreements; memoranda  
2372 of understanding or agreements; non-disclosure agreements; system design documentation;  
2373 enterprise architecture; security architecture; system configuration settings; system security  
2374 plan; other relevant documents or records]

### 2375 **Interview**

2376 [SELECT FROM: personnel with development, implementation, and approval responsibilities for  
2377 system interconnection agreements; personnel who manage systems to which the exchange  
2378 agreements apply; personnel with information security responsibilities]

## 2379 **REFERENCES**

2380 Source Assessment Procedure: [CA-03](#)

## 2381 **3.13. [System and Communications Protection](#)**

### 2382 **3.13.1. Boundary Protection**

2383 **REQUIREMENT:** 03.13.01

#### 2384 **ASSESSMENT OBJECTIVE**

2385 *Determine if:*

2386 **A.03.13.01.a[01]:** communications at external managed interfaces to the system are monitored.

2387 **A.03.13.01.a[02]:** communications at external managed interfaces to the system are controlled.

2388 **A.03.13.01.a[03]:** communications at key internal managed interfaces within the system are  
2389 monitored.

2390 **A.03.13.01.a[04]:** communications at key internal managed interfaces within the system are  
2391 controlled.

2392 **A.03.13.01.b:** subnetworks are implemented for publicly accessible system components that  
2393 are physically or logically separated from internal networks.

2394 **A.03.13.01.c:** external system connections are only made through managed interfaces that  
2395 consist of boundary protection devices arranged in accordance with an organizational security  
2396 architecture.

2397 **ASSESSMENT METHODS AND OBJECTS**

2398 **Examine**

2399 [SELECT FROM: system and communications protection policy and procedures; procedures for  
2400 boundary protection; list of key internal boundaries within the system; boundary protection  
2401 hardware and software; system configuration settings; security architecture; system audit  
2402 records; system design documentation; system security plan; other relevant documents or  
2403 records]

2404 **Interview**

2405 [SELECT FROM: personnel with boundary protection responsibilities; personnel with  
2406 information security responsibilities; system developers; system administrators]

2407 **Test**

2408 [SELECT FROM: mechanisms for implementing boundary protection capabilities]

2409 **REFERENCES**

2410 Source Assessment Procedure: [SC-07](#)

2411 **3.13.2. Withdrawn**

2412 Recategorized as NCO.

2413 **3.13.3. Withdrawn**

2414 Addressed by [03.01.04](#), [03.01.05](#), [03.01.06](#), and [03.01.07](#).

2415 **3.13.4. Information in Shared System Resources**

2416 **REQUIREMENT:** 03.13.04

2417 **ASSESSMENT OBJECTIVE**

2418 *Determine if:*

2419 **A.03.13.04[01]:** unauthorized information transfer via shared system resources is prevented.

2420 **A.03.13.04[02]:** unintended information transfer via shared system resources is prevented.

2421 **ASSESSMENT METHODS AND OBJECTS**

2422 **Examine**

2423 [SELECT FROM: system and communications protection policy and procedures; procedures for  
2424 information protection in shared system resources; system configuration settings; system audit  
2425 records; system design documentation; system security plan; other relevant documents or  
2426 records]

- 2427 **Interview**
- 2428 [SELECT FROM: personnel with information security responsibilities; system developers;  
2429 system administrators]
- 2430 **Test**
- 2431 [SELECT FROM: mechanisms for preventing the unauthorized and unintended transfer of  
2432 information via shared system resources]
- 2433 **REFERENCES**
- 2434 Source Assessment Procedure: [SC-04](#)
- 2435 **3.13.5. Withdrawn**
- 2436 Incorporated into [03.13.01](#).
- 2437 **3.13.6. Network Communications – Deny by Default – Allow by Exception**
- 2438 **REQUIREMENT:** 03.13.06
- 2439 **ASSESSMENT OBJECTIVE**
- 2440 *Determine if:*
- 2441 **A.03.13.06[01]:** network communications traffic is denied by default.
- 2442 **A.03.13.06[02]:** network communications traffic is allowed by exception.
- 2443 **ASSESSMENT METHODS AND OBJECTS**
- 2444 **Examine**
- 2445 [SELECT FROM: system and communications protection policy and procedures; procedures for  
2446 boundary protection; system design documentation; system configuration settings; system audit  
2447 records; system security plan; other relevant documents or records]
- 2448 **Interview**
- 2449 [SELECT FROM: personnel with boundary protection responsibilities; personnel with  
2450 information security responsibilities; system developers; system administrators]
- 2451 **Test**
- 2452 [SELECT FROM: mechanisms for implementing traffic management at managed interfaces]
- 2453 **REFERENCES**
- 2454 Source Assessment Procedure: [SC-07\(05\)](#)
- 2455 **3.13.7. Withdrawn**
- 2456 Addressed by [03.01.12](#), [03.04.02](#) and [03.04.06](#).
- 2457 **3.13.8. Transmission and Storage Confidentiality**
- 2458 **REQUIREMENT:** 03.13.08

2459 **ASSESSMENT OBJECTIVE**

2460 *Determine if:*

2461 **A.03.13.08[01]:** cryptographic mechanisms are implemented to prevent the unauthorized  
2462 disclosure of CUI during transmission.

2463 **A.03.13.08[02]:** cryptographic mechanisms are implemented to prevent the unauthorized  
2464 disclosure of CUI while in storage.

2465 **ASSESSMENT METHODS AND OBJECTS**

2466 **Examine**

2467 [SELECT FROM: system and communications protection policy and procedures; procedures for  
2468 transmission confidentiality; procedures for the protection of information at rest; system design  
2469 documentation; system configuration settings; cryptographic mechanisms and associated  
2470 configuration documentation; information in storage requiring confidentiality protection; system  
2471 audit records; system security plan; other relevant documents or records]

2472 **Interview**

2473 [SELECT FROM: personnel with information security responsibilities; system developers;  
2474 system administrators]

2475 **Test**

2476 [SELECT FROM: mechanisms for supporting and/or implementing transmission confidentiality;  
2477 cryptographic mechanisms for supporting and/or implementing transmission confidentiality;  
2478 mechanisms for supporting and/or implementing confidentiality protection for information in  
2479 storage; cryptographic mechanisms implementing confidentiality protections for information in  
2480 storage]

2481 **REFERENCES**

2482 Source Assessment Procedures: [SC-08](#), [SC-08\(01\)](#), [SC-28](#), [SC-28\(01\)](#)

2483 **3.13.9. Network Disconnect**

2484 **REQUIREMENT:** 03.13.09

2485 **ASSESSMENT OBJECTIVE**

2486 *Determine if:*

2487 **A.03.13.09:** network connections associated with communications sessions are terminated at  
2488 the end of the sessions or after periods of inactivity.

2489 **ASSESSMENT METHODS AND OBJECTS**

2490 **Examine**

2491 [SELECT FROM: system and communications protection policy and procedures; procedures for  
2492 network disconnect; system design documentation; system configuration settings; system audit  
2493 records; system security plan; other relevant documents or records]

2494 **Interview**

2495 [SELECT FROM: personnel with information security responsibilities; system developers;  
2496 system administrators]

- 2497           **Test**
- 2498           [SELECT FROM: mechanisms for supporting and/or implementing a network disconnect  
2499           capability]
- 2500           **REFERENCES**
- 2501           Source Assessment Procedure: [SC-10](#)
- 2502   **3.13.10. Cryptographic Key Establishment and Management**
- 2503           **REQUIREMENT:** 03.13.10
- 2504           **ASSESSMENT OBJECTIVE**
- 2505           *Determine if:*
- 2506           **A.03.13.10.ODP[01]: requirements for key establishment and management are defined.**
- 2507           **A.03.13.10[01]:** cryptographic keys are established in the system in accordance with the  
2508           following key management requirements: **<A.03.13.10.ODP[01]: requirements>**.
- 2509           **A.03.13.10[02]:** cryptographic keys are managed in the system in accordance with the  
2510           following key management requirements: **<A.03.13.10.ODP[01]: requirements>**.
- 2511           **ASSESSMENT METHODS AND OBJECTS**
- 2512           **Examine**
- 2513           [SELECT FROM: system and communications protection policy and procedures; procedures  
2514           for cryptographic key establishment and management; system design documentation; system  
2515           configuration settings; cryptographic mechanisms; system audit records; system security plan;  
2516           other relevant documents or records]
- 2517           **Interview**
- 2518           [SELECT FROM: personnel with responsibilities for cryptographic key establishment and/or  
2519           management; personnel with information security responsibilities; system administrators]
- 2520           **Test**
- 2521           [SELECT FROM: mechanisms for supporting and/or implementing cryptographic key  
2522           establishment and management]
- 2523           **REFERENCES**
- 2524           Source Assessment Procedure: [SC-12](#)
- 2525   **3.13.11. Cryptographic Protection**
- 2526           **REQUIREMENT:** 03.13.11
- 2527           **ASSESSMENT OBJECTIVE**
- 2528           *Determine if:*
- 2529           **A.03.13.11.ODP[01]: the types of cryptography for protecting the confidentiality of CUI**  
2530           **are defined.**
- 2531           **A.03.13.11:** the following types of cryptography are implemented when used to protect the  
2532           confidentiality of CUI: **<A.03.13.11.ODP[01]: types of cryptography>**.

2533 **ASSESSMENT METHODS AND OBJECTS**

2534 **Examine**

2535 [SELECT FROM: system and communications protection policy and procedures; procedures  
2536 for cryptographic protection; system design documentation; system configuration settings;  
2537 cryptographic module validation certificates; list of FIPS-validated cryptographic modules;  
2538 system audit records; system security plan; other relevant documents or records]

2539 **Interview**

2540 [SELECT FROM: personnel with responsibilities for cryptographic protection; personnel with  
2541 information security responsibilities; system developers; system administrators]

2542 **Test**

2543 [SELECT FROM: mechanisms for supporting and/or implementing cryptographic protection]

2544 **REFERENCES**

2545 Source Assessment Procedure: [SC-13](#)

2546 **3.13.12. Collaborative Computing Devices and Applications**

2547 **REQUIREMENT:** 03.13.12

2548 **ASSESSMENT OBJECTIVE**

2549 *Determine if:*

2550 **A.03.13.12.a:** remote activation of collaborative computing devices and applications is  
2551 prohibited.

2552 **A.03.13.12.b:** an explicit indication of use is provided to users who are physically present at  
2553 the devices.

2554 **ASSESSMENT METHODS AND OBJECTS**

2555 **Examine**

2556 [SELECT FROM: system and communications protection policy and procedures; procedures  
2557 for collaborative computing; access control policy and procedures; system configuration  
2558 settings; system design documentation; system audit records; system security plan; other  
2559 relevant documents or records]

2560 **Interview**

2561 [SELECT FROM: personnel with responsibilities for managing collaborative computing  
2562 devices; personnel with information security responsibilities; system developers; system  
2563 administrators]

2564 **Test**

2565 [SELECT FROM: mechanisms supporting and/or implementing the management of remote  
2566 activation of collaborative computing devices; mechanisms for providing an indication of use of  
2567 collaborative computing devices]

2568 **REFERENCES**

2569 Source Assessment Procedure: [SC-15](#)

2570 **3.13.13. Mobile Code**

2571 **REQUIREMENT:** 03.13.13

2572 **ASSESSMENT OBJECTIVE**

2573 *Determine if:*

2574 **A.03.13.13.a[01]:** acceptable mobile code is defined.

2575 **A.03.13.13.a[02]:** acceptable mobile code technologies are defined.

2576 **A.03.13.13.b[01]:** the use of mobile code is authorized.

2577 **A.03.13.13.b[02]:** the use of mobile code is monitored.

2578 **A.03.13.13.b[03]:** the use of mobile code is controlled.

2579 **ASSESSMENT METHODS AND OBJECTS**

2580 **Examine**

2581 [SELECT FROM: system and communications protection policy and procedures; procedures  
2582 for mobile code; mobile code implementation policy and procedures; list of acceptable mobile  
2583 code and mobile code technologies; authorization records; system monitoring records; system  
2584 audit records; system security plan; other relevant documents or records]

2585 **Interview**

2586 [SELECT FROM: personnel with responsibilities for managing mobile code; personnel with  
2587 information security responsibilities; system administrators]

2588 **Test**

2589 [SELECT FROM: processes for authorizing, monitoring, and controlling mobile code;  
2590 mechanisms for supporting and/or implementing the management of mobile code;  
2591 mechanisms for supporting and/or implementing mobile code monitoring]

2592 **REFERENCES**

2593 Source Assessment Procedure: [SC-18](#)

2594 **3.13.14. Withdrawn**

2595 Technology-specific.

2596 **3.13.15. Session Authenticity**

2597 **REQUIREMENT:** 03.13.15

2598 **ASSESSMENT OBJECTIVE**

2599 *Determine if:*

2600 **A.03.13.15:** the authenticity of communications sessions is protected.



2601 **ASSESSMENT METHODS AND OBJECTS**

2602 **Examine**

2603 [SELECT FROM: system and communications protection policy and procedures; procedures  
2604 for session authenticity; system design documentation; system configuration settings; system  
2605 audit records; system security plan; other relevant documents or records]

2606 **Interview**

2607 [SELECT FROM: personnel with information security responsibilities; system administrators]

2608 **Test**

2609 [SELECT FROM: mechanisms for supporting and/or implementing session authenticity]

2610 **REFERENCES**

2611 Source Assessment Procedure: [SC-23](#)

2612 **3.13.16.** Withdrawn

2613 Incorporated into [03.13.08](#).

2614 **3.14. [System and Information Integrity](#)**

2615 **3.14.1. Flaw Remediation**

2616 **REQUIREMENT:** 03.14.01

2617 **ASSESSMENT OBJECTIVE**

2618 *Determine if:*

2619 **A.03.14.01.ODP[01]: time period within which to install security-relevant software**  
2620 **updates after the release of the updates is defined.**

2621 **A.03.14.01.ODP[02]: time period within which to install security-relevant firmware**  
2622 **updates after the release of the updates is defined.**

2623 **A.03.14.01.a[01]:** system flaws are identified.

2624 **A.03.14.01.a[02]:** system flaws are reported.

2625 **A.03.14.01.a[03]:** system flaws are corrected.

2626 **A.03.14.01.b[01]:** security-relevant software updates are installed within **<A.03.14.01.ODP[01]:**  
2627 **time period>** of the release of the updates.

2628 **A.03.14.01.b[02]:** security-relevant firmware updates are installed within **<A.03.14.01.ODP[02]:**  
2629 **time period>** of the release of the updates.

2630 **ASSESSMENT METHODS AND OBJECTS**

2631 **Examine**

2632 [SELECT FROM: system and information integrity policy and procedures; procedures for flaw  
2633 remediation; procedures for configuration management; list of recent security flaw remediation  
2634 actions performed on the system; list of flaws and vulnerabilities that may potentially affect the  
2635 system; test results from the installation of software and firmware updates to correct system

2636 flaws; installation and change control records for security-relevant software and firmware  
2637 updates; system security plan; other relevant documents or records]

2638 **Interview**

2639 [SELECT FROM: personnel responsible for installing, configuring, and/or maintaining the  
2640 system; personnel responsible for flaw remediation; personnel with configuration management  
2641 responsibilities; personnel with information security responsibilities; system administrators]

2642 **Test**

2643 [SELECT FROM: processes for identifying, reporting, and correcting system flaws; processes  
2644 for installing software and firmware updates; mechanisms for supporting and/or implementing  
2645 the reporting and correction of system flaws; mechanisms for supporting and/or implementing  
2646 the testing software and firmware updates]

2647 **REFERENCES**

2648 Source Assessment Procedure: [SI-02](#)

2649 **3.14.2. Malicious Code Protection**

2650 **REQUIREMENT:** 03.14.02

2651 **ASSESSMENT OBJECTIVE**

2652 *Determine if:*

2653 **A.03.14.02.ODP[01]: the frequency at which malicious code protection mechanisms**  
2654 **perform scans is defined.**

2655 **A.03.14.02.a[01]:** malicious code protection mechanisms are implemented at designated  
2656 locations within the system to detect malicious code.

2657 **A.03.14.02.a[02]:** malicious code protection mechanisms are implemented at designated  
2658 locations within the system to eradicate malicious code.

2659 **A.03.14.02.b:** malicious code protection mechanisms are updated as new releases are  
2660 available in accordance with configuration management policy and procedures.

2661 **A.03.14.02.c.01[01]:** malicious code protection mechanisms are configured to perform scans of  
2662 the system **<A.03.14.02.ODP[01]: the frequency>**.

2663 **A.03.14.02.c.01[02]:** malicious code protection mechanisms are configured to perform real-time  
2664 scans of files from external sources at endpoints or network entry and exit points as the files are  
2665 downloaded, opened, or executed.

2666 **A.03.14.02.c.02:** malicious code protection mechanisms are configured to block malicious code,  
2667 quarantine malicious code, or take other actions in response to malicious code detection.

2668 **ASSESSMENT METHODS AND OBJECTS**

2669 **Examine**

2670 [SELECT FROM: system and information integrity policy and procedures; configuration  
2671 management policy and procedures; procedures for malicious code protection; records of  
2672 malicious code protection updates; system design documentation; system configuration  
2673 settings; scan results from malicious code protection mechanisms; record of actions initiated by  
2674 malicious code protection mechanisms in response to malicious code detection; system audit  
2675 records; system security plan; other relevant documents or records]

- 2676 **Interview**
- 2677 [SELECT FROM: personnel responsible for malicious code protection; personnel with system  
2678 installation, configuration, and/or maintenance responsibilities; personnel with information  
2679 security responsibilities; system administrators]
- 2680 **Test**
- 2681 [SELECT FROM: processes for employing, updating, and configuring malicious code protection  
2682 mechanisms; processes for addressing the detection of false positives and resulting potential  
2683 impacts; mechanisms for supporting and/or implementing, employing, updating, and configuring  
2684 malicious code protection mechanisms; mechanisms for supporting and/or implementing  
2685 malicious code scanning and the execution of subsequent actions]
- 2686 **REFERENCES**
- 2687 Source Assessment Procedure: [SI-03](#)

### 2688 **3.14.3. Security Alerts, Advisories, and Directives**

- 2689 **REQUIREMENT:** 03.14.03
- 2690 **ASSESSMENT OBJECTIVE**
- 2691 *Determine if:*
- 2692 **A.03.14.03.a:** system security alerts, advisories, and directives from external organizations are  
2693 received on an ongoing basis.
- 2694 **A.03.14.03.b[01]:** internal security alerts, advisories, and directives are generated, as  
2695 necessary.
- 2696 **A.03.14.03.b[02]:** internal security alerts, advisories, and directives are disseminated, as  
2697 necessary.
- 2698 **A.03.14.03.c:** security directives are implemented in accordance with established time frames.

#### 2699 **ASSESSMENT METHODS AND OBJECTS**

- 2700 **Examine**
- 2701 [SELECT FROM: system and information integrity policy and procedures; procedures for  
2702 security alerts, advisories, and directives; records of security alerts and advisories; system  
2703 security plan; other relevant documents or records]
- 2704 **Interview**
- 2705 [SELECT FROM: personnel with security alert and advisory responsibilities; personnel  
2706 implementing, operating, maintaining, and using the system; personnel, organizational  
2707 elements, and/or external organizations to whom alerts, advisories, and directives are to be  
2708 disseminated; personnel with information security responsibilities; system administrators]
- 2709 **Test**
- 2710 [SELECT FROM: processes for defining, receiving, generating, disseminating, and complying  
2711 with security alerts, advisories, and directives; mechanisms for supporting and/or implementing  
2712 security directives; mechanisms for supporting and/or implementing the definition, receipt,  
2713 generation, and dissemination of security alerts, advisories, and directives]

#### 2714 **REFERENCES**

- 2715 Source Assessment Procedure: [SI-05](#)

2716 **3.14.4. Withdrawn**

2717 Incorporated into [03.14.02](#).

2718 **3.14.5. Withdrawn**

2719 Addressed by [03.14.02](#).

2720 **3.14.6. System Monitoring**

2721 **REQUIREMENT:** 03.14.06

2722 **ASSESSMENT OBJECTIVE**

2723 *Determine if:*

2724 **A.03.14.06.a.01:** the system is monitored to detect attacks and indicators of potential attacks.

2725 **A.03.14.06.a.02:** the system is monitored to detect unauthorized connections.

2726 **A.03.14.06.b:** unauthorized use of the system is identified.

2727 **A.03.14.06.c[01]:** inbound communications traffic is monitored to detect unusual or  
2728 unauthorized activities or conditions.

2729 **A.03.14.06.c[02]:** outbound communications traffic is monitored to detect unusual or  
2730 unauthorized activities or conditions.

2731 **ASSESSMENT METHODS AND OBJECTS**

2732 **Examine**

2733 [SELECT FROM: system and information integrity policy and procedures; procedures for  
2734 system monitoring tools and techniques; continuous monitoring strategy; facility diagram or  
2735 layout; system design documentation; locations within the system where monitoring devices are  
2736 deployed; system configuration settings; system protocols; system audit records; system  
2737 security plan; other relevant documents or records]

2738 **Interview**

2739 [SELECT FROM: personnel with responsibilities for installing, configuring, and/or maintaining  
2740 the system; personnel with system monitoring responsibilities; personnel with intrusion detection  
2741 responsibilities; personnel with information security responsibilities; system administrators]

2742 **Test**

2743 [SELECT FROM: processes for intrusion detection and system monitoring; mechanisms  
2744 supporting and/or implementing system monitoring capabilities; mechanisms for supporting  
2745 and/or implementing intrusion detection and system monitoring capabilities; mechanisms  
2746 supporting and/or implementing the monitoring of inbound and outbound communications traffic]

2747 **REFERENCES**

2748 Source Assessment Procedures: [SI-04](#), [SI-04\(04\)](#)

2749 **3.14.7. Withdrawn**

2750 Incorporated into [03.14.06](#).

2751 **3.14.8. Information Management and Retention**

2752 **REQUIREMENT:** 03.14.08

2753 **ASSESSMENT OBJECTIVE**

2754 *Determine if:*

2755 **A.03.14.08[01]:** CUI within the system is managed in accordance with applicable laws,  
2756 Executive Orders, directives, regulations, policies, standards, guidelines, and operational  
2757 requirements.

2758 **A.03.14.08[02]:** CUI within the system is retained in accordance with applicable laws, Executive  
2759 Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

2760 **A.03.14.08[03]:** CUI output from the system is managed in accordance with applicable laws,  
2761 Executive Orders, directives, regulations, policies, standards, guidelines, and operational  
2762 requirements.

2763 **A.03.14.08[04]:** CUI output from the system is retained in accordance with applicable laws,  
2764 Executive Orders, directives, regulations, policies, standards, guidelines, and operational  
2765 requirements.

2766 **ASSESSMENT METHODS AND OBJECTS**

2767 **Examine**

2768 [SELECT FROM: system and information integrity policy and procedures; laws, Executive  
2769 Orders, directives, policies, regulations, standards, and operational requirements applicable to  
2770 information management and retention; records retention and disposition policy; records  
2771 retention and disposition procedures; media protection policy; media protection procedures;  
2772 audit findings; system security plan; other relevant documents or records]

2773 **Interview**

2774 [SELECT FROM: personnel with information and records management, retention, and  
2775 disposition responsibilities; personnel with information security responsibilities; system  
2776 administrators]

2777 **Test**

2778 [SELECT FROM: processes for information management, retention, and disposition;  
2779 mechanisms for supporting and/or implementing information management, retention, and  
2780 disposition]

2781 **REFERENCES**

2782 Source Assessment Procedure: [SI-12](#)

2783 **3.15. [Planning](#)**

2784 **3.15.1. Policy and Procedures**

2785 **REQUIREMENT:** 03.15.01

2786 **ASSESSMENT OBJECTIVE**

2787 *Determine if:*

- 2788 **A.03.15.01.a[01]**: policies for implementing security requirements are developed and  
2789 documented.
- 2790 **A.03.15.01.a[02]**: policies for implementing security requirements are disseminated to  
2791 organizational personnel or roles.
- 2792 **A.03.15.01.a[03]**: procedures needed to implement security requirements are developed and  
2793 documented.
- 2794 **A.03.15.01.a[04]**: procedures needed to implement security requirements are disseminated to  
2795 organizational personnel or roles.
- 2796 **A.03.15.01.b[01]**: policies and procedures are reviewed periodically.
- 2797 **A.03.15.01.b[02]**: policies and procedures are updated periodically.

## 2798 **ASSESSMENT METHODS AND OBJECTS**

### 2799 **Examine**

2800 [SELECT FROM: security policies and procedures associated with the protection of CUI; audit  
2801 findings; system security plan; other relevant documents or records]

### 2802 **Interview**

2803 [SELECT FROM: personnel with information security responsibilities]

## 2804 **REFERENCES**

2805 Source Assessment Procedures: [AC-01](#), [AT-01](#), [AU-01](#), [CA-01](#), [CM-01](#), [IA-01](#), [IR-01](#), [MA-01](#),  
2806 [MP-01](#), [PE-01](#), [PL-01](#), [PS-01](#), [RA-01](#), [SA-01](#), [SC-01](#), [SI-01](#), [SR-01](#)

## 2807 **3.15.2. System Security Plan**

2808 **REQUIREMENT:** 03.15.02

### 2809 **ASSESSMENT OBJECTIVE**

2810 *Determine if:*

2811 **A.03.15.02.a.01:** a system security plan that defines the constituent system components is  
2812 developed.

2813 **A.03.15.02.a.02:** a system security plan that describes the system operating environment is  
2814 developed.

2815 **A.03.15.02.a.03:** a system security plan that describes any specific threats to the system that  
2816 are of concern to the organization is developed.

2817 **A.03.15.02.a.04:** a system security plan that provides an overview of the security requirements  
2818 for the system is developed.

2819 **A.03.15.02.a.05:** a system security plan that identifies connections to other systems is  
2820 developed.

2821 **A.03.15.02.a.06:** a system security plan that identifies individuals who fulfill system roles and  
2822 responsibilities is developed.

2823 **A.03.15.02.a.07:** a system security plan that includes other relevant information necessary for  
2824 the protection of CUI is developed.

2825 **A.03.15.02.b[01]**: the system security plan is reviewed periodically.

2826 **A.03.15.02.b[02]**: the system security plan is updated periodically.

2827 **A.03.15.02.c:** the system security plan is protected from unauthorized disclosure.

2828 **ASSESSMENT METHODS AND OBJECTS**

2829 **Examine**

2830 [SELECT FROM: security planning policy and procedures; procedures for system security plan  
2831 development and implementation; procedures for security plan reviews and updates; enterprise  
2832 architecture; system security plan; records of system security plan reviews and updates; risk  
2833 assessments; risk assessment results; security architecture and design documentation; other  
2834 relevant documents or records]

2835 **Interview**

2836 [SELECT FROM: personnel with system security planning and plan implementation  
2837 responsibilities; system developers; personnel with information security responsibilities]

2838 **Test**

2839 [SELECT FROM: processes for system security plan development, review, update, and  
2840 approval]

2841 **REFERENCES**

2842 Source Assessment Procedure: [PL-02](#)

2843 **3.15.3. Rules of Behavior**

2844 **REQUIREMENT:** 03.15.03

2845 **ASSESSMENT OBJECTIVE**

2846 *Determine if:*

2847 **A.03.15.03.a[01]:** rules that describe responsibilities and expected behavior for handling CUI  
2848 and system usage are established.

2849 **A.03.15.03.a[02]:** rules of behavior for handling CUI and system usage are provided to  
2850 individuals who require access to the system.

2851 **A.03.15.03.b:** a documented acknowledgement from individuals indicating that they have read,  
2852 understand, and agree to abide by the rules of behavior is received before authorizing access to  
2853 CUI and the system.

2854 **A.03.15.03.c[01]:** the rules of behavior are reviewed periodically.

2855 **A.03.15.03.c[02]:** the rules of behavior are updated periodically.

2856 **ASSESSMENT METHODS AND OBJECTS**

2857 **Examine**

2858 [SELECT FROM: security planning policy and procedures; rules of behavior for system users;  
2859 signed acknowledgements of rules of behavior; records for rules of behavior reviews and  
2860 updates; system security plan; other relevant documents or records]

2861 **Interview**

2862 [SELECT FROM: personnel with rules of behavior establishment, review, and update  
2863 responsibilities; personnel with literacy training and awareness responsibilities; personnel with  
2864 role-based training responsibilities; authorized users of the system who have signed rules of  
2865 behavior; personnel with information security responsibilities]

- 2866           **Test**
- 2867           [SELECT FROM: processes for establishing, reviewing, disseminating, and updating rules of  
2868           behavior; mechanisms for supporting and/or implementing the establishment, dissemination,  
2869           review, and update of rules of behavior]
- 2870           **REFERENCES**
- 2871           Source Assessment Procedure: [PL-04](#)
- 2872   **3.16. System and Services Acquisition**
- 2873   **3.16.1. Acquisition Process**
- 2874           **REQUIREMENT:** 03.16.01
- 2875           **ASSESSMENT OBJECTIVE**
- 2876           *Determine if:*
- 2877           **A.03.16.01.ODP[01]: the security requirements for the system, system component, or**  
2878           **system service are defined.**
- 2879           **A.03.16.01:** the following security requirements are included in the acquisition contract for the  
2880           system, system component, or system service: **<A.03.16.01.ODP[01]: security**  
2881           **requirements>.**
- 2882           **ASSESSMENT METHODS AND OBJECTS**
- 2883           **Examine**
- 2884           [SELECT FROM: system and services acquisition policy and procedures; procedures for the  
2885           integration of information security and SCRM into the acquisition process; configuration  
2886           management plan; acquisition contracts for the system, system component, or system service;  
2887           system design documentation; SCRM plan; system security plan; other relevant documents or  
2888           records]
- 2889           **Interview**
- 2890           [SELECT FROM: personnel with acquisition/contracting responsibilities; personnel with SCRM  
2891           responsibilities; personnel with information security responsibilities; system administrators]
- 2892           **Test**
- 2893           [SELECT FROM: processes for determining system security requirements; processes for  
2894           developing acquisition contracts; mechanisms for supporting and/or implementing acquisitions  
2895           and the inclusion of security requirements in contracts]
- 2896           **REFERENCES**
- 2897           Source Assessment Procedure: [SA-04](#)
- 2898   **3.16.2. Unsupported System Components**
- 2899           **REQUIREMENT:** 03.16.02



2900 **ASSESSMENT OBJECTIVE**

2901 *Determine if:*

2902 **A.03.16.02.a:** system components are replaced when support for the components is no longer  
2903 available from the developer, vendor, or manufacturer.

2904 **A.03.16.02.b:** options for risk mitigation or alternative sources for continued support for  
2905 unsupported components are provided if components cannot be replaced.

2906 **ASSESSMENT METHODS AND OBJECTS**

2907 **Examine**

2908 [SELECT FROM: system and services acquisition policy and procedures; procedures for the  
2909 replacement or continued use of unsupported system components; documented evidence of  
2910 replacing unsupported system components; documented approvals (including justification) for  
2911 the continued use of unsupported system components; SCRM plan; system security plan; other  
2912 relevant documents or records]

2913 **Interview**

2914 [SELECT FROM: personnel with system and service acquisition responsibilities; personnel  
2915 responsible for component replacement; personnel with system development life cycle  
2916 responsibilities; personnel with information security responsibilities]

2917 **Test**

2918 [SELECT FROM: processes for replacing unsupported system components; mechanisms for  
2919 supporting and/or implementing the replacement of unsupported system components]

2920 **REFERENCES**

2921 Source Assessment Procedure: [SA-22](#)

2922 **3.16.3. External System Services**

2923 **REQUIREMENT:** 03.16.03

2924 **ASSESSMENT OBJECTIVE**

2925 *Determine if:*

2926 **A.03.16.03.ODP[01]:** *the security requirements to be employed by external system*  
2927 *service providers are defined.*

2928 **A.03.16.03.a:** the providers of external system services used for the processing, storage, or  
2929 transmission of CUI comply with the following security requirements: **<A.03.16.03.ODP[01]:**  
2930 **security requirements>**.

2931 **A.03.16.03.b:** user roles and responsibilities with regard to external system services, including  
2932 shared responsibilities with external providers, are defined and documented.

2933 **A.03.16.03.c:** processes, methods, and techniques to monitor security requirement compliance  
2934 by external service providers on an ongoing basis are implemented.

2935 **ASSESSMENT METHODS AND OBJECTS**

2936 **Examine**

2937 [SELECT FROM: system and services acquisition policy and procedures; procedures for  
2938 monitoring security requirement compliance by external service providers; acquisition

2939 documentation; contracts; service-level agreements; interagency agreements; licensing  
2940 agreements; list of security requirements for external provider services; assessment results or  
2941 reports from external service providers; SCRM plan; system security plan; other relevant  
2942 documents or records]

2943 **Interview**

2944 [SELECT FROM: personnel with acquisition responsibilities; external providers of system  
2945 services; personnel with SCRM responsibilities; personnel with information security  
2946 responsibilities]

2947 **Test**

2948 [SELECT FROM: organizational processes for monitoring security and privacy control  
2949 compliance by external service providers on an ongoing basis; mechanisms for monitoring  
2950 security and privacy control compliance by external service providers on an ongoing basis]

2951 **REFERENCES**

2952 Source Assessment Procedure: [SA-09](#)

2953 **3.17. [Supply Chain Risk Management](#)**

2954 **3.17.1. Supply Chain Risk Management Plan**

2955 **REQUIREMENT:** 03.17.01

2956 **ASSESSMENT OBJECTIVE**

2957 *Determine if:*

2958 **A.03.17.01.a[01]:** a plan for managing supply chain risks is developed.

2959 **A.03.17.01.a[02]:** the SCRM plan addresses risks associated with the research and  
2960 development of the system, system components, or system services.

2961 **A.03.17.01.a[03]:** the SCRM plan addresses risks associated with the design of the system,  
2962 system components, or system services.

2963 **A.03.17.01.a[04]:** the SCRM plan addresses risks associated with the manufacturing of the  
2964 system, system components, or system services.

2965 **A.03.17.01.a[05]:** the SCRM plan addresses risks associated with the acquisition of the system,  
2966 system components, or system services.

2967 **A.03.17.01.a[06]:** the SCRM plan addresses risks associated with the delivery of the system,  
2968 system components, or system services.

2969 **A.03.17.01.a[07]:** the SCRM plan addresses risks associated with the integration of the system,  
2970 system components, or system services.

2971 **A.03.17.01.a[08]:** the SCRM plan addresses risks associated with the operations and  
2972 maintenance of the system, system components, or system services.

2973 **A.03.17.01.a[09]:** the SCRM plan addresses risks associated with the disposal of the system,  
2974 system components, or system services.

2975 **A.03.17.01.b[01]:** the SCRM plan is reviewed periodically.

2976 **A.03.17.01.b[02]:** the SCRM plan is updated periodically.

2977 **A.03.17.01.c:** the SCRM plan is protected from unauthorized disclosure.

2978 **ASSESSMENT METHODS AND OBJECTS**

2979 **Examine**

2980 [SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition  
2981 policy and procedures; system and services acquisition procedures; procedures for supply  
2982 chain protection; procedures for protecting the SCRM plan from unauthorized disclosure;  
2983 system development life cycle procedures; procedures for the integration of information security  
2984 requirements into the acquisition process; acquisition documentation; service-level agreements;  
2985 acquisition contracts for the system, system components, or system services; list of supply  
2986 chain threats; list of safeguards for supply chain threats; system life cycle documentation; inter-  
2987 organizational agreements and procedures; system security plan; other relevant documents or  
2988 records]

2989 **Interview**

2990 [SELECT FROM: personnel with acquisition responsibilities; personnel with SCRM  
2991 responsibilities; personnel with information security responsibilities]

2992 **Test**

2993 [SELECT FROM: organizational processes for defining and documenting the system  
2994 development life cycle (SDLC); organizational processes for identifying SDLC roles and  
2995 responsibilities; organizational processes for integrating SCRM into the SDLC; mechanisms for  
2996 supporting and/or implementing the SDLC]

2997 **REFERENCES**

2998 Source Assessment Procedure: [SR-02](#)

2999 **3.17.2. Acquisition Strategies, Tools, and Methods**

3000 **REQUIREMENT:** 03.17.02

3001 **ASSESSMENT OBJECTIVE**

3002 *Determine if:*

3003 **A.03.17.02[01]:** acquisition strategies, contract tools, and procurement methods are developed  
3004 and implemented to identify supply chain risks.

3005 **A.03.17.02[02]:** acquisition strategies, contract tools, and procurement methods are developed  
3006 and implemented to protect against supply chain risks.

3007 **A.03.17.02[03]:** acquisition strategies, contract tools, and procurement methods are developed  
3008 and implemented to mitigate supply chain risks.

3009 **ASSESSMENT METHODS AND OBJECTS**

3010 **Examine**

3011 [SELECT FROM: SCRM policy and procedures; SCRM plan; system and services acquisition  
3012 policy and procedures; procedures for supply chain protection; procedures for the integration of  
3013 information security requirements into the acquisition process; solicitation documentation;  
3014 acquisition documentation (including purchase orders); service-level agreements; acquisition  
3015 contracts for the system, system components, or services; documentation of training, education,  
3016 and awareness programs for personnel regarding supply chain risk; system security plan; other  
3017 relevant documents or records]

- 3018 **Interview**
- 3019 [SELECT FROM: personnel with acquisition responsibilities; personnel with SCRM  
3020 responsibilities; personnel with information security responsibilities]
- 3021 **Test**
- 3022 [SELECT FROM: processes for defining and employing tailored acquisition strategies, contract  
3023 tools, and procurement methods; mechanisms for supporting and/or implementing the definition  
3024 and employment of tailored acquisition strategies, contract tools, and procurement methods]
- 3025 **REFERENCES**
- 3026 Source Assessment Procedure: [SR-05](#)
- 3027 **3.17.3. Supply Chain Requirements and Processes**
- 3028 **REQUIREMENT:** 03.17.03
- 3029 **ASSESSMENT OBJECTIVE**
- 3030 *Determine if:*
- 3031 **A.03.17.03.ODP[01]: the security requirements to protect against supply chain risks to**  
3032 **the system, system components, or system services and to limit the harm or**  
3033 **consequences from supply chain-related events are defined.**
- 3034 **A.03.17.03.a:** a process for identifying and addressing weaknesses or deficiencies in the supply  
3035 chain elements and processes is established.
- 3036 **A.03.17.03.b:** the following security requirements are enforced to protect against supply chain  
3037 risks to the system, system components, or system services and to limit the harm or  
3038 consequences of supply chain-related events: **<A.03.17.03.ODP[01]: security requirements>**.
- 3039 **ASSESSMENT METHODS AND OBJECTS**
- 3040 **Examine**
- 3041 [SELECT FROM: SCRM policy and procedures; SCRM strategy; SCRM plan; systems and  
3042 critical system components inventory documentation; system and services acquisition policy  
3043 and procedures; procedures for the integration of security requirements into the acquisition  
3044 process; solicitation documentation; acquisition documentation (including purchase orders);  
3045 acquisition contracts for systems or services; service-level agreements; risk register  
3046 documentation; system security plan; other relevant documents or records]
- 3047 **Interview**
- 3048 [SELECT FROM: personnel with acquisition responsibilities; personnel with information security  
3049 responsibilities; personnel with SCRM responsibilities]
- 3050 **Test**
- 3051 [SELECT FROM: processes for identifying and addressing supply chain element and process  
3052 deficiencies]
- 3053 **REFERENCES**
- 3054 Source Assessment Procedure: [SR-03](#)

## 3055 References

- 3056 [1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available  
3057 at <https://www.govinfo.gov/app/details/PLAW-113publ283>
- 3058 [2] Office of Management and Budget Memorandum Circular A-130, Managing Information as  
3059 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)  
3060 [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)
- 3061 [3] Ross RS, Pillitteri VY (2023) Protecting Controlled Unclassified Information in Nonfederal  
3062 Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg,  
3063 MD), NIST Special Publication (SP) NIST SP 800-171r3 ipd, initial public draft.  
3064 <https://doi.org/10.6028/NIST.SP.800-171r3.ipd>
- 3065 [4] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk:  
3066 Organization, Mission, and Information System View. (National Institute of Standards and  
3067 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39.  
3068 <https://doi.org/10.6028/NIST.SP.800-39>
- 3069 [5] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems  
3070 and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD),  
3071 NIST Special Publication (SP) 800-53A, Rev. 5. [https://doi.org/10.6028/NIST.SP.800-](https://doi.org/10.6028/NIST.SP.800-53Ar5)  
3072 [53Ar5](https://doi.org/10.6028/NIST.SP.800-53Ar5)
- 3073 [6] International Organization for Standardization/International Electrotechnical Commission  
3074 15408-3:2017, Information technology — Security techniques — Evaluation criteria for IT  
3075 security — Part 3: Security assurance requirements, April 2017.  
3076 <https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf>
- 3077 [7] National Institute of Standards and Technology (2019) Security Requirements for  
3078 Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal  
3079 Information Processing Standards Publication (FIPS) 140-3.  
3080 <https://doi.org/10.6028/NIST.FIPS.140-3>
- 3081 [8] Committee on National Security Systems (2022) Committee on National Security Systems  
3082 (CNSS) Glossary. (National Security Agency, Fort George G. Meade, MD), CNSS  
3083 Instruction 4009. Available at <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>
- 3084 [9] Executive Order 13556 (2010) Controlled Unclassified Information. (The White House,  
3085 2340 Washington, DC), DCPD-201000942, November 4, 2010. Available at  
3086 <https://www.govinfo.gov/app/details/DCPD-201000942>

3087	<b>Appendix A. Acronyms</b>
3088	<b>CNSS</b>
3089	Committee on National Security Systems
3090	<b>CUI</b>
3091	Controlled Unclassified Information
3092	<b>FIPS</b>
3093	Federal Information Processing Standards
3094	<b>FISMA</b>
3095	Federal Information Security Modernization Act
3096	<b>GRC</b>
3097	Governance, Risk, and Compliance
3098	<b>ODP</b>
3099	Organization-Defined Parameter
3100	<b>OMB</b>
3101	Office of Management and Budget
3102	<b>OSCAL</b>
3103	Open Security Controls Assessment Language
3104	<b>SCRM</b>
3105	Supply Chain Risk Management
3106	<b>SDLC</b>
3107	System Development Life Cycle
3108	<b>SP</b>
3109	Special Publication

## 3110 **Appendix B. Glossary**

3111 Appendix B provides definitions for the terminology used in NIST SP 800-171A. The definitions  
3112 are consistent with the definitions contained in the Committee on National Security Systems  
3113 (CNSS) Glossary [8] unless otherwise noted.

### 3114 **agency**

3115 Any executive agency or department, military department, Federal Government corporation, Federal Government-  
3116 controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any  
3117 independent regulatory agency. [2]

### 3118 **assessment**

3119 See *security control assessment*.

### 3120 **assessor**

3121 See *security control assessor*.

### 3122 **controlled unclassified information**

3123 Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls,  
3124 excluding information that is classified under Executive Order 13526, Classified National Security Information,  
3125 December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. [9]

### 3126 **information**

3127 Any communication or representation of knowledge such as facts, data, or opinions in any medium or form,  
3128 including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms. [2]

### 3129 **nonfederal organization**

3130 An entity that owns, operates, or maintains a nonfederal system.

### 3131 **nonfederal system**

3132 A system that does not meet the criteria for a federal system.

### 3133 **risk**

3134 A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a  
3135 function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and  
3136 (ii) the likelihood of occurrence. [2]

### 3137 **security**

3138 A condition that results from the establishment and maintenance of protective measures that enable an organization  
3139 to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures  
3140 may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should  
3141 form part of the organization's risk management approach. [8]

### 3142 **security assessment**

3143 See *security control assessment*.

### 3144 **security control**

3145 The safeguards or countermeasures prescribed for an information system or an organization to protect the  
3146 confidentiality, integrity, and availability of the system and its information. [2]

### 3147 **security control assessment**

3148 The testing or evaluation of security controls to determine the extent to which the controls are implemented  
3149 correctly, operating as intended, and producing the desired outcome with respect to meeting the security  
3150 requirements for an information system or organization. [2]

3151 **system**

3152 See *information system*.

3153 **system security plan**

3154 A document that describes how an organization meets the security requirements for a system or plans to meet the  
3155 requirements. In particular, the system security plan describes the system boundary, the environment in which the  
3156 system operates, how the security requirements are implemented, and the relationships with or connections to other  
3157 systems.



3158 **Appendix C. Change Log**

3159 This publication incorporates the following changes from the original edition (June 2018):

- 3160 • Assessment procedures have been updated to be consistent with NIST SP 800-171,  
3161 Revision 3 [3].
- 3162 • Organization-defined parameters (ODPs) have been added to determination statements.
- 3163 • A references section has been added to each assessment procedure providing a hyperlink  
3164 to the source assessment procedure in NIST SP 800-53A [5].

3165 [Table 2](#) shows the changes incorporated into this publication. Errata updates can include  
3166 corrections, clarifications, or other minor changes in the publication that are either *editorial* or  
3167 *substantive* in nature. Any potential updates to this document that are not yet published in an  
3168 errata update or a formal revision, including additional issues and potential corrections, will be  
3169 posted as they are identified. See the publication details for this report. The current release of this  
3170 publication does not include any errata updates.

