



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Incident Analysis Capability

Version 1.1.1

Incident Analysis uses information gathered during Incident Response to determine the root cause of an incident. The Incident Analysis generated is used to develop, recommend, and coordinate Enterprise mitigation actions for technical, personnel, physical, and environmental incidents.



CGS Incident Analysis 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.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	6
7	Capability Interrelationships.....	9
7.1	Required Interrelationships	9
7.2	Core Interrelationships	11
7.3	Supporting Interrelationships.....	12
8	Security Controls	12
9	Directives, Policies, and Standards	14
10	Cost Considerations	16
11	Guidance Statements.....	17



CGS Incident Analysis 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 Incident Analysis 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.

Incident Analysis uses information gathered during Incident Response to determine the root cause of an incident. The Incident Analysis generated is used to develop, recommend, and coordinate Enterprise mitigation actions for technical, personnel, physical, and environmental incidents.

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.

Enterprise Incident Analysis, along with other Gold Standard Capabilities, provides the full spectrum approach to information gathering, analysis, and reporting. This Capability specifically focuses on the ability to analyze. Analysis shall be performed for technical, personnel, physical, and environmental incidents within the Enterprise.

The Incident Analysis Capability provides the capability to analyze any incident, whether it is external to the network, such as with external enterprises (e.g., financial, partner, or law enforcement), or an information technology (IT) related incident. Incident Analysis employs and provides the ability to perform root cause analysis and reporting on the full spectrum of technical, personnel, physical, and environmental incidents. Each of these incidents shall feed into the Incident Analysis Capability.

Incident Analysis shall be available in a timely manner, and standards shall be established governing an acceptable timeframe. The timeframe for analysis shall depend on the severity of the incident. In some cases, Incident Response and Incident Analysis may overlap. Incident Response and Incident Analysis both include damage assessments to determine the scope of the incident. Incident Analysis examines a security incident to determine the extent of the damage, how the event transpired, and what corrective actions can be taken to prevent future occurrences.



CGS Incident Analysis Capability



Version 1.1.1

To provide effective Incident Analysis, an Incident Analysis Team and a process shall be in place. The Incident Analysis Team may comprise internal Organization staff, or Incident Analysis services may be obtained from an external team such as the Computer Network Defense Service Provider (CNDSP). Whether the team is internal or external, the Incident Analysis Team shall be overseen by an experienced team coordinator. This expert shall be responsible for coordinating the efforts of the team and ensuring that all procedures are followed. Upon receiving notification of an incident, the team coordinator shall determine whether there is enough information to create an incident report and will reach out to the Incident Analysis Team that has been identified, if needed. Some information is collected during Incident Response; however, additional information may need to be collected, depending on the specific information needs of the Incident Analysis Team performing the root cause analysis. Upon receiving additional analysis, the team coordinator shall determine whether all required information exists to enable a determination of the root cause.

The Incident Analysis Team shall include individuals with specialized knowledge in the incident areas. These individuals shall bring to the team expertise in technical issues, and strategic leadership in research, examination, and analysis of security topics and trends. Within the team there shall be a wide range of knowledge and skills covering technical, personnel, physical, and environmental incidents such that any team member can reach out to other team members when dealing with an incident outside of his or her personal knowledge and skills. The team shall also have the ability to reach out to subject matter experts outside of the team, when necessary. The Analysis Team shall gather information and perform analysis through various mechanisms such as system integrity checks, traffic identification, processes, operating systems, and resident information (i.e., in memory).

The world of information security is constantly changing. New exploits are discovered daily. To keep up with the industry and be effective at their jobs, members of the Incident Analysis Teams shall receive ongoing training to hone their skills and learn about the newest innovations and challenges. Suitable reference materials shall be made available to the teams to use when they conduct additional research about an incident. Incident Analysis Teams shall have access to any tools or software needed to perform the analysis. These tools will not always be the same, because root cause analysis will require various tools, such as tools to perform different types of forensic analysis, depending on the incident. An environment with the proper tools shall exist to



CGS Incident Analysis Capability



Version 1.1.1

support the specific type of forensic analysis regardless of where the team has to perform the analysis.

If Incident Analysis services are performed by an external team, the appropriate agreements shall be in place. These agreements include Non-Disclosure Agreements (NDAs), Memorandums of Understanding (MOUs), and Scope Definition Documents. It is important to understand the external team's processes and ensure they have the appropriate skill sets and clearance levels to perform the analysis.

The Incident Analysis Capability begins with ensuring that root cause analysis is performed at the Enterprise level to identify the systemic problems. All information to support the analysis shall be gathered upon receiving notification of an incident. The process of gathering information is a cyclical process that will continue until all questions are answered. Incident Analysis shall determine how an incident was executed, know every asset that was touched, identify all resources that were compromised, and provide the information to the appropriate Community Gold Standard (CGS) Capabilities to secure all affected assets. Full exposure to the incident shall be provided to the Analysis Team to enable the team to determine any points of reentry for the adversary. Doing so will enable a better analysis and application of the appropriate mitigations. The Incident Analysis Capability shall provide feedback to Incident Response to resume normal operations and provide feedback to the process for identifying incidents (see Detection Capabilities), as well as to Information Assurance (IA) Training and IA Awareness. Root cause analysis may also result in triggering additional Incident Responses.

The Incident Analysis Capability shall provide reporting to the Threat Assessment and Risk Mitigation Capabilities, as well as to consumers, based on the type of incident and the Enterprise's requirements. The Incident Analysis Capability shall capture lessons learned and provide an Enterprise mitigation plan to help prevent future incidents. Throughout the Incident Analysis process, the Incident Analysis information and results shall be maintained in a centrally managed data repository. The root cause analysis may result in a short list of attribution (i.e., who was behind the incident). Such attribution is critical to understanding the strategic intent of the adversary and devising an appropriate mitigation plan. Attributable sources shall be identified and results fed to the Threat Assessment and Risk Mitigation Capabilities for corrective measures.

Incident Analysis information shall be shared with other Enterprises and be discoverable and accessible in accordance with established information sharing policies. The need to



CGS Incident Analysis Capability



Version 1.1.1

partner with an Enterprise during Incident Analysis is dependent on the type of incident. Partners may include law enforcement, other federal agencies, or other internal organizations within the Enterprise.

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. A forensic capability exists within the Enterprise.
2. Monitoring and detection capabilities exist within the Enterprise.
3. Incident Analysis Teams have sufficient resource access to perform an effective analysis.
4. Evidence has been preserved to enable performance of Incident Analysis.
5. Incident Response has occurred or is in the process of occurring.

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 provides root cause analysis of incidents related to technical, personnel, physical, and environmental assets.
2. The Capability provides cataloging/classification of the incident and placing it in a searchable place.
3. Incident Analysis reports are provided to stakeholders to affect overall Enterprise security.
4. Incidents have the potential not to repeat themselves in the exact same manner.
5. Incident Analysis cannot always identify aspects of the root cause.

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).



CGS Incident Analysis Capability



Version 1.1.1

For an Organization to successfully implement or use an Incident Analysis Capability, the Organization will have the ability to analyze any incident within the Enterprise, which includes technical, personnel, physical, and environment incidents. This analysis can be performed by a team internal or external to the Organization.

When an Organization stands up its own internal Incident Analysis Capability, the Organization will ensure that there is a dedicated Incident Analysis Team, which includes a team coordinator who is responsible for coordination and management of the team. The team will consist of a group of dedicated individuals with specialized knowledge and the skill sets that range the multitude of areas where incidents can occur (technical, personnel, physical, and environmental). The Organization will ensure team members have expertise in technical issues and strategic leadership in research, examination, and analysis of security topics and trends. The Organization will provide a documented Incident Analysis process that includes standard operating procedures (SOPs) and a Concept of Operations (CONOPS). When the Incident Analysis Capability is implemented internally, each Organization will ensure Incident Analysis Team members receive ongoing training to maintain skills and learn about the newest innovations and challenges. Suitable reference materials will be made available to the teams to support research activities.

For external Incident Analysis Capabilities, the Organization will ensure the CNDSP has the appropriate skill sets for the specific incident and has the appropriate clearance levels, and that agreements are in place, as defined in the Gold Standard definition. The CNDSP will also provide its documented process to the Organization for review. Whether the Capability is internal or external, the Organization will ensure the Incident Analysis Capability is available in a timeframe consistent with the severity of the incident.

Incident Analysis is crucial to the ongoing defense of an Enterprise. Each intrusion will be fully investigated by an Organization to make adjustments that will prevent future incidents. Every Organization has vulnerabilities, some of which are well known and some of which are relatively or completely unknown. The Organization's Incident Analysis Capability will identify which vulnerabilities the adversary took advantage of to gain access to the Enterprise. By identifying specific vulnerabilities and implementing countermeasures, it is more likely that future incidents using the same weaknesses may be prevented.



CGS Incident Analysis Capability



Version 1.1.1

Each Organization that obtains sufficient evidence that a breach to the Enterprise has occurred will assess the extent and severity of the breach. The Organization will leverage the Risk Mitigation Capability to determine the realistic alternatives for addressing the compromised entity given ongoing mission and/or business requirements and the degree of difficulty in resuming operations.

Each Organization will perform root cause analysis once an incident has been reported and mission function has been restored. The Organization will identify the real cause of the incident, the root problem, and not just a symptom of the problem. Root cause analysis is a disciplined process that may take hours, days, or weeks. Organizations will ensure there is a cyclical process to determine how an incident was executed, know every asset that was touched, identify all resources that were compromised, and secure all affected assets. The Organization will establish procedures that allow the team coordinators to determine whether they have enough information to write the incident report (who, what, where, how) and will ensure there is a supporting team of individuals with required skill sets to perform analysis when needed. The Organization will ensure mechanisms are in place for individuals to gather information and perform analysis, such as system integrity checks, traffic identification, processes, operating systems, and resident information (i.e., in memory). The Organization will ensure that information that was collected during Incident Response is available to the Analysis Team along with any additional information that may be needed. The Analysis Team will use logs from the Enterprise Audit Capability to recreate each step the adversary took (where possible).

Each Organization will ensure that the analysis is appropriately documented in an Incident Analysis report and made available to other CGS Capabilities such as Threat Assessment and Risk Mitigation. The Organization will provide reporting to consumers based on the type of incident and the Organization's requirements. Incident Analysis reports include, but are not limited to, the following:

- Intelligence Analysis Reports
- National Security Information Systems Incident Program (NSISIP) Reports
- Effectiveness Reports
- Efficiency Reports

The Organization will capture lessons learned and Enterprise mitigation recommendations to proactively address other areas susceptible to the same incident. See the Capability Interrelationships section for other areas within the Gold Standard scope that assist with Enterprise feedback.



CGS Incident Analysis Capability



Version 1.1.1

Each Organization will identify and coordinate with partner organizations to share Incident Analysis information. The Organization will ensure appropriate Organization-level agreements are in place and will provide information for others to consume for awareness. Partners may include, but are not limited to, the following: National Cyber Investigative Joint Task Force (NCI JTF), National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), United States Computer Emergency Readiness Team (US-CERT), and law enforcement/counterintelligence (LECI).

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.

- Network Mapping—The Incident Analysis Capability relies on the Network Mapping Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Network Boundary and Interfaces—The Incident Analysis Capability relies on the Network Boundary and Interfaces Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Utilization and Performance Management—The Incident Analysis Capability relies on the Utilization and Performance Management Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Understand Mission Flows—The Incident Analysis Capability relies on the Understand Mission Flows Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.



CGS Incident Analysis Capability



Version 1.1.1

- Understand Data Flows—The Incident Analysis Capability relies on the Understand Data Flows Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Hardware Device Inventory—The Incident Analysis Capability relies on the Hardware Device Inventory Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Software Inventory—The Incident Analysis Capability relies on the Software Inventory Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Understand the Physical Environment—The Incident Analysis Capability relies on the Understand the Physical Environment Capability for information used to understand the Enterprise environment, inform its decision-making processes, and formulate the details of possible courses of action.
- Configuration Management—The Incident Analysis Capability relies on the Configuration Management Capability for information used to determine whether a configuration change or implementation contributed to an incident.
- Network Security Evaluations—The Incident Analysis Capability relies on the Network Security Evaluations Capability for information about the cause of incidents.
- Network Enterprise Monitoring—The Incident Analysis Capability relies on the Network Enterprise Monitoring Capability for information used to provide notification of incidents.
- Physical Enterprise Monitoring—The Incident Analysis Capability relies on the Physical Enterprise Monitoring Capability for information used to provide notification of incidents.
- Personnel Enterprise Monitoring—The Incident Analysis Capability relies on the Personnel Enterprise Monitoring Capability for information used to provide notification of incidents.
- Network Intrusion Detection—The Incident Analysis Capability relies on the Network Intrusion Detection Capability for information used to provide notification of incidents.
- Host Intrusion Detection—The Incident Analysis Capability relies on the Host Intrusion Detection Capability for information used to provide notification of incidents.



CGS Incident Analysis Capability



Version 1.1.1

- Network Hunting—The Incident Analysis Capability relies on the Network Hunting Capability for information used to provide notification of incidents.
- Physical Hunting—The Incident Analysis Capability relies on the Physical Hunting Capability for information used to provide notification of incidents.
- Enterprise Audit Management—The Incident Analysis Capability relies on the Enterprise Audit Management Capability for information used to provide notification of incidents.
- Incident Response—The Incident Analysis Capability relies on the Incident Response Capability to provide information about incidents.
- Network Intrusion Prevention—The Incident Analysis Capability relies on the Network Intrusion Prevention Capability for information used to determine the root cause of an incident.
- Host Intrusion Prevention—The Incident Analysis Capability relies on the Host Intrusion Prevention Capability for information used to determine the root cause of an incident.
- Contingency Planning—The Incident Analysis Capability relies on the Contingency Planning Capability to provide mission disruption and recovery information to inform its root cause analysis processes and for the formulation of possible courses of action.
- Risk Mitigation – The Incident Analysis Capability relies on the Risk Mitigation Capability to eliminate the vulnerabilities that caused the incident and restore the Enterprise to pre-incident operational status.

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 Incident Analysis 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 Incident Analysis Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness—The Incident Analysis Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.



CGS Incident Analysis Capability



Version 1.1.1

- IA Training—The Incident Analysis Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities—The Incident Analysis 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.

- Risk Analysis—The Incident Analysis Capability relies on the Risk Analysis Capability for information used to make adjustments to its functions as the Enterprise risk posture changes over time.
- Risk Monitoring—The Incident Analysis 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-7 AUDIT REDUCTION AND REPORT GENERATION	Control: The information system provides an audit reduction and report generation capability. 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. Enhancement/s: (1) The information system provides the capability to automatically process audit records for events of interest based



CGS Incident Analysis Capability



Version 1.1.1

	on selectable event criteria.
IR-4 INCIDENT HANDLING	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (3) The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions. (4) The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
IR-5 INCIDENT MONITORING	<p>Control: The organization tracks and documents information system security incidents.</p> <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
IR-6 INCIDENT REPORTING	<p>Control: The organization:</p> <ul style="list-style-type: none"> a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to designated authorities. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
SI-4 INFORMATION SYSTEM MONITORING	<p>Enhancement/s:</p> <ul style="list-style-type: none"> (2) The organization employs automated tools to support near real-time analysis of events.



CGS Incident Analysis Capability



Version 1.1.1

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.

Incident Analysis Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
DRAFT IC Standard 2008-xx Federal Information Security Management Act (FISMA) Compliance Reporting, 2008	Summary: Purpose: To standardize how member agencies of the IC report to the Associate Director of National Intelligence (ADNI) and CIO and the Office of the DNI Inspector General (ODNI/OIG) to meet the Federal Information Security Management Act (FISMA) reporting requirements... This Draft Standard addresses Incident Reporting –Intelligence Community members do not report directly to the US-CERT; incidents are reported to the JTF-GNO (for DoD IC) and the IC/IRC who, in turn, report to the US-CERT.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-61, Rev 1, Computer Security Incident Handling Guide, March 2008, Unclassified	Summary: This publication seeks to assist Organizations by providing practical guidelines on responding to incidents. The Incident Response has four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity.
NIST SP 800-83, Guide to Malware Incident	Summary: This special publication provides recommendations for improving an Organization's malware



CGS Incident Analysis Capability



Version 1.1.1

Prevention and Handling, November 2005, Unclassified	incident prevention measures and gives extensive recommendations for enhancing the existing Incident Response Capability so that it is better prepared to handle malware incidents, particularly widespread ones. Organizations should have a robust Incident Response process capability that addresses malware incident handling. During the detection and analysis phase, they should strive to detect and validate malware incidents rapidly by monitoring alerts produced by technical controls (e.g., antivirus software, spyware detection and removal utilities, intrusion detection systems) to identify likely impending malware incidents.
NIST SP 800-86, Guide to Integrating Forensic Techniques Into Incident Response, April 2006, Unclassified	Summary: This special publication helps Organizations in investigating computer security incidents. The process for performing digital forensics contains the following phases: Collection, Examination, Analysis, and Reporting. This guide provides general recommendations for performing the forensic process.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Incident Analysis Standards

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



CGS Incident Analysis Capability



Version 1.1.1

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	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

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. Travel expenses—The Incident Analysis Team may need to travel somewhere when an incident occurs.
2. Research costs—This Capability needs to know how to tailor standardized functions to meet the specialized needs of the Enterprise systems.



CGS Incident Analysis Capability



Version 1.1.1

3. Number of connections—The more network and Internet connections in an Enterprise, the greater the amount of work the Incident Analysis Team will have to perform.
4. Infrastructure—The Incident Analysis Team will have to be able to operate in various environments that feature different facilities, computers, networks, voice equipment, software, and specialized technology.
5. Solution used for implementation—The Enterprise can establish the Incident Analysis Capability internally or use external contracts. If established internally, the Enterprise must provide the necessary tools for response.
6. Time to implement, maintain, and execute—Analysis processes can take time, especially if approval is needed to begin work.

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 Incident Analysis Capability.

- The Enterprise shall perform incident analysis using a full spectrum approach to information gathering, analysis, and reporting.
- The Enterprise shall establish an incident analysis process.
- The Enterprise shall perform incident analysis for technical, personnel, physical, and environmental incidents.
- Incident analysis shall provide the capability to analyze any incident, whether external or internal to the Enterprise.
- Incident analysis shall employ and provide the ability to perform root cause analysis and reporting on the full spectrum of technical, personnel, physical, and environmental incidents.
- The Enterprise shall establish standards governing an acceptable timeframe for incident analysis activities.
- The timeframe for incident analysis shall depend on the severity of the incident.
- Incident analysis shall include damage assessments to determine the scope of the incident.
- Incident analysis shall examine a security incident to determine the extent of the damage.
- Incident analysis shall examine a security incident to determine how the event transpired.



CGS Incident Analysis Capability



Version 1.1.1

- Incident analysis shall examine a security incident to determine what corrective actions can be taken to prevent future occurrences.
- The Enterprise shall establish an incident analysis team.
- Incident analysis teams shall be overseen by an experienced team coordinator who is responsible for coordinating the incident analysis activities.
- The incident analysis team shall be composed of individuals with specialized knowledge in incident areas including technical, personnel, physical, and environmental incidents.
- The incident analysis team shall have the ability to reach out to appropriate subject matter experts, when necessary.
- The incident analysis team shall use a variety of mechanisms to gather information including system integrity checks, traffic identification, processes, operating systems, and resident information (i.e., in memory).
- Incident analysis personnel shall receive ongoing training to remain up to date with changing technology and evolving threats.
- Suitable reference materials shall be made available to incident analysis teams to use when they conduct additional research about an incident.
- Incident analysis teams shall have access to any tools or software needed to perform the analysis.
- If incident analysis services are performed by a team external to the Enterprise, appropriate agreements including NDAs, MOUs, and Scope Definition Documents shall be in place governing their involvement and activities.
- Incident analysis begins with ensuring that root cause analysis shall be performed at the Enterprise level to identify systemic problems.
- All information to support root cause analysis shall be gathered by the incident analysis team upon receiving notification of an incident.
- Incident analysis activities shall determine how an incident was executed, know every asset that was touched, identify all resources that were compromised, and provide information to other appropriate systems to secure all affected assets.
- The incident analysis team shall be provided full exposure to the incident to determine any points of reentry for the adversary, perform a better analysis, and facilitate the application of appropriate mitigations.
- The incident analysis team shall provide feedback to the Enterprise as to when affected systems can resume normal operations.
- The incident response team shall provide feedback to the Enterprise processes for identifying incidents. Root cause analysis may also result in triggering additional incident responses.



CGS Incident Analysis Capability



Version 1.1.1

- The incident analysis team shall provide reports to appropriate Enterprise stakeholders.
- The incident analysis team shall capture lessons learned and provide an Enterprise mitigation plan to help prevent future incidents.
- Incident analysis information and results shall be maintained in a centrally managed data repository.
- Attributable sources of the cause of incidents shall be identified and results fed into the additional appropriate Enterprise systems for corrective measures.
- The Enterprise shall make incident analysis information available to other Organizations, when appropriate, in accordance with Enterprise policy.