



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS Risk Identification Capability

Version 1.1.1

Risk Identification is the creation of a relationship between the results of the Threat Assessment and Vulnerability Assessment Capabilities. It establishes the influence that the threats and vulnerabilities are perceived to have on the Enterprise's risk. The risk-related data comprises known threats and vulnerabilities and their combined impact. The impact portion of the relationship is determined in the Risk Analysis Capability.

07/30/2012



CGS Risk Identification 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	4
5	Capability Post-Conditions.....	5
6	Organizational Implementation Considerations	5
7	Capability Interrelationships.....	6
7.1	Required Interrelationships	6
7.2	Core Interrelationships	7
7.3	Supporting Interrelationships.....	8
8	Security Controls	8
9	Directives, Policies, and Standards	8
10	Cost Considerations	13
11	Guidance Statements.....	13



CGS Risk Identification 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 Identification 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.

Risk Identification is the creation of a relationship between the results of the Threat Assessment and Vulnerability Assessment Capabilities. It establishes the influence that the threats and vulnerabilities are perceived to have on the Enterprise's risk.

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 relationships between Risk, Threat, Vulnerability, and Impact is $R = f(T, V, I)$ as represented by a portfolio of attacks. The impact portion of the relationship is determined in the Risk Analysis 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.

Notionally, Risk Identification requires threat and vulnerability information. The Capability relies on obtaining the threat and vulnerability information for Enterprise assets and establishes a risk relationship between the threat and vulnerability pairs. The relationship decisions shall be determined by stakeholders and divisions across the Enterprise to ensure involvement of the right people who understand how the threat/vulnerability information is associated.

Risk may be identified at different levels of abstraction (tier-like) within the Enterprise and is of different types. For example, the Organization may identify risks at the department, enclave, or Enterprise-wide levels, and the risks may be associated with people, operations, technology, or environment. Because risks are not independent from other risks, the presence of one risk may generate another instance or an entirely new risk for an Enterprise asset. Risks can be "inherited" across a lower level in the Enterprise, which will aggregate to upper levels. This is also the case when looking at systems having



CGS Risk Identification Capability



Version 1.1.1

multiple owners or crossing different domains. It is important to identify and address shared and inherited risks. Mechanisms are employed to ensure that risks identified at each level and of each type are communicated horizontally and vertically. This provides the overall risk picture for identified risks and is necessary to depict shared and inherited risk. In addition, the Risk Identification Capability shall identify scenarios that may impose future risks, and these risks shall be considered in the Risk Identification process.

All Risk Identification information (threat/vulnerability pair and relationship) shall be maintained and be made available for reuse within a risk repository that is maintained as a part of this Capability. In addition to the risk information, the Organization/official function or role that identified the risk shall be documented. Documentation of the risk identifier facilitates reuse and reconsideration/reanalysis when information changes (e.g., new attacks, vulnerabilities, mitigations, missions). Attribution does not imply ownership; rather, it serves as a way to converse with a risk stakeholder. Across stakeholders, this could possibly be used to gauge which stakeholders are best suited for analyzing particular information.

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. Threats and vulnerabilities have already been accurately identified.
2. Threat and vulnerability assessment results are available for use by the Risk Identification Capability.
3. Risk Identification Teams have sufficient access to resources to identify all risks (as a result of known threats/vulnerabilities) and have direct knowledge/expertise to correctly establish the risk relationships.
4. All stakeholders of an asset participate in its Risk Identification.
5. The Enterprise understands the relationship between its various assets and their mission needs and data flows.



CGS Risk Identification Capability



Version 1.1.1

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 Organization identifies perceived risk associated with all Enterprise assets (associated with people, operations, technology, and environment).
2. The Organization may not be able to identify all risk.
3. The risk and risk information are not static and will be routinely considered as the threats, vulnerabilities, and policies change within the Enterprise.
4. The Capability maintains a risk repository that stores information on threat/vulnerability pairs and their relationship....

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).

The Organization will use the threat and vulnerability information provided by the Threat and Vulnerability Assessment Capabilities. In addition, the Organization will employ objective and scenario-based methods to help determine the risk relationship between threat and vulnerability pairs. The Organization will examine a defined threat exploiting a particular vulnerability in the context of a particular scenario or context of an objective, environment, or other impact factors (i.e., mission flows or data flows) to determine the nature of the risk relationship. This will help to define whether the relationship is truly a risk. This information will then be communicated to the Risk Analysis Capability to determine the likelihood and impact factors. This will provide analysis information to stakeholders to make the risk decision.

The Organization will use subject matter expert (SME) resources from across the Enterprise to establish the risk relationships. The SMEs will be used to ensure that the appropriate risk relationship is generated (or reused from previously identified risks). For example, physical security experts will be used to identify environmental-related risks, and network operations personnel will be used to identify technology-related risks.



CGS Risk Identification Capability



Version 1.1.1

The Organization may employ Risk Identification tools to help automate the risk relationship decision. These tools may be specific to a threat/vulnerability type or environment but all Risk Identification tools employed will be interoperable with an overarching tool or toolkit that helps to identify all perceived risk with the Organization at multiple levels (tiers) and of different risk types. The tools employed for specific risks types will be vetted by the SMEs for that specific type of risks. Any specific requirements for the tool will also be identified by the risk SME.

The Organization will use industry-established “risk lists” in addition to the risks uniquely identified in the Organization. The industry lists can be checked for application to a particular situation. The Organization will determine the validity of the risk lists and use only those that are from valid and approved sources. This may also be determined by an overarching organizational authority outside of the Organization itself. The Organization will also maintain risk libraries for internal use that can be shared with other members of the Community. These risk libraries may be used to store information on uniquely identified or classified risks.

The Organization will not limit itself to preexisting lists and will perpetually allocate a reasonable level of resources to identify previously unidentified risks. In addition, stakeholders will be trained, and a documentation/communication system will exist to identify, prompt stakeholder discussion, and generate appropriate responses to events that modify Risk Identification decisions.

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 Identification Capability relies on the Network Mapping Capability to provide information about the status of the Enterprise.
- Network Boundary and Interfaces—The Risk Identification Capability relies on the Network Boundary and Interfaces Capability to provide information about the status of the Enterprise.



CGS Risk Identification Capability



Version 1.1.1

- Utilization and Performance Management—The Risk Identification Capability relies on the Utilization and Performance Management Capability to provide information about the status of the Enterprise.
- Understand Mission Flows—The Risk Identification Capability relies on the Understand Mission Flows Capability to provide information about the status of the Enterprise.
- Understand Data Flows—The Risk Identification Capability relies on the Understand Data Flows Capability to provide information about the status of the Enterprise.
- Hardware Device Inventory—The Risk Identification Capability relies on the Hardware Device Inventory Capability to provide information about the status of the Enterprise.
- Software Inventory—The Risk Identification Capability relies on the Software Inventory Capability to provide information about the status of the Enterprise.
- Understand the Physical Environment—The Risk Identification Capability relies on the Understand the Physical Environment Capability to provide information about the status of the Enterprise.
- Vulnerability Assessment—The Risk Identification Capability relies on the Vulnerability Assessment Capability to provide information about Enterprise vulnerabilities.
- Threat Assessment—The Risk Identification Capability relies on the Threat Assessment Capability to provide information about Enterprise threats.

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 Identification 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 Identification 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 Risk Identification Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Risk Identification Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.



CGS Risk Identification Capability



Version 1.1.1

- Organizations and Authorities–The Risk Identification 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.

- Network Security Evaluations–The Risk Identification Capability relies on the Network Security Evaluations Capability to provide information about Enterprise vulnerabilities.

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>	
PM-7 ENTERPRISE ARCHITECTURE	Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Enhancements: None Specified

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 Identification Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503, IC Information Technology Systems Security Risk	Summary: This directive establishes Intelligence Community (IC) policy for information technology (IT) systems security risk management certification and accreditation (C&A). It



CGS Risk Identification Capability



Version 1.1.1

<p>Management, Certification and Accreditation, 15 September 2008, Unclassified</p>	<p>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 Identification is an important element of the risk management process.</p>
<p>ICD 801, Acquisition, 16 August 2009, Unclassified</p>	<p>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 acquisition are managed within a tolerable range to enable cost, schedule, and performance constraints to be met. Risk Identification 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 Institute 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 Identification 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</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.</p>



CGS Risk Identification Capability



Version 1.1.1

Initiative [CNCI]), 8 January 2008, Classified	Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001, Classified	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 external and internal threats ... Risk Identification is an important element of the risk management process.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction provides joint policy and 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 Identification is an important element in conducting risk management.
Risk Management Guide for DoD Acquisition, version 2.0, June 2003, Unclassified	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



CGS Risk Identification Capability



Version 1.1.1

	risk management, i.e., planning, assessment, handling, and monitoring. Risk Identification is an important element of a risk management program.
Committee for National Security Systems (CNSS)	
CNSSP-22, Information Assurance Risk Management Policy for National Security Systems, February 2009, Unclassified	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 Identification is an important element of the risk management framework (RMF).
Other Federal (OMB, NIST, ...)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Risk Identification 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 Risk Identification Capability



Version 1.1.1

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 special publication (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 Identification 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, Unclassified	This publication transforms the traditional C&A process into the six-step 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.
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 Identification is an important element of a RMF.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	



CGS Risk Identification Capability



Version 1.1.1

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. Solution used for implementation—The Enterprise will need to provide for the development and/or acquisition of risk identification tools.
2. Identification of differences—Different types of risks being identified may require various solutions to perform comprehensive Risk Identification.
3. Storage requirements—This Capability uses a risk repository to store information about risks that have been identified.

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 Identification Capability.

- The Enterprise shall identify risks that the threats and vulnerabilities are perceived to cause to the Enterprise.
- The Enterprise shall obtain threat and vulnerability information from appropriate Enterprise monitoring systems.



CGS Risk Identification Capability



Version 1.1.1

- The Enterprise shall establish risk relationships between threat and vulnerability pairs that are determined by stakeholders and divisions across the Enterprise.
- The Enterprise shall identify risks that are shared or inherited as a result of relationships with other Enterprises.
- The Enterprise shall employ mechanisms to ensure that risks identified at each level of the Organization and of each type are communicated horizontally and vertically.
- The Enterprise shall identify scenarios that may impose future risks.
- Risk identification information shall be maintained and made available for reuse within a risk repository
- All identified risks shall be documented in accordance with Organizational policy to facilitate reuse and reconsideration/reanalysis when information changes (e.g., new attacks, vulnerabilities, mitigations, missions).