



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Risk Analysis Capability

Version 1.1.1

The Risk Analysis Capability collects and analyzes risk-related data from the Risk Identification Capability for the broader purpose of providing decision-makers information on the benefits, costs, and uncertainty of alternative courses of action with respect to executing the assigned mission in multiple environments. The risk-related data comprises known threats and vulnerabilities and their combined impact. The threat and vulnerability information is aggregated from the Threat and Vulnerability Assessment Capabilities during the risk identification process in the Risk Identification Capability.

07/30/2012



CGS Risk 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.....	7
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	11
7.1	Required Interrelationships	11
7.2	Core Interrelationships	12
7.3	Supporting Interrelationships.....	13
8	Security Controls	13
9	Directives, Policies, and Standards	15
10	Cost Considerations	20
11	Guidance Statements.....	20



CGS Risk 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 Risk 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.

The Risk Analysis Capability collects and analyzes risk-related data from the Risk Identification Capability for the broader purpose of providing decision-makers information on the benefits, costs, and uncertainty of alternative courses of action with respect to executing the assigned mission in multiple environments. The risk-related data comprises known threats and vulnerabilities and their combined impact. With this in mind, a simple notional function that demonstrates the relative notional relationships between Risk, Threat, Vulnerability, and Impact is $R = f(T, V, I)$, as represented by a portfolio of attacks. The threat and vulnerability information is aggregated from the Threat and Vulnerability Assessment Capabilities during the risk identification process in the Risk Identification Capability.

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.

Conducting Risk Analysis reveals the likelihood and impact of possible threats (potential attacks by specified adversaries) to the network. To truly capture the entire picture of Risk Analysis an appropriate formula to use would be $R = f(T, V, I)$, with the specific function being dependent on the definition of the variables. The threat and vulnerability information is generated in the Threat and Vulnerability Assessment Capabilities, and the relationship of those is established in the Risk Identification Capability. The Risk Identification Capability shall provide the identified risks to the Risk Analysis Capability. How T, V, and I are defined will impact the weight each of these variables places on the equation.

Risk Analysis is conducted centrally (meaning by a specific Organization or role) to maintain consistency. The degree of centrality of Risk Analysis is a function of the type of risk decision that is being made. The Risk Analysis is reviewed and accepted at the



CGS Risk Analysis Capability



Version 1.1.1

level where the Organization has assigned risk management decision authority. This can be delegated locally or retained at a corporate or community level. For example, for the operational risk management decisions, a centrally managed Risk Analysis process to provide the information needed to make a quick response decision may not be responsive enough to the decision-cycle time. On the other hand, a centrally managed Risk Analysis effort associated with certification and accreditation (C&A) types of risk management decisions may be appropriate because the decision-cycle time is greater and the alternative decisions more complex. In addition, there is a need to compare decisions made with this C&A decision with standards and/or previous C&A decisions. Risks shall be reassessed regularly (appropriate to the subject of analysis) to facilitate awareness and areas such as compliance or design trade-off decisions. Risk Analysis is also dependent on the latitude of decision-making given by the Organization to the risk decision-maker to “accept the risk.” Residual or accepted risks feed the Risk Mitigation Capability and all Detect Events Capabilities as well as shape the risk posture.

The most effective method of Risk Analysis is dependent on the type of decision that needs to be made. For example, Risk Analysis will be conducted differently for a C&A determination than for an architectural framework decision. The parameters of the decision type also have to be taken into account. These parameters include whether the decision needs to be made in a certain period of time and what data is available to make that decision. These are important to the type of Risk Analysis conducted.

The basic steps in a Risk Analysis are:

- Foundation Research and Incident Analysis—This is the basic foundation information (threat/vulnerability information will be aggregated in the Risk Identification Capability) collection activity of 1) discovering basic vulnerabilities to systems, technologies, and applications from the Vulnerability Assessment Capability; 2) collecting information about the culture, attitudes, preferences, capabilities, and known and potential attack activities of various known and potential adversaries from the Threat Assessment Capability; 3) conducting analyses of reported incidents from the Incident Analysis Capability, to derive meanings and understanding from specific incidents and diagnosing broader trends from statistical analyses of composite incidents; and 4) conducting analysis of the costs of defending against attacks (acquisition, performance, manpower, interoperability, ease of use, among others) against attacks within the system’s attack portfolio.
- Basic Area-Specific Analyses—These are the traditional independent analyses that provide additional insights and meanings to the basic body of collected



CGS Risk Analysis Capability



Version 1.1.1

information. The typical approach to developing these analyses is to assign them to specialty Organizations to produce a specialty focus report. These separate reports are separately forwarded to the decision-makers and used as the basis for their risk decisions. Each analysis typically results in a single-focus viewpoint and recommendations of 1) vulnerabilities of a system (aggregated and provided by Risk Identification); 2) threats to a system (aggregated and provided by Risk Identification); or 3) operational impact to a mission of loss of information or capability. Using these separate reports as the decision information forces the decision-maker to internally synthesize the results of these separate reports.

- Synthesized Risk Analysis—Risk Analysis is taking these separate area-specific analyses and conducting a synthesized focus analysis that combines and relates elements of the specialty-area analyses to address and answer specific issues necessary for making effective risk management decisions. This approach applies additional analytical resources to synthesize and apply the vulnerability, threat, mission impact, and countermeasure information to the specific system and situation. Multidiscipline teams (Risk Team) are brought together with the express purpose of digesting, analyzing, and interpreting the information to better assist the decision-makers in conducting this synthesis. The three steps of this synthesized Risk Analysis are:
 1. Identify and Characterize—This type of analysis groups individual vulnerabilities into mission attack scenarios and then compares and contrasts these various scenarios based on the following: a) the immediate objective of the attack (i.e., defeat confidentiality, integrity, or availability); b) the ultimate impact on an operational mission; c) the costs and resources needed by an adversary in mounting the attack; d) the risks incurred by an adversary through possible detection, attribution, and retaliation; and e) the likelihood of the attack being successful given hypothesized expenditure of resources.
 2. Develop Theory of Adversarial Behavior—This analysis looks at the menu of attacks developed in the previous step from the perspective of various adversaries, or adversary groups, to determine which set of attacks they would more likely invest in during various phases of a conflict or competition. This helps to place the previously analyzed attacks in an adversary perspective by relating the attacks to the following: a) adversary objectives, intentions, and motives; b) adversary capabilities; c) adversary resources; d) adversary tolerance for risk; and e) adversary preferences for different attacks or attack characteristics.



CGS Risk Analysis Capability



Version 1.1.1

3. Develop Theory of Mission Impact—This analysis takes the previous two analyses a step further by placing a value on what the ultimate operational impact might be, given that attacks of various types by various adversaries are successful. This step tries to put into an operational perspective the harm that can result from a successful attack. This resultant harm takes into account the Organization's capability to detect and block the attacks, ability to continue effective operations in the face of successful attacks, and ability to recover and reconstitute within an operationally acceptable period of time. This information makes up the risk posture for the Enterprise, which documents the desired or accepted risk state.

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. Tradeoffs exist between characteristics of risk management alternative courses of action.
2. Not all levels of the variables used to estimate risk are known or easily quantifiable.
3. Risk Analysis Teams have sufficient access to the data to perform their analysis (mission and data flows, architectures, system descriptions, appropriately characterized vulnerability and system attack information, adversary and adversary attack preference information to cover the lifecycle and conflict continuum situations in which the system exists, and appropriately characterized defensive measures considered as part of the set of potential risk management courses of action, among others).
4. A core of analysts, risk modelers, and community-vetted analytical tools and methodologies are employed to appropriately analyze the costs and benefits of alternative risk management decisions and provide results to the decision-makers in a form and format that best supports them in making informed risk management decisions.

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.



CGS Risk Analysis Capability



Version 1.1.1

1. The Capability prioritizes instances of risk.
2. The Capability places in a system attack framework the characterization and adversary exploitation behaviors of all identified vulnerabilities....
3. The Capability estimates unknown levels of $p(\text{success} | \text{attempt})$, $p(\text{attempt})$, mission impact and other relevant input variables and use sound analytical techniques to estimate the risks associated with system attacks and the costs and benefits of alternative risk management courses of action to the best of its ability.
4. The Capability provides the results of the analytics that analysts and decision-makers will use to determine mitigation strategies (if the same analysts are not performing both the Risk Analysis and Risk Mitigation).
5. The Risk Analysis is put in a form and format that is consumable by decision-makers.
6. The Capability provides information for decision-makers who will be responsible for making the decision.
7. Mission Harm (Impact), system architecture, design, and operations, risk identification, and characterized defensive measure information are made available to this Capability.
8. This Capability establishes the risk posture for the Enterprise.

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).

Traditionally Organizations have followed an approach of "find a vulnerability—fix a vulnerability." This assumes that any vulnerability discovered can lead to such a devastating mission impact that we have no alternative but to immediately invest resources to eliminate it. Unfortunately there are usually insufficient resources to pursue this approach. Limited resources need to be more efficiently expended against the vulnerabilities and attacks that will be most harmful to the mission. These are difficult decisions and require effective analysis to provide sound decision information and recommendations.



CGS Risk Analysis Capability



Version 1.1.1

Risk Analysis is a part of all phases of system development and operation, starting with requirements specification, through development, deployment, operation and maintenance, to system decommission. Risk Analysis is not always technology-centric and also applies to physical/environmental and personnel factors. Again, these factors contribute to making the decision on the most appropriate type of Risk Analysis to be conducted.

Selecting the most appropriate Risk Analysis data, methodology, and associated tools for the analytical task is important to the Risk Analysis process. No universal tool does everything. In most cases, a variety of tools and methodologies need to be tailored and appropriately applied to the analysis at hand.

Addressing the following issues will help the Organization make the best Risk Analysis approach selection.

1. **Select the Best Approach Based on Risk Management Decisions To Be Supported**—The purpose of conducting an analysis is to provide analytical results to help decision-makers make informed decisions. When decisions involve any competing alternative courses of action, multiple criteria to evaluate these alternatives, multiple scenarios, and/or complex relationships, analysis is often conducted to clarify and put into perspective for the decision-makers the benefits and costs of the various alternative courses of action. The decision may be to select one of the analyzed courses of action or it may be to provide insight into the complexity of the decision space so that the decision-maker can direct and scope further analysis.
2. **Select the Best Approach Based on the Scope, Issues Associated with the System Being Analyzed**—Analyses of large complex decision spaces can provide many different focuses of the analysis and can consume a large amount of time and resources collecting data and analyzing marginally important issues if not properly scoped. Understanding the type of information needed by a decision-maker to make more informed decisions can help to focus the available time and resources on uncovering the most important information and relationships for the decision.
3. **Select the Best Approach Based on the Level of Granularity of Design Detail Necessary to Define and Decide Between Alternative Courses of Action**—Analyses can be conducted at many different levels of granularity. The more detail, the more complex the relationships and the more time and resources needed to collect and analyze the data. If the risk management decision is to choose between two different alternative systems, the level of granularity that will



CGS Risk Analysis Capability



Version 1.1.1

be used is the level needed to sufficiently distinguish between the alternatives. If that can be done at a system or sub-system level, it may not be worth the time and effort to analyze down to the component or piece-part level.

4. Select the Best Approach Based on the Availability of Data That Can Be Collected Within the Decision Cycle Time—Associated with the level of detail granularity needed by the decision-maker in determining the appropriate level of detail of the analysis is the level of granularity of the available data to conduct the analysis. The data is the foundation of any analysis. If there is a great discrepancy between the level of granularity needed by the decision-maker and the level of available data, some translation and transformation functions may be needed to condition the collected information to be appropriate for the analysis. A subfunction of this issue is the necessity of selecting the appropriate units of measure for the available data and transformation functions. Not all risk methodologies are appropriate for all forms of data. Understanding the units of measure of the collected data may determine the proper methodology selected, and/or the methodology selected may dictate the units of measure of the collected data. It is important that the data units of measure and methodology correspond to one another.
5. Select the Best Approach Based on the Constraints Imposed on the Analysis—All analyses have constraints. These come in the form of scope limitations, defined assumptions, time to conduct the analysis, resources to conduct the analysis (budget, skills, personnel, facilities, data, etc.), and, although not always explicitly defined, "believability" factors that influence whether decision-makers will accept or believe the results of the analysis. While it is often natural to discuss most of these constraints when establishing an analysis plan of action, the "believability" factor is one that is worthwhile exploring with the decision-makers early in the analysis. It could involve refining the assumption parameters to make sure they cover the scenarios the decision-makers want addressed. It could involve including or excluding elements within the scope of the analysis. Or it could involve the "believability" of the data, data sources, and/or analysis methodology. It is helpful to understand and uncover prior to the analysis what aspects of an analysis would make the results more "believable" or "less believable" to the decision-makers.
6. Select the Best Approach Based on the Need for Comparability Across Risk Analysis Results—Some decisions are one-time decisions independent of other decisions such that the results, assumptions, value scales, and methodologies need to be internally consistent and accurate but not necessarily identical and comparable to the results of other analyses. Project-specific environment, value



CGS Risk Analysis Capability



Version 1.1.1

scales, data units of measure, and assumptions can be used. In this case, the relative value of the results is a necessary trait. There are other decisions that are a specific instance of a series of decisions where the results of one analysis need to be compared with the results of other analyses. In this case, more care and effort shall be made to define the environment, the value scales, the data units of measure, and the assumptions so that all analyses to be compared are consistent and drawing from the same data sources. The absolute value within the defined scales of the analysis is a necessary trait in this case. Developing the comparable analysis framework will take more time, resources, and cooperation from the community conducting these analyses than an analysis that does not require its results to be compared directly with others.

The major elements of a security Risk Analysis methodology and some issues to consider with them are described below:

1. Output Presentation of Results to decision-maker—Issues to be considered:
 - a. Accurate reflection of the results of the analysis
 - b. Appropriate identification of analysts' interpretation of results
 - c. Presentation in a form and format understandable to the decision-maker
 - d. Granularity of detail and focus necessary to help inform decision-makers about the specific decision
 - e. Clarity of scope, assumptions, methodology, origin of data, and results confidence interval (quantitative or intuitive).
2. Analysis Results—Issues to be considered:
 - a. Appropriateness of results to supporting decisions
 - b. Accuracy of results based on data, methodology, and assumptions
 - c. Clarity of the meaning and units of measure of the results
 - d. Granularity of the results
 - e. Sensitivity of results to input and assumptions.
3. Analysis Techniques—Issues to be considered:
 - a. Soundness of analytical techniques
 - b. Appropriateness of techniques for the desired problem insights
 - c. Appropriateness of techniques for type and units of measure of the input data
 - d. Accuracy of the implementation of the analytical techniques.
4. Analysis Input Data—Issues to be considered:
 - a. Soundness of the data definition in terms of meaning and units of measure
 - b. Accuracy of data derived from data source or data transformation functions



CGS Risk Analysis Capability



Version 1.1.1

- c. Reliability of the source of the data
 - d. Appropriateness of data for analytical techniques.
5. Data Transformation and Conditioning—Issues to be considered:
 - a. Soundness of the data transformation and conditioning theory
 - b. Accuracy of the implementation of the transformation and conditioning theory
 - c. Appropriateness of the transformation and conditioning theory to the data and analytical techniques.
6. Data Collection—Issues to be considered
 - a. Reliability of the source(s) of the data
 - b. Accuracy of the collected data
 - c. Soundness of the data collection techniques
 - d. Appropriateness of the data collected to the decision and analytical techniques.

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 Risk Analysis Capability relies on the Network Mapping Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Network Boundary and Interfaces—The Risk Analysis Capability relies on the Network Boundary and Interfaces Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Utilization and Performance Management—The Risk Analysis Capability relies on the Utilization and Performance Management Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.



CGS Risk Analysis Capability



Version 1.1.1

- Understand Mission Flows—The Risk Analysis Capability relies on the Understand Mission Flows Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Understand Data Flows—The Risk Analysis Capability relies on the Understand Data Flows Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Hardware Device Inventory—The Risk Analysis Capability relies on the Hardware Device Inventory Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Software Inventory—The Risk Analysis Capability relies on the Software Inventory Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Understand the Physical Environment—The Risk Analysis Capability relies on the Understand the Physical Environment Capability to provide information about the Enterprise, which is used to assess the mission impacts of threat and vulnerability pairs.
- Network Security Evaluations—The Risk Analysis Capability relies on the Network Security Evaluations Capability for information to supplement the information received from the Risk Identification Capability, when necessary.
- Vulnerability Assessment—The Risk Analysis Capability relies on the Vulnerability Assessment Capability for information to supplement the information received from the Risk Identification Capability, when necessary.
- Threat Assessment—The Risk Analysis Capability relies on the Threat Assessment Capability for information to supplement the information received from the Risk Identification Capability, when necessary.
- Risk Identification—The Risk Analysis Capability relies on the Risk Identification Capability to identify threat and vulnerability pairs.

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 Risk 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 Risk 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.



CGS Risk Analysis Capability



Version 1.1.1

- IA Awareness–The Risk Analysis Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Risk 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 Risk 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.

- Incident Response–The Risk Analysis Capability relies on the Incident Response Capability for information used for situational awareness.
- Incident Analysis–The Risk Analysis Capability relies on the Incident Analysis Capability for information used for situational awareness.

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>	
CA-2 SECURITY ASSESSMENTS	Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: Security controls and control enhancements under assessment; Assessment procedures to be used to determine security control effectiveness; and Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system



CGS Risk Analysis Capability



Version 1.1.1

	<p>[Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;</p> <p>c. Produces a security assessment report that documents the results of the assessment; and</p> <p>d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.</p> <p>Enhancement/s:</p> <p>(1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.</p>
<p>CA-6 SECURITY AUTHORIZATION</p>	<p>Control: The organization:</p> <p>a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;</p> <p>b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and</p> <p>Enhancement/s: None Specified</p>
<p>RA-2 SECURITY CATEGORIZATION</p>	<p>Control: The organization:</p> <p>a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;</p> <p>b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and</p> <p>c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.</p> <p>Enhancement/s: None Specified.</p>
<p>RA-3 RISK ASSESSMENT</p>	<p>Control: The organization:</p> <p>a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;</p> <p>b. Documents risk assessment results in [Selection: security</p>



CGS Risk Analysis Capability



Version 1.1.1

	<p>plan; risk assessment report; [Assignment: organization-defined document]];</p> <p>Enhancement/s: None Specified</p>
<p>PM-10 SECURITY AUTHORIZATION PROCESS</p>	<p>Control: The organization:</p> <p>a. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and</p> <p>b. Fully integrates the security authorization processes into an organization-wide risk management program.</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.

Risk Analysis Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503, IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified	Summary: This directive establishes Intelligence Community (IC) policy for information technology (IT) systems security risk management certification and accreditation (C&A). It directs the use of standards for IT risk management established, published, issued, and promulgated by the IC Chief Information Officer (CIO), which may include standards, policies, and guidelines approved by the National Institute of Standards and Technology (NIST) and/or the Committee on National Security Systems (CNSS). Risk Analysis is an important element of the risk management process.
ICD 801, Acquisition, 16 August 2009, Unclassified	Summary: National Intelligence Program (NIP) major system acquisitions (MSA) shall be undertaken using a balanced and proactive risk management approach to create innovative and responsive systems for use by the IC. Proactive risk management is the acceptance of appropriate risk to allow the necessary innovation and technology insertion in an acquisition, while ensuring, through positive means, that the uncertainties of the



CGS Risk Analysis Capability



Version 1.1.1

	<p>acquisition are managed within a tolerable range to enable cost, schedule, and performance constraints to be met. Risk Analysis is an important element of a proactive risk management approach.</p>
<p>ODNI/CIO-2008-108, Committee on National Security Systems (CNSS) Agreement to Use National Institutes of Standards and Technology (NIST) Documents as Basis for Information Security Controls and Risk Management, 20 April 2009, Unclassified</p>	<p>Summary: This documented CNSS intent for federal agencies, IC, and Department of Defense (DoD) to use the same set of standards, controls, and procedures to secure government information systems; and Committee consensus to assist NIST in incorporating National Security System (NSS) requirements within NIST policies and instructions that define information security controls to protect systems and information (NIST Special Publication [SP] 800-53 v3), as well as the NIST instructions for assessing systems (SP 800-37) and performing risk management (SP 800-30 and SP 800-39). Risk Analysis is an important phase in performing risk management.</p>
<p>Comprehensive National Cybersecurity Initiative (CNCI)</p>	
<p>NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>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.</p>
<p>Department of Defense (DoD)</p>	
<p>DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Classified</p>	<p>Summary: This directive establishes Computer Network Defense (CND) policy, definition, and responsibilities for CND within the DoD, including the implementation of robust infrastructure and information assurance (IA) practices, such as regular and proactive vulnerability analysis and assessment, including active penetration testing and Red Teaming, and implementation of identified improvements; and adherence to a defense-in-depth strategy using risk management principles to defend against both external and internal threats ... Risk Analysis is an important element of the risk management process.</p>
<p>CJCSI 6510.01E,</p>	<p>Summary: This instruction provides joint policy and</p>



CGS Risk Analysis Capability



Version 1.1.1

<p>Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified</p>	<p>guidance for IA and CND operations. Policy includes the following: a. The risk management process will consider the Mission Assurance Category (MAC) of the system, the classification or sensitivity of information handled (i.e., processed, stored, displayed, or transmitted) by the system, potential threats, documented vulnerabilities, protection measures, and need-to-know. ... c. Risk management will be conducted and integrated in the lifecycle for information systems. There must be a specific schedule for periodically assessing and mitigating mission risks caused by major changes to the IT system and processing environment due to changes resulting from policies and new technologies. Risk Analysis is an important element in conducting risk management.</p>
<p>Risk Management Guide for DoD Acquisition, version 2.0, June 2003, Unclassified</p>	<p>Summary: This document provides acquisition professionals and program management offices with a practical reference for dealing with system acquisition risks. It discusses risk and risk management, examines risk management concepts relative to the DoD acquisition process, discusses the implementation of a risk management program from the program management office perspective, and describes a number of techniques that address the aspects (phases) of risk management, i.e., planning, assessment [analysis], handling, and monitoring.</p>
<p>Committee for National Security Systems (CNSS)</p>	
<p>CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, February 2009, Unclassified</p>	<p>Summary: This document establishes the requirements for Enterprise IA risk management within the national security community, which requires a holistic view of the IA risks to NSS operating within the Enterprise using disciplined processes, methods, and tools. It provides a framework for decision-makers to continuously evaluate and prioritize IA risks to accept or recommend strategies to remediate or mitigate those risks to an acceptable level. Risk Analysis is an important element of the risk management framework.</p>
<p>Other Federal (OMB, NIST, ...)</p>	
<p>Nothing found</p>	



CGS Risk Analysis Capability



Version 1.1.1

Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Risk 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	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002, Unclassified	Summary: This SP provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. Risk Analysis is an important element of an effective risk management program.
NIST SP 800-37 Rev-1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010,	This publication transforms the traditional C&A process into the six-step Risk Management Framework (RMF). It provides guidelines for applying the RMF to federal information systems including conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.



CGS Risk Analysis Capability



Version 1.1.1

Unclassified	
NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, Unclassified	Summary: This SP provides guidelines for managing risk to organizational operations, organizational assets, individuals, other Organizations, and the nation resulting from the operation and use of information systems. It implements an RMF, a structured, yet flexible approach for managing that portion of risk resulting from the incorporation of information systems into the mission and business processes of Organizations. Risk Analysis is an important element of an RMF.
NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume 1, Rev 1, August 2008, Unclassified	Summary: This SP provides basic guidelines for mapping types of information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation) and types of information systems (e.g., mission critical, mission support, administrative) to categories of potential security impact. Security categories are used in conjunction with vulnerability and threat information in assessing the risk (i.e., Risk Analysis) to an Organization.
FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, Unclassified	Summary: This document provides standards for categorizing information and information systems. Security categories are based on the potential impact on an Organization should certain events occur that jeopardize the information and information systems needed by the Organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are used in conjunction with vulnerability and threat information in assessing the risk (i.e., Risk Analysis) to an Organization.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	



CGS Risk Analysis Capability



Version 1.1.1

--	--

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. Research component—Risk Analysis requires a certain amount of research to properly analyze Enterprise risks.
2. Life-cycle maintenance—There needs to be data management and collection capabilities. Risk models need to be maintained and revised as necessary.

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 Risk Analysis Capability.

- The Enterprise shall collect and analyze risk-related data for the broader purpose of providing decision-makers information on the benefits, costs, and uncertainty of alternative courses of action with respect to executing the assigned mission in multiple environments.
- The Enterprise shall establish a role or Organization that is responsible for conducting risk analysis in a centralized manner.



CGS Risk Analysis Capability



Version 1.1.1

- Risks shall be reassessed regularly to facilitate awareness and areas such as compliance or design trade-off decisions
- The method of risk assessment used shall be dependent on the type of decision that needs to be made.
- The Enterprise shall conduct foundation research and incident analysis to collect background information on all risks prior to conducting a risk analysis.
- The Enterprise shall conduct independent analyses that provide additional meanings and insights into identified risks including vulnerabilities of a system, threats to a system, or operational impact to a mission, including loss of information or capability.
- The Enterprise shall use separate area-specific analyses to conduct a synthesized focus analysis that combines and relates elements of the specialty-area analyses to address and answer specific issues necessary for making effective risk management decisions.
- The Enterprise shall perform analysis such that individual vulnerabilities are grouped into mission attack scenarios and compared based on their objective, impact, cost, risk to adversary, and the likelihood of the attack being successful.
- The Enterprise shall analyze mission attack scenarios from the perspective of various adversaries to determine which set of attacks is more likely to be used during a conflict.
- The Enterprise shall analyze mission attack scenarios to identify the ultimate operational impact.