



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Enterprise Audit Management Capability

Version 1.1.1

The Enterprise Audit Management Capability involves the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of the Capability.

07/30/2012



CGS Enterprise Audit Management Capability

Version 1.1.1



Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	5
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	6
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	10
7.3	Supporting Interrelationships.....	11
8	Security Controls	11
9	Directives, Policies, and Standards	16
10	Cost Considerations	21
11	Guidance Statements.....	21



CGS Enterprise Audit Management Capability



Version 1.1.1

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Enterprise Audit Management Capability



Version 1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Enterprise Audit Management Capability involves the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of the Capability. An Enterprise Audit Management solution should be deployed to centralize audit collection and provide appropriate storage for and access to audit data. For each type of audit (specific to system/mission/data), auditable events are identified, auditing is conducted to properly capture and store that data, and analysis and reporting are performed. Certain high-profile events should trigger automated notification to individuals such as systems administrators.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Each agency and Organization within the Enterprise, from the device level in the enclave to the Enterprise and department levels, shall be able to identify security events that have occurred on all platforms, devices, and operating systems. These events can be either human or computer generated and shall be detected from the audit logs and audit-like files from these systems. Other Capabilities, such as the Network Intrusion Detection Capability, can also provide event information to this Capability.

Implementation of an Enterprise-wide audit management system provides the identification, collection, correlation, analysis, storage, and reporting of audit and event information, and monitoring and maintenance of the Capability. These functions are automated and performed in near real-time. Specific responsiveness requirements shall be determined by Enterprise policy. During identification, the system components to be audited for actionable events shall be selected. This includes such components as workstations, servers, gateways, routers, firewalls, as well as embedded devices (e.g., printers with built-in web servers, video teleconferencing bridges, feature phone



CGS Enterprise Audit Management Capability



Version 1.1.1

systems, network sensors). The security events that will cause audit data to be generated, and the elements of audit information to be collected shall also be determined. A date-time stamp based on a system-wide authoritative and trusted source shall always be included. To the extent that they exist, standardized formats shall be used. The Audit Management system and the components being audited shall be fully configurable, and changes to their configurations shall be managed and controlled under the authority of Configuration Management Capabilities.

Collection of audit data shall occur at various levels within a system. In addition, other Capabilities can provide event information to the Enterprise Audit Management Capability. Before further processing can take place, the Enterprise Audit Management Capability shall normalize the audit data to a common format (allows data that originated on different platforms to be understood and accommodates manually generated input). Event correlation occurs in near real-time to detect obvious problems and generate critical event notifications. Detailed analysis is performed in near real-time using automated tools, and administrators perform manual review as needed. Analysts and administrators shall be responsible for reviewing and analyzing logs and alerts provided from other Capabilities to correlate events across the Enterprise, and for generating notifications, as appropriate. Manually (human) produced reports shall be generated periodically or as needed. Results shall be submitted to inform other Capabilities and for further processing (e.g., incident analysis, threat assessment, risk identification), thus establishing an enhanced situational awareness of security-relevant events occurring in the Enterprise.

Storage of audit information shall be centrally managed but may be distributed across multiple devices and geographic locations to meet response time and survivability requirements. All audit information shall be stored securely. Robust backup and recovery procedures shall be documented, in effect, and tested to ensure requirements are met. Backup and recovery procedures shall be tested any time a configuration (hardware or software) change is made to the audit management systems. Access to backup media shall be restricted at the same level as access to the original information and shall also be securely stored. Older audit information shall be moved to offline/archive storage in accordance with policy requirements and as dictated by response time parameters and availability of online storage capacity. Various categories of audit information are retained for the periods specified by Enterprise policy. All audit information shall be discoverable and accessible by authorized requestors. Audit information shall be shared across security domains, when appropriate and in



CGS Enterprise Audit Management Capability



Version 1.1.1

accordance with Enterprise policy, with assistance from the Network Boundary Protection Capability.

Audit reports shall be generated using pre-established (i.e., configured in advance) formats and distributed periodically to authorized recipients based on functional need or subscription. Requestors authorized to submit ad hoc queries shall be able to receive tailored audit reports as needed.

The Enterprise Audit Management system shall monitor its functions and operational status to detect problems. Audit system failures shall be security events that cause the generation of audit information and critical event notifications. The critical nature of Enterprise Audit Management dictates that system operation shall be suspended until the Capability is restored. For this reason, the Audit Management Capability is typically implemented to meet Enterprise-defined high-availability requirements. Capability implementation includes determining and documenting specific audit capability failure conditions and appropriate responses for the Enterprise, based on the mission being supported by the system and the types of audits being done. Capability maintenance shall be performed in response to problems that affect its operation and routinely to make configuration changes in response to direction and changing conditions.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Audits cover physical environments (e.g., facilities), technology, and personnel.
2. Other Capabilities that provide services or input to and/or receive input from Enterprise Audit Management exist and are operational.
3. Devices are generating audit information, and the information selection is configurable.
4. Sufficient infrastructure resources (e.g., network bandwidth, computing power, data repository capacity) are available to support capability implementation. A system-wide authoritative source is available to provide a date-time stamp.
5. The impacts of auditing on system resources and performance are understood and accepted.



CGS Enterprise Audit Management Capability



Version 1.1.1

6. Policies are in place that prescribe specific system-wide audit management requirements and that establish separation of duties among operations, systems administration, and security personnel.
7. Detection may require knowledge and analysis of multiple components in the Enterprise.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability is able to identify the system components to be audited, the security events that will cause audit data to be generated, and the elements of audit information to be collected.
2. The Capability is able to collect audit data from various levels in the system and normalize it to a common data format.
3. The Capability is able to manually input audit data from components that do not automatically generate such data.
4. The Capability is able to perform event correlation and detailed analysis in near real-time using automated tools.
5. The Capability provides a centrally managed storage repository for all audit information that enables the information to be discoverable and accessible in accordance with requestor privilege and authority based on functional need.
6. The Capability is able to balance response time requirements with the availability of online storage capacity by adjusting its configuration to transition audit information to offline/archive storage.
7. The Capability is able to generate reports using pre-established (i.e., configured in advance) formats and in response to ad hoc queries for distribution to authorized requestors.
8. The Capability is able to monitor its functions and operational status and report problems in a timely manner for resolution.
9. The Capability is able to add new and update/maintain existing audit management configurations in response to direction and changing conditions.
10. The Capability is able to exchange information securely with other capabilities.
11. The Capability reviews the Enterprise Audit Management process periodically as defined by IA policies.



CGS Enterprise Audit Management Capability



Version 1.1.1

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Enterprise Audit Management is implemented correctly, the Organization will possess a capability that effectively identifies, collects, correlates, analyzes, stores, and reports audit information. Audit processing functions will use automated tools to ensure response capabilities can react in near real-time to unfolding events.

Correlation and analysis results will be fed to other capabilities (see Capability Interrelationships section below) to alert them to emerging security events, provide corroborating evidence of known events, offer insight into the efficacy of steps taken in response to events, and generally enhance situational awareness of the Enterprise. Similarly, Enterprise Audit Management will be able to initiate, adjust, and control its functions in response to input received from other Capabilities.

The requirements for Enterprise Audit Management reporting to the enclave, Enterprise, or department levels will be identified and documented so it is clear what information is to be passed to the next level at each level, how often, and where it is to be directed. Standardized formats will be used to facilitate interoperability (e.g., Common Event Expression [CEE™] and Common Event Format [CEF]).

Responsive access to securely stored audit information by authorized consumers will be ensured through the use of a centrally managed, distributed data repository and robust infrastructure resources. Scheduled backups will be performed, and media will be securely stored and available when needed for capability recovery. Audit information will not be modified. Attempts to modify audit data will be considered auditable events that will receive close scrutiny. Stored audit information will be discoverable and accessible by authorized users who can search the repository, request standardized reports, and submit ad hoc queries for specialized results.

Because the Enterprise Audit Management Capability must be functioning for overall mission system operation to begin or continue, the Capability will be implemented in accordance with defined high-availability requirements to minimize mission downtime. The Capability will be closely monitored for failure indications, and maintenance actions



CGS Enterprise Audit Management Capability



Version 1.1.1

will be taken quickly to restore operation. Enterprise Audit Management will have adequate system resources available to support its operation with minimal impact to overall mission performance.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Utilization and Performance Management–The Enterprise Audit Management Capability relies on the Utilization and Performance Management Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Hardware Device Inventory–The Enterprise Audit Management Capability relies on the Hardware Device Inventory Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Software Inventory–The Enterprise Audit Management Capability relies on the Software Inventory Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- System Protection–The Enterprise Audit Management Capability relies on the System Protection Capability to provide audit information to assist in the analysis and correlation of records to gain Enterprise-wide situational awareness. The Enterprise Audit Management Capability also relies on the System Protection Capability for security controls to protect the audit system from unauthorized (accidental or intentional) modification, destruction, or disclosure.
- Network Boundary Protection–The Enterprise Audit Management Capability relies on the Network Boundary Protection Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness. The Enterprise Audit Management Capability uses the Network Boundary Protection Capability to enable the sharing of audit data across security domains.



CGS Enterprise Audit Management Capability



Version 1.1.1

- Access Management—The Enterprise Audit Management Capability relies on the Access Management Capability to establish policies and processes that access rights to the audit system and its resources. The Enterprise Audit Management Capability relies on the Access Management Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Digital Policy Management—The Enterprise Audit Management Capability relies on the Digital Policy Management Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Metadata Management—The Enterprise Audit Management Capability relies on the Metadata Management Capability to enable information sharing by managing the metadata associated with stored audit information that makes it discoverable and accessible. The Enterprise Audit Management Capability relies on the Metadata Management Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Signature Repository—The Enterprise Audit Management Capability relies on the Signature Repository Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Network Enterprise Monitoring—The Enterprise Audit Management Capability relies on information from the Network Enterprise Monitoring Capability to make adjustments to its audit functions in response to potential problems detected and under review. The Enterprise Audit Management Capability also relies on the Network Enterprise Monitoring Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Physical Enterprise Monitoring—The Enterprise Audit Management Capability relies on information from the Physical Enterprise Monitoring Capability to make adjustments to its audit functions in response to potential problems detected and under review. The Enterprise Audit Management Capability also relies on the Physical Enterprise Monitoring Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Personnel Enterprise Monitoring—The Enterprise Audit Management Capability relies on information from the Personnel Enterprise Monitoring Capability to make adjustments to its audit functions in response to potential problems detected and under review. The Enterprise Audit Management Capability also relies on the Personnel Enterprise Monitoring Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.



CGS Enterprise Audit Management Capability



Version 1.1.1

- Network Intrusion Detection—The Enterprise Audit Management Capability relies on information from the Network Intrusion Detection Capability to make adjustments to its audit functions in response to potential problems detected and under review. The Enterprise Audit Management Capability also relies on the Network Intrusion Detection Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Host Intrusion Detection—The Enterprise Audit Management Capability relies on information from the Host Intrusion Detection Capability to make adjustments to its audit functions in response to potential problems detected and under review. The Enterprise Audit Management Capability also relies on the Host Intrusion Detection Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Incident Response—The Enterprise Audit Management Capability relies on information from the Incident Response Capability to make adjustments to focus its audit collection, correlation, and analysis functions based on steps being taken in reaction to specific incidents.
- Incident Analysis—The Enterprise Audit Management Capability relies on information from the Incident Analysis Capability to make adjustments to focus its audit collection, correlation, and analysis functions based on specific incident characteristics.
- Network Intrusion Prevention—The Enterprise Audit Management Capability relies on the Network Intrusion Prevention Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Host Intrusion Prevention—The Enterprise Audit Management Capability relies on the Host Intrusion Prevention Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Operations and Maintenance—The Enterprise Audit Management Capability relies on the Operations and Maintenance Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Enterprise Audit Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Enterprise Audit Management Capability relies on the IA Policies, Procedures, and Standards Capability to



CGS Enterprise Audit Management Capability



Version 1.1.1

provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Enterprise Audit Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Enterprise Audit Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Enterprise Audit Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Identity Management–The Enterprise Audit Management Capability relies on the Identity Management Capability to provide audit information for analysis and correlation to gain Enterprise-wide situational awareness.
- Vulnerability Assessment–The Enterprise Audit Management Capability relies on the Vulnerability Assessment Capability for information about potential problems that enables audit activities to adjust in order to learn more about the problems.
- Risk Monitoring–The Enterprise Audit Management Capability relies on the Risk Monitoring Capability for information used to make adjustments to its functions as the Enterprise risk posture changes over time.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
AU-2 AUDITABLE EVENTS	Control: The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be



CGS Enterprise Audit Management Capability



Version 1.1.1

	<p>capable of auditing the following events: [Assignment: organization-defined list of auditable events];</p> <p>b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;</p> <p>c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and</p> <p>d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].</p> <p>Enhancement/s: (3) The organization reviews and updates the list of auditable events [Assignment: organization-defined frequency].</p> <p>(4) The organization includes execution of privileged functions in the list of events to be audited by the information system.</p>
<p>AU-3 CONTENT OF AUDIT RECORDS</p>	<p>Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.</p> <p>Enhancement/s:</p> <p>(1) The information system includes [Assignment: organization-defined additional, more detailed information] in the audit records for audit events identified by type, location, or subject.</p> <p>(2) The organization centrally manages the content of audit records generated by [Assignment: organization-defined information system components].</p>
<p>AU-4 AUDIT STORAGE CAPACITY</p>	<p>Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.</p> <p>Enhancement/s: None Specified</p>
<p>AU-5 RESPONSE TO</p>	<p>Control: The information system:</p>



CGS Enterprise Audit Management Capability



Version 1.1.1

<p>AUDIT PROCESSING FAILURES</p>	<p>a. Alerts designated organizational officials in the event of an audit</p>
<p>AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING</p>	<p>Control: The organization:</p> <p>a. Reviews and analyzes information system audit records processing failure; and</p> <p>b. 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)].</p> <p>Enhancement/s:</p> <p>(1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of maximum audit record storage capacity.</p> <p>(2) The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].</p> <p>(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [Selection: rejects or delays] network traffic above those thresholds.</p> <p>(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists. [Assignment: organization-defined frequency] for indications of inappropriate or unusual activity, and report's findings to designated organizational officials; and</p> <p>b. 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.</p> <p>Enhancement/s:</p> <p>(1) The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.</p> <p>(3) The organization analyzes and correlates audit records across different repositories to gain organization-wide</p>



CGS Enterprise Audit Management Capability



Version 1.1.1

	<p>situational awareness.</p> <p>(4) The information system centralizes the review and analysis of audit records from multiple components within the system.</p> <p>(5) The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.</p> <p>(6) The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.</p> <p>(7) The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.</p> <p>(8) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts].</p> <p>(9) The organization performs, in a physically dedicated information system, full-text analysis of privileged functions executed.</p>
<p>AU-7 AUDIT REDUCTION AND REPORT GENERATION</p>	<p>Control: The information system provides an audit reduction and report generation capability.</p> <p>Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records.</p> <p>Enhancement/s:</p> <p>(1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.</p>
<p>AU-8 TIME STAMPS</p>	<p>Control: The information system uses internal system clocks to generate time stamps for audit records.</p> <p>Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern</p>



CGS Enterprise Audit Management Capability



Version 1.1.1

	<p>continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.</p> <p>Enhancement/s:</p> <p>(1) The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source].</p>
<p>AU-9 PROTECTION OF AUDIT INFORMATION</p>	<p>Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.</p> <p>Enhancement/s:</p> <p>(1) The information system produces audit records on hardware-enforced, write-once media.</p> <p>(2) The information system backs up audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.</p> <p>(3) The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.</p> <p>(4) The organization:</p> <p>(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and</p> <p>(b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.</p>
<p>AU-11 AUDIT RECORD RETENTION</p>	<p>Control: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.</p> <p>Enhancement/s: None Specified</p>
<p>AU-12 AUDIT GENERATION</p>	<p>Control: The information system:</p> <p>a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components];</p> <p>b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and</p> <p>c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.</p>



CGS Enterprise Audit Management Capability



Version 1.1.1

	<p>Enhancement/s:</p> <p>(1) The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].</p> <p>(2) The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.</p>
AU-14 <i>SESSION AUDIT</i>	<p>Control: The information system provides the capability to:</p> <p>a. Capture/record and log all content related to a user session; and</p> <p>b. Remotely view/hear all content related to an established user session in real time.</p> <p>Enhancement/s:</p> <p>(1) The information system initiates session audits at system start-up.</p>
CM-5 <i>ACCESS RESTRICTIONS FOR CHANGE</i>	<p>Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.</p> <p>Enhancement/s:</p> <p>(2) The organization conducts audits of information system changes [Assignment: organization-defined frequency] and when indications so warrant to determine whether unauthorized changes have occurred.</p>
SI-4 <i>INFORMATION SYSTEM MONITORING</i>	<p>(16) The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.</p>

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Enterprise Audit Management Directives and Policies

Title, Date, Status	Excerpt / Summary
---------------------	-------------------



CGS Enterprise Audit Management Capability



Version 1.1.1

Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Enterprise Audit Management Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	



CGS Enterprise Audit Management Capability



Version 1.1.1

Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, September 2009, Unclassified	Summary: This document provides an overview of firewall technologies and discusses their security capabilities and relative advantages and disadvantages; examples of where firewalls can be placed within networks and the implications of deploying firewalls in particular locations; and recommendations for establishing firewall policies and for selecting, configuring, testing, deploying, and managing firewall solutions. The firewall configuration process includes setting up logging and alerts. Logging is a critical step in preventing and recovering from failures as well as ensuring that proper security configurations are set on the firewall. Proper logging can also provide vital information for responding to security incidents. Whenever possible, firewalls should be configured both to store logs locally and to send them to a centralized log management infrastructure.
NIST SP 800-61, Rev 1, Computer Security Incident Handling Guide, March 2008, Unclassified	Summary: This document provides practical guidelines on responding to computer security incidents effectively and efficiently, and establishing an effective incident response program. Its primary focus is detecting, analyzing, prioritizing, and handling incidents. In describing incident analysis, the use of centralized logging is recommended. Organizations should deploy one or more centralized logging servers and configure logging devices throughout the Organization to send duplicates of their log entries to the centralized logging servers.
NIST SP 800-77, Guide to IPsec VPNs, December 2005, Unclassified	Summary: This document provides an overview of the types of security controls that can provide protection for Transmission Control Protocol/Internet Protocol (TCP/IP) network communications, which are widely used throughout the world. Internet Protocol Security (IPsec) is a framework of open standards for ensuring private



CGS Enterprise Audit Management Capability



Version 1.1.1

	<p>communications over public networks and has become the most common network layer security control, typically used to create a virtual private network (VPN). The solution design section on log management states that IPSec should be configured so it logs sufficient details regarding successful and failed login attempts to support troubleshooting and incident response activities. Such logging should adhere to the Organization's policies on log management, such as requiring copies of all log entries to be sent through a secure mechanism to centralized log servers.</p>
<p>NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, August 2006, Unclassified</p>	<p>Summary: This document provides detailed information on establishing a computer and network forensic capability, including the development of policies and procedures. It describes the processes for performing effective forensics activities and provides advice regarding different sources of data. The description of how the forensics process is performed includes the implementation of centralized logging, which means that certain systems and applications forward copies of their logs to secure central log servers. Centralized logging prevents unauthorized users from tampering with logs and employing anti-forensic techniques to impede analysis.</p>
<p>NIST SP 800-92, Guide to Computer Security Log Management, September 2006, Unclassified</p>	<p>Summary: This document provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an Enterprise. It covers several topics, including establishing log management infrastructures, and developing and performing robust log management processes throughout an Organization.</p>
<p>NIST SP 800-113, Guide to SSL VPNs, July 2008, Unclassified</p>	<p>Summary: This document discusses the fundamental technologies and features of Secure Sockets Layer (SSL) VPNs. It discusses the fundamental technologies and features of SSL VPNs, describes SSL and how it fits within the context of layered network security, and presents a phased approach to SSL VPN planning and implementation that can help in achieving successful SSL VPN deployments. The solution design section on log</p>



CGS Enterprise Audit Management Capability



Version 1.1.1

	management states that SSL VPN devices should be configured so they log sufficient details regarding successful and failed login attempts to support troubleshooting and incident response activities. Such logging should adhere to the Organization’s policies on log management, such as requiring copies of all log entries to be sent through a secure mechanism to centralized log servers.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Common Event Expression (CEE™), under development, Unclassified	Summary: The Common Event Expression (CEE™) is an initiative to create an open community-developed event interoperability standard for electronic systems. CEE™ standardizes the way computer events are described, logged, and exchanged. It consists of several specifications: Common Log Transport (CLT), Common Log Syntax (CLS), Common Event Expression Taxonomy (CEET), and Common Event Log Recommendations (CELR). Together they will provide the framework for a community consensus in log transportation, log syntax, event representation, and event logging recommendations for various log sources and scenarios. Tasks including log correlation and aggregation, enterprise-wide log management, auditing, and incident handling—which once required expensive, specialized analysts or equipment—can now be performed more efficiently and produce better results.
Common Event Format (CEF), Unclassified	Summary: The Common Event Format (CEF) developed by ArcSight is an extensible, text-based, high-performance format designed to support multiple device types from security and non-security devices and applications. It is an open log management standard that improves the



CGS Enterprise Audit Management Capability



Version 1.1.1

	interoperability of security-related information from different security and network devices and applications. CEF is the first log management standard to support a broad range of device types, enabling technology companies and customers to use a common event log format so that data can easily be collected and aggregated for analysis by an Enterprise management system.
ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems, 1 March 2007, Unclassified	Summary: This standard provides guidance and specifies standards to be used by organizations providing audit and certification of information security management systems (ISMS).

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Audit oversight—Needed to provide additional resources to ensure oversight measures are in place and followed.
2. Storage requirements—Aggregated audit information needs to be stored securely.



CGS Enterprise Audit Management Capability



Version 1.1.1

3. Degree of customization beyond “as-delivered” functionality—Customized solutions may be more difficult to collect audit information from.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Enterprise Audit Management Capability.

- The Enterprise audit management solution shall identify, collect, correlate, analyze, store, and report audit information, monitoring, and maintenance of the Enterprise. The solution shall be deployed to centralize audit collection and provide appropriate storage for and access to audit data.
- The Enterprise shall identify security events (human or computer generated) that have occurred on all platforms, devices, and operating systems at the device, department, and Enterprise level.
- The Enterprise shall implement an Enterprise-wide audit system that provides the identification, collection, correlation, analysis, storage, and reporting of audit and event information in an automated and real-time manner.
- During identification, the system components to be audited for actionable events shall be selected. This includes workstations, servers, gateways, routers, firewalls, as well as embedded devices (e.g., printers with built-in web servers, video teleconferencing bridges, feature phone systems, network sensors).
- The Enterprise shall determine the security events that will cause audit data to be generated and the elements of audit information to be collected.
- A date-time stamp based on a system-wide authoritative and trusted source shall be included with audit data.
- To the extent that they exist, standardized formats shall be used with audit data.
- The audit management system and the components being audited shall be fully configurable, and changes to their configurations shall be managed and controlled under the authority of a configuration management system.
- All audit data collected and received shall be normalized to a common format (allows data that originated on different platforms to be understood and accommodates manually generated input) before further processing can take place.
- Event correlation shall occur in near real-time to detect obvious problems and generate critical event notifications.



CGS Enterprise Audit Management Capability



Version 1.1.1

- Detailed analysis shall be performed in near real-time using automated tools, and analysts/administrators shall perform manual review of logs and alerts as needed to correlate events and generate notifications.
- Manually (human) produced reports shall be generated periodically or as needed, and results shall be submitted to inform other systems and for further processing (e.g., incident analysis, threat assessment, risk identification).
- Storage of audit information shall be centrally managed and shall be distributed across multiple devices and geographic locations when necessary to meet response time and survivability requirements.
- All audit information shall be stored securely.
- Backup and recovery procedures shall be documented and tested any time a configuration (hardware or software) change is made to the audit management systems.
- Older audit information shall be moved to offline/archive storage in accordance with policy requirements and as dictated by response time parameters and availability of online storage capacity.
- All audit information shall be discoverable and accessible by authorized requestors.
- Audit information shall be shared across security domains, when appropriate and in accordance with Enterprise policy.
- Audit reports shall be generated using pre-established (i.e., configured in advance) formats and distributed periodically to authorized recipients based on functional need or subscription.
- Requestors authorized to submit ad hoc queries shall be able to receive tailored audit reports as needed.
- The Enterprise shall monitor the functions and operational status of the Enterprise audit management system to detect problems.
- Audit system failures shall be security events that cause the generation of audit information and critical event notifications.
- If an audit system failure occurs, the system operation shall be suspended until the audit system is restored.
- Enterprise audit management systems shall be implemented to meet Enterprise-defined high-availability requirements.
- The Enterprise shall determine and document specific audit capability failure conditions and appropriate responses for the Enterprise, based on the mission being supported by the system and the types of audits being done.



CGS Enterprise Audit Management Capability



Version 1.1.1

- Maintenance shall be performed in response to problems that affect the audit system's operation and routinely to make configuration changes in response to direction and changing conditions.