

Information Assurance  
is a MUST DO.  
It is Everyone's Responsibility!

You are essential to  
reaching the Gold  
Standard of Security.



Visit our unclassified Community Gold Standard Website:  
[www.IAD.gov](http://www.IAD.gov)

Select the CGS link located on the IAD.gov homepage menu

Or contact the CGS Team directly:  
Unclassified Email Alias: [CGS@NSA.gov](mailto:CGS@NSA.gov)

National Security Agency  
Information Assurance Directorate  
9800 Savage Road, Suite 6730  
Fort Meade, MD 20755-6730

# COMMUNITY GOLD STANDARD

FOR INFORMATION ASSURANCE

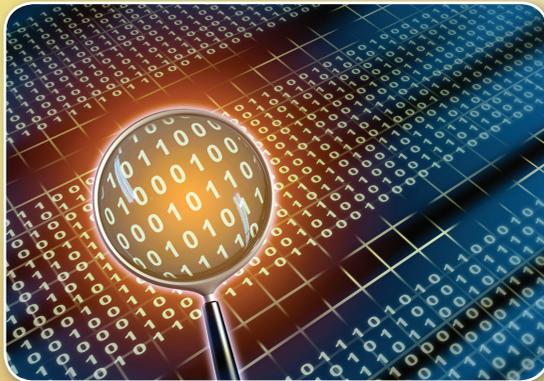


Sponsored by the National Security Agency

## The Community Gold Standard DEFINED

The Community Gold Standard (CGS) is a comprehensive Information Assurance (IA) framework to develop, operate, and maintain an enterprise security plan. The CGS framework is organized into discrete capabilities that can be applied to any enterprise.

CGS defines what it means for capabilities to be considered at “the Gold Standard” level of contribution to the IA mission. The Gold Standard characterizes the highest level of practice for IA Capabilities in accordance with policies and standards, while considering limitations in effect through current technologies and other constraints.



### CGS is...

- **A Capability Framework** – Organizes IA information and activities applicable to any enterprise
- **Inclusive IA Capability Analysis** – Enables a comprehensive understanding of the organization’s mission, operating environment, security posture, and resource management
- **Implementation Agnostic** – Enables organizations to choose their own solutions as part of a full enterprise security plan

## WHY USE the Community Gold Standard?

Now, more than ever, it is critical for organizations to efficiently use their resources to meet the challenges of developing and maintaining secure cyber solutions. The comprehensive nature of CGS helps an organization assess its information assurance environment by addressing people, process, and technology. Assessing these areas within the context of an organization’s mission helps prioritize needed security investments.



### Provides a Holistic View of Information Assurance

Understand and respond to threats, provide a layered defense, and make informed risk decisions from an enterprise perspective.

### Supports Mitigation Development

Enhance your Information Assurance program and provide context for risk mitigation development.

### Enables Effective Risk Management

Increase your organization’s ability to manage risk by building a strong enterprise security plan.

### Transcends Technology

Apply and track mitigations according to IA capabilities rather than dynamic, evolving technologies, to protect against obsolete IA solutions.

## APPLICATION OF the Community Gold Standard

Current uses of CGS content:

- Identifying capability gaps
- Performing portfolio management
- Developing enterprise policies
- Supporting enterprise architecture development
- Supporting acquisition efforts

The application of CGS content into an enterprise security plan gives organizations the ability to:

- **Harden** – Against information compromise
- **Defend** – Mission, resources, and information



CGS provides decision support for a wide variety of organizational needs. For example:

- **IA Mission Planning** – Enables a comprehensive vision of future IA projects and programs
- **Current Security Posture** – Identifies enterprise IA capability gaps
- **Threats and Vulnerabilities** – Clarifies IA capabilities for informed risk assessment and mitigation decisions

CGS content provides users with a common IA lexicon based on the Committee of National Security Systems Instruction (CNSSI) 4009 Glossary and aligns to the latest National Institute of Standards and Technology (NIST) SP 800-53 (Series) Security Controls.