



National Security Agency/Central Security Service



# INFORMATION ASSURANCE DIRECTORATE

## CGS Risk Mitigation Capability

Version 1.1.1

Risk Mitigation is the reduction of the likelihood and/or impact of Enterprise security risk. The Risk Mitigation Capability decides which mitigations will be applied to identified risks, implements those mitigations, and subsequently reduces the risk level.



# CGS Risk Mitigation 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.....	7
6	Organizational Implementation Considerations .....	7
7	Capability Interrelationships.....	9
7.1	Required Interrelationships .....	9
7.2	Core Interrelationships .....	10
7.3	Supporting Interrelationships.....	10
8	Security Controls .....	11
9	Directives, Policies, and Standards .....	12
10	Cost Considerations .....	17
11	Guidance Statements.....	17



# CGS Risk Mitigation 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 Mitigation 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 Mitigation is the reduction of the likelihood and/or impact of Enterprise security risk. The Risk Mitigation Capability decides which mitigations will be applied to identified risks, implements those mitigations, and subsequently reduces the risk level.

## 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.

The Risk Mitigation Capability reduces the overall security risk to the Enterprise. The responsibilities of this Capability include identifying possible mitigations, determining which of those mitigations are the most appropriate to implement, and implementing the mitigations. Implementation shall require coordination with other Capabilities that are responsible for individual countermeasures. For example, System Protection and Communication Protection are responsible for implementing mitigations having to do with safeguarding systems and communication channels, respectively.

The level of risk introduced by a given vulnerability is a product of the probability that the vulnerability will be exploited and the impact that its exploitation will have on the mission. Therefore, there are generally two ways to reduce the level of risk presented by a vulnerability, either decrease the probability that it will be exploited or reduce the impact that the exploitation would cause. The Risk Mitigation Capability shall do one or both of these to reduce the level of risk to one that meets the Enterprise’s standards for being acceptable as established in the risk posture (see the Risk Analysis Capability). Mitigations are applied to reduce risk. It is not possible to completely eliminate risk.

Risk Mitigation considers any events that disrupt the mission. Events can be of a technical, physical, personnel, and/or environmental nature. A number of different types of mitigations can be used to reduce the risk associated with these events, which



# CGS Risk Mitigation Capability



Version 1.1.1

include technology (hardware and software), training, policy, doctrine, and procedure. Some examples of mitigations could include system hardening, hunting and prosecuting attackers, increasing or improving training, changing usage policies, and increasing or improving accountability and oversight measures.

Risk Mitigation shall employ a group of decision-makers who together choose the appropriate course of action for mitigating Enterprise risk. This group of decision-makers shall be made up of management, operations, information technology (IT), and information assurance (IA) personnel, and the group shall have the appropriate authority to make decisions regarding Risk Mitigation. In addition, decision-making groups shall also include or solicit input from individuals who are subject matter experts on various topics related to the risks or mitigations that are under consideration.

Risk Mitigations may be an individual countermeasure, or they may be a set of countermeasures that are implemented together. Mitigations can be used to reduce a single risk or multiple risks. Decision-makers shall enumerate and prioritize the decision criteria they will use to compare each mitigation alternative. Decision criteria shall include factors such as mission impact, security, performance, cost, and interoperability. The decision-makers shall choose the mitigation option that optimally balances the factors they deem the most critical, such as mission and cost.

Decision-makers may have unique preferences that affect their attitudes toward different mitigation options. Decision-making groups shall be composed of multiple individuals from a variety of functional roles to prevent these preferences from becoming detrimental. The mitigation option decided on shall be one that optimally balances the established decision criteria. If there are multiple options that all balance these factors equally well, it is acceptable for the decision-makers to choose one option over another for preferential reasons. Decision-makers shall make their decision criteria known so that the options they consider when they collect information about potential countermeasures will be as useful to them as possible.

The Risk Mitigation Capability shall consider input from other members of the Community if risks span more than a single Enterprise. These risks can originate from within the Organization (owned risks), or they can be caused by another Organization (inherited risks). When this happens, each Organization affected by a risk shall have a say in how it is mitigated. Effective mitigation may require action from multiple Organizations. When there are disagreements about the optimal course of action, the decision shall be deferred to the Organization with the highest authority. This



# CGS Risk Mitigation Capability



Version 1.1.1

authoritative Organization shall make a decision based on mission impacts, mission importance, and risk severity.

The Risk Mitigation Capability shall include a function that provides testing/vetting for all countermeasure options prior to the finalization of the mitigation decisions. This testing/vetting process provides the decision-makers with a level of confidence that the countermeasure or combination of countermeasures will perform as intended and not create any additional vulnerabilities. The decision-makers determine the necessary level of confidence and the types of data needed for an option to be considered. Testing and vetting may not be necessary for all mitigation scenarios, depending on factors such as mission impact, cost, and time constraints as well as the type of mitigation.

The decision-makers shall develop a Risk Mitigation plan that specifies all of the details for implementing the mitigation countermeasures (e.g., technology, policy, timeline, resources, assigned roles) and describes the logic that led to the adoption of the specific solution selected (decision criteria, mitigation options considered, testing, and confidence levels). This thorough documentation ensures that the implementation process receives the necessary planning, provides justification for a decision, aids in process improvement efforts, and allows future Risk Mitigation decision-makers to reuse or gather knowledge from previous decisions. Risk Mitigation plans shall be centrally stored and accessible and follow an Enterprise standardized format, which aids in reuse. Other specific details on the types of content to include in mitigation plans shall be dictated by the Enterprise.

Users in austere environments, defined by intermittent connectivity and limited bandwidth, may require special accommodations to maintain operational capabilities when the infrastructure services (e.g., vulnerability scanning, patch updates) are not accessible for periods of time. The Risk Mitigation Capability shall work with the teams who provide infrastructure services to establish mitigations that will ameliorate the risks caused by this intermittent connectivity.

The Risk Mitigation plans shall include a Plan of Action and Milestones (POA&M) to document actions taken to apply the mitigations or other implementation information. The maintenance of the POA&M shall be the responsibility of the Program Managers or Program Management Office (PMO). The Risk Mitigation Capability shall employ services from a Program Manager or PMO to ensure that all activities and resources are managed according to the program management plan and are able to track and implement the mitigations assigned.



# CGS Risk Mitigation Capability

Version 1.1.1



The Risk Mitigation Capability has a function that provides solutions to potential risk scenarios that are created by Risk Identification. Risk Identification produces these scenarios by providing a future outlook on how the risk environment could change. These scenarios are analyzed using the same process as actual risks. By determining mitigation actions ahead of time, if these scenarios occur, they can be mitigated faster because the options have already been considered.

The Risk Mitigation Capability receives input from the Risk Identification and Risk Analysis Capabilities detailing the risks facing the Enterprise and their impacts, respectively. As necessary, information shall flow back and forth between Risk Mitigation and these other risk Capabilities to fully enumerate risks and potential mitigation options so that Risk Mitigation decision-makers can make the optimal decision.

The Risk Mitigation Capability provides output that is used by the Risk Monitoring Capability to measure the effectiveness of the mitigations that are implemented. Output, in the form of reports, shall be provided to Enterprise stakeholders to keep them informed of the activities performed by this Capability.

The Risk Mitigation Capability shall work in conjunction with the Incident Analysis Capability after the Enterprise has suffered an IA incident. Together, these Capabilities shall determine appropriate responses to eliminate the vulnerabilities that caused the incident and restore the Enterprise and its resources to pre-incident operational status.

## 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. Risk analysis results are accurate and available.
2. Risk analysis provides the impact analysis and likelihood of a risk.
3. The Enterprise's accepted risk posture has been defined and documented.
4. Mission assets have been prioritized, and the business need has been defined and documented.
5. All programs have an established program management role or office to manage a POA&M.



# CGS Risk Mitigation 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 Capability considers constraints for the mitigations, such as cost, time, and resources, when determining risk reduction.
2. The Capability considers feasibility when deciding which Risk Mitigation(s) to apply.
3. Risk Mitigation teams have sufficient authority and system access to make decisions and implement mitigations.

## 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 uses Risk Mitigation to reduce risk. It does this by decreasing the probability that a threat will exploit a vulnerability and/or by reducing the mission impact if it is exploited. Addressing all identified risks may not be practical; therefore, the Organization will give priority to the threat and vulnerability pairs that have the potential to cause the most significant mission impact or harm. Because each Organization's environment and mission objectives are different, when it comes to safeguarding an Organization's mission and resources, the options used to mitigate risks and the methods used to implement mitigations will vary.

To make Risk Mitigation decisions, the Organization will use information from Risk Identification to understand the vulnerabilities, from Risk Analysis to determine the impact for each risk, and from subject matter experts to understand potential countermeasures. The Organization will assign the task of evaluating mitigation options to groups of decision-makers. These groups will be composed of personnel from various roles, including management, IA, operations, and technology. The decision-makers will use all of the collected information to determine which mitigation(s) to implement.



# CGS Risk Mitigation Capability



Version 1.1.1

The Organization will assess each mitigation option. Each option can be composed of one or more countermeasures and can be used to mitigate one or more risks. The assessment process, as set by Organization policy, will weigh each option based on a set of prioritized decision criteria that are determined by the group of decision-makers responsible for overseeing mitigation decision. The Organization will implement the mitigation option that finds the optimal balance of the factors making up the decision criteria.

The Organization will develop an implementation plan that will be used throughout the course of the mitigation. Included in this plan will be all of the relevant acquisition needs, their costs, and the expected mission impact. The plan will define a timeline for completion with milestones along the way. In addition, the plan will specify the roles for everyone involved in the mitigation, the function of each role, and the individual assigned to each role.

The Organization will establish a testing process for assessing the viability of mitigation options prior to their implementation. Not all mitigations are tested or are able to be tested. The Organization will determine which mitigations to test based on the severity of the risk, mission impact, time constraints, cost, and the complexity of the mitigation. For example, an inexpensive policy-based mitigation that reduces a risk that presents a small mission impact may not need to go through rigorous testing.

The Organization will use potential risk scenarios provided by Risk Identification to proactively plan for changing Enterprise risk. These risk scenarios represent changes to the environment and/or threats that could arise over time. Based on these scenarios, the Organization will go through the Risk Mitigation process to develop predetermined mitigation plans. These mitigation plans will be developed and documented like any other mitigation plan. If one of the potential risk scenarios materializes, the Organization will mitigate it according to the same process used for other risks. The only difference will be that it will have already selected an optimal mitigation option that can be implemented without having to weigh the various options first.

The Organization may face risks that also affect other members of the Community. The Organization will work with other Organizations to mitigate these risks in a mutually beneficial way. Other members of the Community may have differing mission needs that conflict with those of the Organization. In these circumstances, the Organization will defer to an Organization with a higher authority to make a decision. The Organization



# CGS Risk Mitigation Capability



Version 1.1.1

will establish an Enterprise group to provide oversight and ensure compliance with mitigation actions.

The Organization will establish standards governing documentation for Risk Mitigation. This documentation will include information about what risks were being mitigated, what their mission impact was, which mitigation options were considered, which mitigation option was selected, the logical process the decision-makers used to find the solution, and who was responsible for implementing each countermeasure. All documentation will comply with an Organization or Community standardized format and be stored in a centrally managed repository.

To keep relevant stakeholders informed, the Organization will provide them with reports on the status of Risk Mitigation activities. The contents of the reports will be tailored to the needs of the recipient. The frequency by which reports are distributed will be determined by mission need.

## 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.

- Configuration Management—The Risk Mitigation Capability relies on the Configuration Management Capability for information used to determine which configurable items need to be monitored, as well as which have been successfully mitigated.
- Architecture Reviews—The Risk Mitigation Capability relies on the Architecture Reviews Capability to provide information about systems where security requirements are unmet.
- Risk Identification—The Risk Mitigation Capability relies on the Risk Identification Capability to provide information about Enterprise risks.
- Risk Analysis—The Risk Mitigation Capability relies on the Risk Analysis Capability to provide information about the mission impact of Enterprise risks.



# CGS Risk Mitigation Capability



Version 1.1.1

- Risk Monitoring—The Risk Mitigation Capability relies on the Risk Monitoring Capability to monitor the effectiveness of mitigations implemented.

## 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 Mitigation 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 Mitigation 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 Mitigation Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training—The Risk Mitigation 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 Mitigation 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 Mapping—The Risk Mitigation Capability relies on the Network Mapping Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Network Boundary and Interfaces—The Risk Mitigation Capability relies on the Network Boundary and Interfaces Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Utilization and Performance Management—The Risk Mitigation Capability relies on the Utilization and Performance Management Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.



# CGS Risk Mitigation Capability



Version 1.1.1

- Understand Mission Flows—The Risk Mitigation Capability relies on the Understand Mission Flows Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Understand Data Flows—The Risk Mitigation Capability relies on the Understand Data Flows Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Hardware Device Inventory—The Risk Mitigation Capability relies on the Hardware Device Inventory Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Software Inventory—The Risk Mitigation Capability relies on the Software Inventory Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Understand the Physical Environment—The Risk Mitigation Capability relies on the Understand the Physical Environment Capability to provide information on the status of the Enterprise, which is used to determine appropriate mitigations.
- Network Security Evaluations—The Risk Mitigation Capability relies on the Network Security Evaluations Capability to provide information that is used to make recommendations regarding how to mitigate the risks associated with 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>	
CA-5 PLAN OF ACTION AND MILESTONES	Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and



# CGS Risk Mitigation Capability



Version 1.1.1

	<p>continuous monitoring activities.</p> <p>Enhancement/s:</p> <p>(1) The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.</p>
CM-4 SECURITY IMPACT ANALYSIS	<p>Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.</p> <p>(NOTE: This analysis is based on the existing threats and vulnerabilities which could pose a risk to the organization.)</p> <p>Enhancement/s: None Applicable</p>
IA-5 AUTHENTICATOR MANAGEMENT	<p>Enhancement/s:</p> <p>(8) The organization takes [Assignment: organization-defined measures] to manage the risk of compromise due to individuals having accounts on multiple information systems.</p>
PM-4 PLAN OF ACTION AND MILESTONE PROCESS	<p>Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.</p> <p>Enhancement/s: None Specified</p>
RA-3 RISK ASSESSMENT	<p>Control: The organization:</p> <p>c. Reviews risk assessment results [Assignment: organization-defined frequency];</p> <p>Enhancement/s: None Specified</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 Mitigation Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503, IC Information	Summary: This directive establishes Intelligence



# CGS Risk Mitigation Capability



Version 1.1.1

<p>Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified</p>	<p>Community (IC) policy for information technology (IT) systems security risk management and certification and accreditation (C&amp;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 Monitoring 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 Monitoring 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 Systems (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 Monitoring is an important phase in performing risk management.</p>
<p>Comprehensive National Cybersecurity Initiative (CNCI)</p>	
<p>NSPD-54/HSPD-23 Cybersecurity Presidential</p>	<p>Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-</p>



# CGS Risk Mitigation Capability



Version 1.1.1

<p>Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified</p>	<p>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 Mitigation is an important element of the risk management process.</p>
<p>CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified</p>	<p>Summary: This instruction provides joint policy and guidance for IA and CND operations. Policy includes: 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 life cycle 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 Mitigation 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</p>



# CGS Risk Mitigation Capability



Version 1.1.1

	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, handling, and monitoring.
<b>Committee for National Security Systems (CNSS)</b>	
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 Monitoring is an important element of the risk management framework (RMF).
<b>Other Federal (OMB, NIST, ...)</b>	
OMB M-02-01, Memorandum for Heads of Executive Departments and Agencies, 17 October 2001, Unclassified	Summary: This memo provides specific instructions that describe and provide a standard format for writing Plans of Actions and Milestones (POA&Ms). Examples are also provided to assist when preparing for the POA&Ms.
OMB M-10-15, Memorandum for Heads of Executive Departments and Agencies, 21 April 2010, Unclassified	Summary: Agencies need to have an enterprise-wide system to continuously monitor security-related information in a way that is both manageable and actionable. Agency stakeholders need to have relevant security information delivered in a timely manner. Agencies must develop automated risk models for monitoring threats and vulnerabilities.
<b>Executive Branch (EO, PD, NSD, HSPD, ...)</b>	
Nothing found	
<b>Legislative</b>	
Nothing found	



# CGS Risk Mitigation Capability



Version 1.1.1

## Risk Mitigation 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 Mitigation 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. 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



# CGS Risk Mitigation Capability



Version 1.1.1

	business processes of an Organization. Risk Mitigation is an important element of an RMF.
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. Solution used for implementation—Risk Mitigation requires the use of tools and cooperation with other Capabilities to be effective.
2. Manpower to implement, maintain, and execute—Personnel are required to generate cost-benefit data. Use of an internal versus external team will affect costs, motivations, and response time.



# CGS Risk Mitigation Capability



Version 1.1.1

## 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 Mitigation Capability.

- The Enterprise shall reduce the overall security risk by identifying possible mitigations, determining which of those mitigations are the most appropriate to implement, and implementing the mitigations.
- Risk Mitigation shall consider any events that disrupt the mission. This includes events that are of a technical, physical, personnel, and/or environmental nature.
- A number of different types of mitigations shall be used to reduce the risk associated with these events, including technology (hardware and software), training, policy, doctrine, and procedure. Some examples of mitigations could include system hardening, hunting and prosecuting attackers, increasing or improving training, changing usage policies, and increasing or improving accountability and oversight measures.
- The Enterprise shall employ a group of authoritative decision-makers who together choose the appropriate course of action for mitigating Enterprise risk. This group of decision-makers shall include multiple individuals from a variety of roles including management, operations, IT, and IA.
- Decision-making groups shall include or solicit input from individuals who are subject matter experts on various topics related to the risks or mitigations that are under consideration
- Decision-makers shall enumerate and prioritize the decision criteria they will use to compare each mitigation alternative. Decision criteria shall include factors such as mission impact, security, performance, cost, and interoperability.
- The risk mitigation system shall consider input from other members of the Community if risks span more than a single Enterprise. These risks can originate from within the Organization (owned risks) or they can be caused by another Organization (inherited risks).
- When mitigation requires action from multiple Organizations and there are disagreements about the optimal course of action, the decision shall be deferred to the Organization with the highest authority.
- Testing shall occur for all countermeasure options prior to the finalization of the mitigation decisions to ensure the countermeasure(s) will perform as intended and not create any additional vulnerabilities.



# CGS Risk Mitigation Capability



Version 1.1.1

- The decision-makers shall determine the necessary level of confidence and the types of data needed for an option to be considered for the testing process.
- Decision-makers shall develop a risk mitigation plan that specifies all of the details for implementing the mitigation countermeasures (e.g., technology, policy, timeline, resources, assigned roles) and describes the logic that led to the adoption of the specific solution selected (decision criteria, mitigation options considered, testing, and confidence levels).
- Risk mitigation plans shall be centrally stored and accessible.
- Risk mitigation plans shall follow an Enterprise standardized format, which aids in reuse.
- The risk mitigation plans shall include a POA&M to document actions taken to apply the mitigations or other implementation information.
- A Program Manager or PMO shall maintain the POA&M to ensure that all activities and resources are managed appropriately and mitigations are tracked and implemented.
- Teams that provide infrastructure services shall help establish mitigations to ameliorate the risks caused by intermittent connectivity and limited bandwidth (e.g., vulnerability scanning, patch updates not accessible for periods of time) to maintain operational capabilities.
- Risk mitigation shall provide solutions for identified risk scenarios.
- Reports shall be provided to Enterprise stakeholders to keep them informed of the effectiveness of risk mitigations that have been implemented.