| **assessment case** | | |
| --- | --- | --- |
| ASSESSMENT – Base Control, Part 1 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-6** | AUDIT REVIEW, ANALYSIS, AND REPORTING | |
| **AU-6.1**  **AU-6.1.1**  **AU-6.1.2**  **AU-6.1.3** | **ASSESSMENT OBJECTIVE:**  *Determine if:*   1. *the organization defines the frequency of information system audit record reviews and analyses;* 2. *the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and* 3. *the organization reports findings of inappropriate/unusual activities, to designated organizational officials.*   **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].  **Test**: [*select from:* Information system audit review, analysis, and reporting capability]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, IR-4, IR-5, IR-6, SI-4  successor controls: None |
| **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. |
| **AU-6.1.1.1** | | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, or other relevant documents; [*reviewing*] for the frequency of information system audit record reviews and analyses. |
|  | |  |
| **AU-6.1.2.1** | | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to review and analyze information system audit records for indications of inappropriate or unusual activities in accordance with the frequency identified in AU-6.1.1.1. |
| **AU-6.1.2.2** | | **Examine** an agreed-upon [*basic*] sample of information system audit record reviews/analyses; [*reviewing*] for evidence that the measures identified in AU-6.1.2.1 are being applied. |
| **AU-6.1.2.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit record review, analysis, and reporting; conducting [*basic*] discussions for further evidence that the measures identified in AU-6.1.2.1 are being applied. |
|  | |  |
| **AU-6.1.3.1** | | **Examine** audit and accountability policy, procedures addressing audit review, analysis and reporting, security plan, or other relevant documents; [*reviewing*] for the organizational officials designated to receive reports of findings of inappropriate/unusual activities and the measures to be employed to report such findings to these individuals. |
| **AU-6.1.3.2** | | **Examine** an agreed-upon [*basic*] sample of audit finding reports, audit record reviews/analyses, or other relevant documents provided to the organizational officials identified in AU-6.1.3.1; [*reviewing*] for evidence that the measures identified in AU-6.1.3.1 are being applied. |
| **AU-6.1.3.3** | | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit record review, analysis, and reporting, and the organizational officials identified in AU-6.1.3.1; conducting [*basic*] discussions for further evidence that the measures identified in AU-6.1.3.1 are being applied. |
| ASSESSMENT – Base Control, Part 2 of 2 | | |
| Assessment Information from Special Publication 800-53A Rev. 1 (June 2010) | | |
| **AU-6** | AUDIT REVIEW, ANALYSIS, AND REPORTING | |
| **AU-6.2**  **AU-6.2.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information , intelligence information, or other credible sources of information.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; threat information documentation from law enforcement, intelligence community, or other sources; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. | |
| **Additional Assessment Case Information** | | |
|  | | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14, CA-2, RA-3  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CA-7, IR-4, IR-5, IR-6, SI-4  successor controls: None |

|  |  |
| --- | --- |
| **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. |
| **AU-6.2.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, or other relevant documents; [*reviewing*] for the measures to be employed to adjust the level of audit review, analysis, and reporting performed within the information system in response to changes in the level of risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other sources of information deemed credible and appropriate by the organization. |
| **AU-6.2.1.2** | **Examine** an agreed-upon [*basic*] sample of risk assessments, security assessment reports, continuous monitoring assessment reports, or other relevant documents for the information system; [*reviewing*] for evidence that the measures identified in AU-6.2.1.1 are being applied. |
| **AU-6.2.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for adjusting audit review, analysis and reporting levels within the information system; conducting [*basic*] discussions for further evidence that the measures identified in AU-6.2.1.1 are being applied. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 1** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(1)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(1).1**  **AU-6(1).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; procedures for investigating and responding to suspicious activities; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].  **Test**: [*select from:* Information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, IR-4, IR-5, IR-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(1).1.1.1** | **Examine** procedures addressing audit review, analysis, and reporting, procedures addressing investigation and response to suspicious activities, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including automated mechanisms and their configuration settings) to be employed to integrate audit review, analysis, and reporting activities into the organization’s overall process for investigation and response to suspicious activities. |
| **AU-6(1).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(1).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(1).1.1.1. |
| **AU-6(1).1.1.3** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit review, analysis, and reporting, and organizational personnel responsible for incident monitoring and response; conducting [*basic*] discussions for further evidence that the measures identified in AU-6(1).1.1.1 are being applied. |
| **AU-6(1).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-6(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)** | |
| **AU-6(2)** | AUDIT REVIEW, ANALYSIS, AND REPORTING  [Withdrawn: Incorporated into SI-4]. |
| **AU-6(2).1** | **ASSESSMENT OBJECTIVE:**  [Withdrawn: Incorporated into SI-4].  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  [Withdrawn: Incorporated into SI-4]. |
|  | |
| **ASSESSMENT – Control Enhancement 3** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(3)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(3).1**  **AU-6(3).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system audit records across different repositories; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, IR-4, IR-5, IR-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(3).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the repositories whose audit records are to be analyzed and correlated to gain organization-wide situational awareness. |
| **AU-6(3).1.1.2** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to analyze and correlate audit records across the repositories identified in AU-6(3).1.1.1. |
| **AU-6(3).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(3).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(3).1.1.2. |
| **AU-6(3).1.1.4** | **Examine** the process identified in AU-6(3).1.1.2 to analyze and correlate audit records across an agreed-upon [*basic*] sample of the repositories identified in AU-6(3).1.1.1; [*observing*] for evidence that the process identified in AU-6(3).1.1.2 is being applied. |
| **AU-6(3).1.1.5** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit record review, analysis, and reporting on the repositories identified in AU-6(3).1.1.1; conducting [*basic*] discussions for further evidence that the measures identified in AU-6(3).1.1.2 are being applied. |
| **AU-6(3).1.1.6** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-6(3).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 4** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(4)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(4).1**  **AU-6(4).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the information system centralizes the review and analysis of audit records from multiple components within the system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; security plan; information system audit records; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities].  **Test**: [*select from:* Information system capability for centralizing review and analysis of audit records from multiple information system components]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, IR-4, IR-5, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(4).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the information system components whose audit records are to be subjected to centralized review and analysis. |
| **AU-6(4).1.1.2** | **Examine** security plan, information system design documentation, or other relevant documents; [*reviewing*] for the automated mechanisms and their configuration settings to be employed to centralize the review and analysis of audit records from the information system components identified in AU-6(4).1.1.1. |
| **AU-6(4).1.1.3** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(4).1.1.2; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(4).1.1.2. |
| **AU-6(4).1.1.4** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-6(4).1.1.2; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 5** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(5)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(5).1**  **AU-6(5).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to enhance the ability to identify inappropriate or unusual activity.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; other relevant documents or records].  **Test**: [*select from:* Information system capability for centralizing review and analysis of audit records from multiple information system components]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, IR-4, IR-5, IR-6, RA-5, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(5).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to integrate analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to enhance the ability to identify inappropriate or unusual activity. |
| **AU-6(5).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(5).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(5).1.1.1. |
| **AU-6(5).1.1.3** | **Examine** the process identified in AU-6(5).1.1.1 to integrate analysis of audit records, vulnerability scanning information, performance data, and network monitoring information; [*observing*] for evidence that the process identified in AU-6(5).1.1.1 is being applied. |
| **AU-6(5).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit review, analysis and reporting; conducting [*basic*] discussions for further evidence that the measures identified in AU-6(5).1.1.1 are being applied. |
| **AU-6(5).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-6(5).1.1.1; conducting [*basic*] testing for evidence that these mechanisms are operating as intended. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 6** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(6)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(6).1**  **AU-6(6).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization correlates information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; security plan; other relevant documents or records].  **Test**: [*select from:* Information system capability for centralizing review and analysis of audit records from multiple information system components]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, IR-4, IR-5, IR-6, PE-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(6).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to correlate information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. |
| **AU-6(6).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(6).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(6).1.1.1. |
| **AU-6(6).1.1.3** | **Examine** the process identified in AU-6(6).1.1.1 to correlate information from audit records with information obtained from monitoring physical access; [*observing*] for evidence that the process identified in AU-6(6).1.1.1 is being applied. |
| **AU-6(6).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for audit record review, analysis, and reporting; conducting [*basic*] discussions for further evidence that the measures identified in AU-6(6).1.1.1 are being applied. |
| **AU-6(6).1.1.5** | **Test** an agreed-upon [*basic*] sample of the automated mechanisms and their configuration settings identified in AU-6(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)** | |
| **AU-6(7)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(7).1**  **AU-6(7).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; security plan; other relevant documents or records]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AC-6  concurrent controls: None  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(7).1.1.1** | **Examine** audit and accountability policy, or other relevant documents; [*reviewing*] for the permitted actions specified for each authorized information system process, role, and/or user. |
|  | |
| **ASSESSMENT – Control Enhancement 8** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(8)** | AUDIT REVIEW, ANALYSIS, AND REPORTING  [Withdrawn: Incorporated into SI-4]. |
| **AU-6(8).1** | **ASSESSMENT OBJECTIVE:**  [Withdrawn: Incorporated into SI-4].  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  [Withdrawn: Incorporated into SI-4]. |
|  | |

|  |  |
| --- | --- |
| **ASSESSMENT – Control Enhancement 9** | |
| **Assessment Information from Special Publication 800-53A Rev. 1 (June 2010)** | |
| **AU-6(9)** | AUDIT REVIEW, ANALYSIS, AND REPORTING |
| **AU-6(9).1**  **AU-6(9).1.1** | **ASSESSMENT OBJECTIVE:**  *Determine if the organization performs full-text analysis of privileged functions executed in a physically dedicated information system.*  **POTENTIAL ASSESSMENT METHODS AND OBJECTS:**  **Examine**: [*select from:* Audit and accountability policy; procedures addressing audit review, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].  **Interview**: [*select from:* Organizational personnel with information system audit review, analysis, and reporting responsibilities]. |
| **Additional Assessment Case Information** | |
|  | **POTENTIAL ASSESSMENT SEQUENCING:**  precursor controls: AU-2, AU-3, AU-8, AU-14  concurrent controls: AU-4, AU-5, AU-7, AU-11, AU-12, CM-6, SI-4  successor controls: None |
| **Action Step** | **Potential Assessor Evidence Gathering Actions** |
| **AU-6(9).1.1.1** | **Examine** audit and accountability policy, procedures addressing audit review, analysis, and reporting, security plan, information system design documentation, or other relevant documents; [*reviewing*] for the physically dedicated information system and the measures (including the process and/or the automated mechanisms and their configuration settings) to be employed to perform full-text analysis of privileges functions executed in this system. |
| **AU-6(9).1.1.2** | **Examine** documentation describing the current configuration settings for an agreed-upon [*basic*] sample of the automated mechanisms identified in AU-6(9).1.1.1; [*reviewing*] for evidence that these mechanisms are configured as identified in AU-6(9).1.1.1. |
| **AU-6(9).1.1.3** | **Examine** the process identified in AU-6(9).1.1.1 to perform full-text analysis of privileged functions executed in the information system identified in AU-6(9).1.1.1; [*observing*] for evidence that the process identified in AU-6(9).1.1.1 is being applied. |
| **AU-6(9).1.1.4** | **Interview** an agreed-upon [*basic*] sample of organizational personnel responsible for performing full-text analysis of privileged functions executed in the information system identified in AU-6(9).1.1.1; conducting [*basic*] discussions for further evidence that the measures identified in AU-6(9).1.1.1 are being applied. |