| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **RA-5** | VULNERABILITY SCANNING | |
| **RA-5.1**  **RA-5.1.1**  **RA-5.1.1a**  **RA-5.1.1b**  **RA-5.1.2**  **RA-5.1.3**  **RA-5.1.4**  **RA-5.1.4a**  **RA-5.1.4b**  **RA-5.1.4c**  **RA-5.1.5** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines:*    * *the frequency for conducting vulnerability scans on the information system and hosted applications and/or;*    * *the organization-defined process for conducting random vulnerability scans on the information system and hosted applications;* 2. *the organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and/or the organization-defined process for random scans;* 3. *the organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported;* 4. *the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:*    * *enumerating platforms, software flaws, and improper configurations;*    * *formatting/and making transparent checklists and test procedures; and*    * *measuring vulnerability impact, and* 5. *the organization analyzes vulnerability scan reports and results from security control assessments.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with risk assessment and vulnerability scanning responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-2  concurrent controls: AU-6, CA-2, CA-6, CA-7, CM-4, CM-6, CM-7, RA-3, SA-11, SI-2, SI-3,  SI-4  successor controls: CA-5, PM-4 |

|  |  |
| --- | --- |
| **Action Step** | **Potential Assessor Evidence Gathering Actions**  **\*\*See “**[**Assessment Case Overview**](http://csrc.nist.gov/groups/SMA/fisma/assessment-cases-overview.html)**” for selecting, tailoring and executing action steps\*\*** |
|  | *\*\*Assessment Case Assessor Note:* More convincing evidence (i.e., greater assurance) of correct implementation and operating as intended can be obtained through the assessment case actions by:   1. **Replacing bracketed values in action gathering statements to apply greater rigor in the assessment** (e.g, . replacing [“*reviewing*”] with “*studying*” or “*analyzing*”; replacing [“*observing*”] with “*inspecting*” or “*analyzing*”; replacing [“*basic*”] with “*focused*” or “*comprehensive*”); 2. **Replacing bracketed values in action gathering statements to apply greater sample coverage in the assessment** (e.g, . replacing [“*basic”*] sample with “*focused*” or “*sufficiently large”* sample); 3. **Defining additional action steps to the list of action steps suggested herein that exercise additional test methods** (i.e., Examine, Interview or Test) on additional assessment objects. |
| **RA-5.1.1.1**  **RA-5.1.1.1.a**  **RA-5.1.1.1.b** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for:   * the frequency for conducting vulnerability scans on the information system and hosted applications and/or; * the process for conducting random vulnerability scans on the information system and hosted applications. |
|  |  |
| **RA-5.1.2.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to scan for vulnerabilities in the information system and hosted applications in accordance with the frequency identified in RA-5.1.1.1.a and/or the process identified in RA-5.1.1.1.b for random scans. |
| **RA-5.1.2.2** | **Examine** an agreed-upon [*basic*] sample of vulnerability scan reports for the information system and hosted applications; [*reviewing*] for evidence that the measures identified in RA-5.1.2.1 are being applied to conduct vulnerability scans in accordance with the frequency identified in RA-5.1.1.1.a. |
| **RA-5.1.2.3** | **Examine** an agreed-upon [*basic*] sample of vulnerability scan reports for the information system and hosted applications; [*reviewing*] for evidence that the measures identified in RA-5.1.2.1 are being applied to conduct random vulnerability scans in accordance with the process identified in RA-5.1.1.1.b. |
| **RA-5.1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-5.1.2.1 are being applied to conduct vulnerability scans in accordance with the frequency identified in RA-5.1.1.1.a. |
| **RA-5.1.2.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-5.1.2.1 are being applied to conduct random vulnerability scans in accordance with the process identified in RA-5.1.1.1.b. |
|  |  |
| **RA-5.1.3.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the process to be employed to identify and report new vulnerabilities that may potentially affect organization systems/applications. |
| **RA-5.1.3.2** | **Examine** an agreed-upon [*basic*] sample of risk assessments, vulnerability identification reports, security control assessments, or other relevant documents resulting from the process identified in RA-5.1.3.1; [*reviewing*] for evidence that the process identified in RA-5.1.3.1 is being applied. |
| **RA-5.1.3.3** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to scan for vulnerabilities in the information system and hosted applications as a result of the process identified in RA-5.1.3.1 to identify and report new vulnerabilities potentially affecting the system/applications. |
| **RA-5.1.3.4** | **Examine** an agreed-upon [*basic*] sample of vulnerability scan reports resulting from the measures identified in RA-5.1.3.3 for the information system and hosted applications; [*reviewing*] for evidence that the measures identified in RA-5.1.3.3 are being applied. |
| **RA-5.1.3.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-5.1.3.3 are being applied. |
|  |  |
| **RA-5.1.4.1**  **RA-5.1.4.1.a**  **RA-5.1.4.1.b**  **RA-5.1.4.1.c** | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the vulnerability management process to be employed for the information system, and that parts of the process focus on:   * enumerating platforms, software flaws, and improper configurations; * formatting and making transparent checklists and test procedures; and * measuring vulnerability impact. |
| **RA-5.1.4.2** | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, security plan, vulnerability scanning tools and techniques documentation, or other relevant documents; [*reviewing*] for the vulnerability scanning tools and techniques to be employed that use standards to promote interoperability among tools, and that automate parts of the vulnerability management process as identified in RA-5.1.4.1. |
| **RA-5.1.4.3** | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the standards to be used by the tools and techniques identified in RA-5.1.4.2 to promote interoperability among the tools, and automate parts of the vulnerability management process as identified in RA-5.1.4.1. |
| **RA-5.1.4.4** | **Examine** security plan, information system design documentation, vulnerability scanning tools and techniques documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and configuration settings to be employed by the tools and techniques identified in RA-5.1.4.2 to enforce the standards identified in RA-5.1.4.3 that promote interoperability among these tools, and that automate the parts of the vulnerability management process as identified in RA-5.1.4.1. |
| **RA-5.1.4.5** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5.1.4.4; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5.1.4.4 to promote interoperability among the tools identified in RA-5.1.4.2. |
| **RA-5.1.4.6** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.a for enumerating platforms, software flaws, and improper configurations; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5.1.4.4. |
| **RA-5.1.4.7** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.b for formatting and making transparent checklists and test procedures; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5.1.4.4. |
| **RA-5.1.4.8** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.c for measuring vulnerability impact; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5.1.4.4. |
| **RA-5.1.4.9** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.a for enumerating platforms, software flaws, and improper configurations; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **RA-5.1.4.10** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.b for formatting and making transparent checklists and test procedures; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
| **RA-5.1.4.11** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in RA-5.1.4.4 that automate parts of the process identified in RA-5.1.4.1.c for measuring vulnerability impact; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  |  |
| **RA-5.1.5.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to analyze vulnerability scan reports and results from security control assessments. |
| **RA-5.1.5.2** | **Examine** the measures identified in RA-5.1.5.1 to analyze an agreed-upon [*basic*] sample of vulnerability scan reports and results from security control assessments conducted for the information system; [*reviewing*] or [*observing*] for evidence that the measures identified in RA-5.1.5.1 are being applied. |
| **RA-5.1.5.3** | **Interview** organizational personnel with vulnerability scanning and security control assessment responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-5.1.5.1 are being applied to analyze vulnerability scan reports and results from security control assessments. |

|  |  |  |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| **RA-5.2**  **RA-5.2.1**  **RA-5.2.2**  **RA-5.2.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the response times for remediating legitimate vulnerabilities in accordance with an organizational assessment of risk;* 2. *the organization remediates legitimate vulnerabilities in accordance with organization-defined response times; and* 3. *the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with risk assessment and vulnerability scanning responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-2  concurrent controls: CA-2, CA-6, CA-7, CM-4, RA-3, SA-11, SI-2, SI-3, SI-4  successor controls: CA-5, PM-4 |
| **Action Step** | | **Potential Assessor Evidence Gathering Actions** |
| **RA-5.2.1.1** | | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, risk assessment methodology, security plan, or other relevant documents; [*reviewing*] for the risk designations to be assigned to all legitimate vulnerabilities as a result of an organizational assessment of risk. |
| **RA-5.2.1.2** | | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, risk assessment methodology, security plan, or other relevant documents; [*reviewing*] for the response times assigned to the risk designations identified in RA-5.2.1.1 in order to remediate legitimate vulnerabilities assigned to these risk designations as a result of an organizational assessment of risk. |
|  | |  |
| **RA-5.2.2.1** | | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, risk assessment methodology, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to remediate legitimate vulnerabilities based on the risk designation identified in RA-5.2.1.1 and response time identified in RA-5.2.1.2 that are assigned to each vulnerability as a result of an organizational assessment of risk. |
| **RA-5.2.2.2** | | **Examine** an agreed-upon [*basic*] sample of risk assessments, vulnerability scan reports, security control assessments, and corresponding corrective/remediation actions for the information system; [*reviewing*] for evidence that the measures identified in RA-5.2.2.1 are being applied. |
|  | |  |
| **RA-5.2.3.1** | | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the organizational personnel designated to receive information obtained from the vulnerability scanning process and security control assessments. |
| **RA-5.2.3.2** | | **Examine** risk assessment policy, procedures addressing vulnerability management, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to share information obtained from the vulnerability scanning process and security control assessments with the organizational personnel identified in RA-5.2.3.1 to help eliminate similar vulnerabilities in other information systems. |
| **RA-5.2.3.3** | | **Examine** an agreed-upon [*basic*] sample of reports, memos, emails, or other relevant documents communicating results obtained from the vulnerability scanning process and security control assessments to an agreed-upon [*basic*] sample of the personnel identified in RA-5.2.3.1; [*reviewing*] for evidence that the measures identified in RA-5.2.3.2 are being applied. |
| **RA-5.2.3.4** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel with risk assessment and vulnerability scanning responsibilities and/or organizational personnel identified in RA-5.2.3.1; conducting [*basic*] discussions for further evidence that the measures identified in RA-5.2.3.2 are being applied. |
|  | | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(1)** | VULNERABILITY SCANNING |
| **RA-5(1).1**  **RA-5(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization uses vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; records of updates to vulnerabilities scanned; other relevant documents or records].  **Test**: [*select from:* Vulnerability scanning capability and associated scanning tools]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(1).1.1.1** | **Examine** security plan, information system design documentation, vulnerability scanning tools and techniques documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed by the tools and techniques identified in RA-5.1.4.2 to readily update the list of information system vulnerabilities scanned. |
| **RA-5(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5(1).1.1.1. |
| **RA-5(1).1.1.3** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in RA-5(1).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 2** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(2)** | VULNERABILITY SCANNING |
| **RA-5(2).1**  **RA-5(2).1.1**  **RA-5(2).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of updates for information system vulnerabilities scanned; and* 2. *the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-7, RA-3, SI-2, SI-3, SI-4  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(2).1.1.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the frequency for updating the list of information system vulnerabilities to be scanned. |
|  |  |
| **RA-5(2).1.2.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to update the list of information system vulnerabilities scanned in accordance with the frequency identified in RA-5(2).1.1.1 or the process identified in RA-5.1.3.1 to identify and report new vulnerabilities. |
| **RA-5(2).1.2.2** | **Examine** the list of vulnerabilities scanned and records of updates to vulnerabilities scanned; [*reviewing*] for evidence that the measures identified in RA-5(2).1.2.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(3)** | VULNERABILITY SCANNING |
| **RA-5(3).1**  **RA-5(3).1.1**  **RA-5(3).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization employs vulnerability scanning procedures that can demonstrate the breadth of coverage (i.e., information system components scanned); and* 2. *the organization employs vulnerability scanning procedures that can demonstrate the depth of coverage (i.e., vulnerabilities checked).*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and information system components checked; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: RA-2  concurrent controls: CA-2, CA-6, CA-7, CM-4, RA-3, SA-11, SI-2, SI-3, SI-4  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(3).1.1.1** | **Examine** vulnerability scanning procedures; [*reviewing*] for the measures to be employed that can demonstrate a breadth of coverage that identifies the information system components scanned. |
| **RA-5(3).1.1.2** | **Examine** an agreed-upon [*basic*] sample of vulnerability scan reports for the information system; [*reviewing*] for evidence that the procedures identified in RA-5(3).1.1.1 can demonstrate a breadth of coverage that identifies the information system components scanned. |
| **RA-5(3).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the vulnerability scanning procedures identified in RA-5(3).1.1.1 demonstrate a breadth of coverage that identifies the information system components scanned. |
|  |  |
| **RA-5(3).1.2.1** | **Examine** vulnerability scanning procedures; [*reviewing*] for the measures to be employed that can demonstrate a depth of coverage that identifies the vulnerabilities checked. |
| **RA-5(3).1.2.2** | **Examine** an agreed-upon [*basic*] sample of vulnerability scan reports for the information system; [*reviewing*] for evidence that the procedures identified in RA-5(3).1.2.1 demonstrate a depth of coverage that identifies the vulnerabilities checked. |
| **RA-5(3).1.2.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the vulnerability scanning procedures identified in RA-5(3).1.2.1 demonstrate a depth of coverage that identifies the vulnerabilities checked. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(4)** | VULNERABILITY SCANNING |
| **RA-5(4).1**  **RA-5(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization attempts to discern what information about the information system is discoverable by adversaries.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; penetration test results; vulnerability scanning results; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2, CA-7, CM-4, RA-3, SA-11, SI-2, SI-3, SI-4  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(4).1.1.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to attempt to discern what information about the information system is discoverable by adversaries. |
| **RA-5(4).1.1.2** | **Examine** an agreed-upon [*basic*] sample of penetration test results, vulnerability scanning results, or other relevant results for the information system; [*reviewing*] for evidence that the measures identified in RA-5(4).1.1.1 are being applied. |
| **RA-5(4).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that measures identified in RA-5(4).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(5)** | VULNERABILITY SCANNING |
| **RA-5(5).1**  **RA-5(5).1.1**  **RA-5(5).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities; and* 2. *the organization includes privileged access authorization to organization-defined information system components identified for selected vulnerability scanning activities to facilitate more thorough scanning.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; security plan; list of information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: AC-2, AC-3, AC-6, IA-4, CM-5, PE-2, PE-3, RA-3, SA-11, SI-2, SI-3,  successor controls: CM-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(5).1.1.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the vulnerability scanning activities requiring authorized privileged access to information system components to facilitate more thorough scanning. |
| **RA-5(5).1.1.2** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the information system components to which privileged access is to be authorized to perform the vulnerability scanning activities identified in RA-5(5).1.1.1. |
|  |  |
| **RA-5(5).1.2.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to include privileged access authorization to the information system components identified in RA-5(5).1.1.2 in order for the activities identified in RA-5(5).1.1.1 to be performed to facilitate more thorough scanning. |
| **RA-5(5).1.2.2** | **Examine** access authorization records and authorization credentials associated with an agreed-upon [*basic*] sample ofthe information system components identified in RA-5(5).1.1.2; [*reviewing*] for evidence that the measures identified in RA-5(5).1.2.1 are being applied to provide privileged authorized access to these components in order to facilitate more thorough scanning. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(6)** | VULNERABILITY SCANNING |
| **RA-5(6).1**  **RA-5(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; vulnerability scanning tools and techniques documentation; vulnerability scanning results; other relevant documents or records].  **Test**: [*select from:* Vulnerability scanning capability and associated scanning tools]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CM-6, RA-3  successor controls: CA-5, PM-4 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(6).1.1.1** | **Examine** security plan, information system design documentation, vulnerability scanning tools and techniques documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. |
| **RA-5(6).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5(6).1.1.1. |
| **RA-5(6).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in RA-5(6).1.1.1 are being applied to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. |
| **RA-5(6).1.1.4** | **Test** an agreed-upon [*basic*]sample of the automated mechanisms and their configuration settings identified in RA-5(6).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 7** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(7)** | VULNERABILITY SCANNING |
| **RA-5(7).1**  **RA-5(7).1.1**  **RA-5(7).1.2** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency for employing automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials; and* 2. *the organization employs automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated officials in accordance with the organization-defined frequency.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; security plan; information system design documentation; list of unauthorized software; notifications or alerts of unauthorized software on organizational information systems; other relevant documents or records].  **Test**: [*select from:* Vulnerability scanning capability and associated scanning tools]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: CM-2  concurrent controls: AU-6, CA-7, CM-6, IR-4, IR-5, IR-6, RA-3, SA-11, SI-2, SI-3, SI-4  successor controls: CM-7 |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(7).1.1.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the organizational officials to be notified when the presence of unauthorized software on organizational information systems is detected. |
| **RA-5(7).1.1.2** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the frequency for employing automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify the organizational officials identified in RA-5(7).1.1.1. |
|  |  |
| **RA-5(7).1.2.1** | **Examine** security plan, information system design documentation, vulnerability scanning tools and techniques documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to detect the presence of unauthorized software on organizational information systems and notify the organizational officials identified in RA-5(7).1.1.1. |
| **RA-5(7).1.2.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in RA-5(7).1.2.1; [*reviewing*] for evidence that these mechanisms are configured as identified in RA-5(7).1.2.1. |
| **RA-5(7).1.2.3** | **Examine** notifications or alerts provided to the organizational officials identified in RA-5(7).1.1.1.1 when the mechanisms identified in RA-5(7).1.2.1 are employed to detect the presence of unauthorized software on the information system; [*reviewing*] for evidence that these mechanisms are being employed in accordance with the frequency identified in RA-5(7).1.1.2.  Note to assessor: Execution of this assessor action depends on the actual detection of unauthorized software on the information system and the resulting notifications or alerts being generated. |
| **RA-5(7).1.2.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system and/or organizational personnel identified in RA-5(7).1.1.1; conducting [*basic*] discussions for further evidence that the mechanisms and configurations identified in RA-5(7).1.2.1 are being employed in accordance with the frequency identified in RA-5(7).1.1.2. |
|  | |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(8)** | VULNERABILITY SCANNING |
| **RA-5(8).1**  **RA-5(8).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; procedures addressing vulnerability scanning; audit logs; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with vulnerability scanning responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-4  concurrent controls: AU-6, AU-7, AU-8, AU-11, AU-12, CA-7, IR-4, IR-5, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(8).1.1.1** | **Examine** risk assessment policy, procedures addressing vulnerability scanning, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. |
| **RA-5(8).1.1.2** | **Examine** the measures identified in RA-5(8).1.1.1; [*reviewing*] for evidence that these measures are being applied to review historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. |
| **RA-5(8).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning responsibilities for the information system; conducting [*basic*] discussions for further evidence that the measures identified in RA-5(8).1.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **RA-5(9)** | VULNERABILITY SCANNING |
| **RA-5(9).1**  **RA-5(9).1.1**  **RA-5(9).1.1a**  **RA-5(9).1.1b** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization employs an independent penetration agent or penetration team to:*   * *conduct a vulnerability analysis on the information system; and* * *perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Risk assessment policy; security assessment policy; procedures addressing vulnerability analysis; risk assessment; security plan; other relevant documents or records].  **Interview:** [*select from:* Organizational personnel with vulnerability scanning and analysis responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: None  concurrent controls: CA-2, CA-7, SA-11  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **RA-5(9).1.1.1**  **RA-5(9).1.1.1.a**  **RA-5(9).1.1.1.b** | **Examine** risk assessment policy, security assessment policy, procedures addressing vulnerability analysis, security plan, or other relevant documents; [*reviewing*] for the independent penetration agent or penetration team to be employed by the organization to:   * conduct a vulnerability analysis on the information system; and * perform penetration testing on the information system based on the vulnerability analysis identified in RA-5(9).1.1.1.a to determine the exploitability of identified vulnerabilities. |
| **RA-5(9).1.1.2** | **Examine** rules of engagement, vulnerability analysis reports, risk assessments, or other relevant documents associated with conducting a vulnerability analysis on the information system; [*reviewing*] for evidence that the independent penetration agent or penetration team identified in RA-5(9).1.1.1.a is being employed to conduct a vulnerability analysis on the information system. |
| **RA-5(9).1.1.3** | **Examine** penetration test results for the information system and corresponding vulnerability analysis reports, risk assessments, or other relevant documents identified in RA-5(9).1.1.2; [*reviewing*] for evidence that the independent penetration agent or penetration team identified in RA-5(9).1.1.1.b is being employed to perform penetration testing on the information system based on vulnerability analysis to determine the exploitability of identified vulnerabilities. |
| **RA-5(9).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning and analysis responsibilities for the information system; conducting [*basic*] discussions for further evidence that the independent penetration agent or penetration team identified in RA-5(9).1.1.1.a is being employed to conduct vulnerability analyses on the information system. |
| **RA-5(9).1.1.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel with vulnerability scanning and analysis responsibilities for the information system; conducting [*basic*] discussions for further evidence that the independent penetration agent or penetration team identified in RA-5(9).1.1.1.b is being employed to perform penetration testing on the information system based on vulnerability analysis to determine the exploitability of identified vulnerabilities. |