For High-Impact Information Systems

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

AU-1.1 - Examine audit and accountability policy and procedures; other relevant documents or records **and**

Interview organizational personnel with audit and accountability responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents audit and accountability policy and procedures.				
(ii)	The organization disseminates audit and accountability policy and procedures to appropriate elements within the organization.				
(iii)	Responsible parties within the organization periodically review audit and accountability policy and procedures.				
(iv)	The organization updates audit and accountability policy and procedures when organizational review indicates updates are required.				

AU-1.2 - Examine audit and accountability policy and procedures; other relevant documents or records **and**

Interview organizational personnel with audit and accountability responsibilities to determine if the following requirements are met:

Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The audit and accountability policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.				
(ii)	The audit and accountability policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance.				
(iii)	The audit and accountability procedures address all areas identified in the audit and accountability policy and address achieving policy-compliant implementations of all associated security controls.				

AU-2 AUDITABLE EVENTS - The information system generates audit records for the following events: [Assignment: organization-defined auditable events].

AU-2.1 – Examine audit and accountability policy; procedures addressing auditable events; information system security plan (for list of organization-defined auditable events); information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines information system auditable events.				
(ii)	The organization-defined auditable events are adequate to support after-the-fact investigations of security incidents.				
(iii)	The information system generates audit records for the organization-defined auditable events.				

and

Test automated mechanisms implementing information system auditing of organization-defined auditable events.

Test Steps		S	N	Findings	Initials & Date
1					

AU-2(3).1 - Examine audit and accountability policy; procedures addressing auditable events; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization periodically reviews and updates the list of organization-defined auditable events.				

AU-3 CONTENT OF AUDIT RECORDS - The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

AU-3.1- Examine audit and accountability policy; procedures addressing the content of audit records; list of organization-defined auditable events; information system audit records; information system incident reports; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system audit records capture sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.				

and

Test automated mechanisms implementing information system auditing of auditable events.

Test Steps		S	N	Findings	Initials & Date
1					

AU-3(1).1- Examine audit and accountability policy; procedures addressing the content of audit records; information system design documentation; information system security plan; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.				

and

Test information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the information system's audits to ensure that audited events are identified by type, location, or subject.				

AU-4 AUDIT STORAGE CAPACITY - The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-4.1 – Examine audit and accountability policy; procedures addressing audit storage capacity; information system design documentation; organization-defined audit record storage capacity for information system components generating audit records; list of organization-defined auditable events; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines audit record storage capacity for the information system components that generate audit records.				
(ii)	The organization establishes information system configuration settings to reduce the likelihood of the audit record storage capacity being exceeded.				

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES - The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

AU-5.1 – Examine audit and accountability policy; procedures addressing response to audit processing failures; information system design documentation; information system security plan (for list of actions to be taken by the information system in case of an audit processing failure); information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines actions to be taken in the event of an audit processing failure.				
(ii)	The organization defines personnel to be notified in case of an audit processing failure.				
(iii)	The information system alerts appropriate organizational officials and takes any additional organization-defined actions in the event of an audit failure or audit storage capacity being reached.				

and

Test automated mechanisms implementing information system response to audit processing failures.

Test Steps		S	N	Findings	Initials & Date
1					

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING - The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions

AU-6.1 - Examine audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity.				
(ii)	The organization investigates suspicious activity or suspected violations.				
(iii)	The organization reports findings of inappropriate/usual activities, suspicious behavior, or suspected violations to appropriate officials.				
(iv)	The organization takes necessary actions in response to the reviews/analyses of audit records.				

and

Test information system audit monitoring, analysis, and reporting capability.

Test Steps		S	N	Findings	Initials & Date
1					

AU-6.2 - Examine audit and accountability policy; procedures addressing audit monitoring, 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 **and**

Interview organizational personnel with information system audit monitoring, analysis, and reporting responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization increases the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources.				

AU-6(2).1 - Examine audit and accountability policy; procedures addressing audit monitoring, analysis, and reporting; information system design documentation; information system configuration settings and associated documentation; information system security plan (for list of organization-defined inappropriate or unusual activities with security implications); information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines inappropriate or unusual activities with security implications.				
(ii)	The organization employs automated mechanisms to alert security personnel of the occurrence of any organization-defined inappropriate or unusual activities with security implications.				

and

Test automated mechanisms implementing security alerts to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the information system configuration to determine if the organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications by artificially generating auditable events and monitoring the results.				

AU-7 AUDIT REDUCTION AND REPORT GENERATION - The information system provides an audit reduction and report generation capability.

AU-7.1 - Examine audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records **and**

Interview organizational personnel with information system audit monitoring, analysis, and reporting responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides an audit reduction and report generation capability.				

and

Test audit reduction and report generation capability to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the audit reduction and report generation capability by artificially generating a sufficient number of auditable events to cause an audit reduction and report generation condition.				

AU-7(1).1 - Examine audit and accountability policy; procedures addressing audit reduction and report generation; information system design documentation; information system configuration settings and associated documentation; audit reduction, review, and reporting tools; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.				

and

Test audit reduction and report generation capability to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides an audit reduction and report generation capability.				

AU-8 TIME STAMPS - The information system provides time stamps for use in audit record generation.

AU-8.1 - **Examine** audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system provides time stamps for use in audit record generation.				

and

Test automated mechanisms implementing time stamp generation to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the information system configuration to determine if the system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria by artificially generating auditable events based on selected event criteria.				

AU-8(1).1 - **Examine** audit and accountability policy; procedures addressing time stamp generation; information system security plan (for organization-defined frequency for internal clock synchronization for the information system); information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of internal clock synchronization for the information system.				
(ii)	The organization synchronizes internal information system clocks periodically in accordance with organization-defined frequency.				

and

Test automated mechanisms implementing internal information system clock synchronization to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Test the use of time stamps within the audit record generation capability of the information system by artificially generating an auditable event at a known time and compare the time stamp on the resulting audit record.				

AU-9 PROTECTION OF AUDIT INFORMATION - The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

AU-9.1 - **Examine** audit and accountability policy; procedures addressing audit information protection; access control policy and procedures; media protection policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.				

and

Test automated mechanisms implementing audit information protection to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the information system protects audit information and audit tools from unauthorized access, modification, and deletion.				

AU-11 AUDIT RECORD RETENTION - The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11.1 - **Examine** audit and accountability policy; procedures addressing audit record retention; organization-defined retention period for audit records; information system audit records; other relevant documents or records **and**

Interview organizational personnel with information system audit record retention responsibilities determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the retention period for audit records generated by the information system.				
(ii)	The organization retains information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.				