



National Security Agency/Central Support Service



INFORMATION ASSURANCE DIRECTORATE

CGS Utilization and Performance Management Capability

Version 1.1.1

Utilization and Performance Management provides the capability to ensure availability and reliability of resources that directly or indirectly provide support to mission functionality such that they are accessible and usable on demand by an authorized entity.

07/30/2012



CGS Utilization and Performance Management Capability



Version 1.1.1

Table of Contents

- 1 Revisions2
- 2 Capability Definition3
- 3 Capability Gold Standard Guidance.....3
- 4 Environment Pre-Conditions5
- 5 Capability Post-Conditions.....6
- 6 Organizational Implementation Considerations6
- 7 Capability Interrelationships.....9
 - 7.1 Required Interrelationships9
 - 7.2 Core Interrelationships9
 - 7.3 Supporting Interrelationships.....10
- 8 Security Controls10
- 9 Directives, Policies, and Standards11
- 10 Cost Considerations14
- 11 Guidance Statements.....14



CGS Utilization and Performance Management 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 Utilization and Performance Management 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.

Utilization and Performance Management provides the capability to ensure availability and reliability of resources that directly or indirectly provide support to mission functionality such that they are accessible and usable on demand by an authorized entity. Operations must manage the system to target Utilization and Performance levels to ensure availability and reliability of resources. Specifically, Utilization Management is the directed action to control the use or consumption of organizational resources; Performance Management is the directed action to control and facilitate the accomplishment of a given task.

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 Utilization and Performance Management Capability focuses on service delivery. The Enterprise shall define and manage target Utilization and Performance levels. Defining target Utilization and Performance levels includes both network resources and thresholds for triggering corrective action. Networks shall be designed to incorporate target performance levels and be managed at the target levels that shall help to ensure the reliability of resources. The Enterprise shall establish target baselines based on the following schema:

1. Perform modeling and simulation in a test environment
2. Run exercises to measure actual performance in an operational or semi-operational environment
3. Establish baselines from exercise results
4. Reestablish baselines based on mission need and trend analysis as experience is gained through running the network
5. Iteratively revisit the definition of target levels as experience is gained



CGS Utilization and Performance Management Capability



Version 1.1.1

There are specific characteristics for Utilization and Performance, including defining the required threshold and determining appropriate responses when particular Utilization and Performance issues occur. The process for Utilization and Performance Management is as follows:

1. Identify characteristics of resource utilization and network performance
2. Gather data on resource utilization and network performance characteristics
3. Analyze data to articulate a target operational Utilization and Performance level
4. Define Utilization and Performance thresholds that when exceeded shall trigger corrective action (e.g., escalation to incident response, operations support, or other to subject matter expert [SME] for analysis and potential intervention)

The goal of Utilization Management is to systematically monitor and evaluate resource consumption to ensure cost-efficient operations. The Capability shall identify network utilization anomalies and generate useful alerts of the identified anomalies. Utilization and Performance Management are complementary constructs that balance demand for resources (performance) and consumption of those resources (utilization)—e.g., the consumption of the following resources: network bandwidth, power, cooling, space, CPU, RAM, and media storage.

Utilization and Performance Management consists of both reactive and proactive management. Reactive Utilization Management involves responding to real-time resource consumption in operations, while proactive Utilization Management involves network simulation and examination of “what-if” scenarios to plan for resource consumption before that consumption occurs in real-time operations. For Performance Management, reactive is responding to unforeseen difficulties in real-world operations. Proactive Performance Management involves network simulation and the examination of “what-if” scenarios to mitigate operational risks before they occur in real-world operations.

The goal of Performance Management is to systematically monitor and evaluate service delivery to ensure effective and efficient operations (e.g., with respect to network performance management—network throughput, service response times, path utilization, priority, and preemption).

Effective Performance Management requires the measuring and tracking of end-to-end performance, which involves managing for an application as well as managing for a mission. The Utilization and Performance Management Capability ensures that



CGS Utilization and Performance Management Capability



Version 1.1.1

applications shall perform efficiently, that systems shall have sufficient capacity to support them, and that networks that deliver application functionality can meet service level agreements (SLAs). An SLA is a contract between the service provider and the service user to provide a range of support services, up to an agreed minimum standard. The SLA shall define the obligations and expectations that each have with the other, how they shall be monitored, and how deviations shall be rectified.

The Utilization and Performance Management Capability shall support quality of service (QoS) and priority of resources. Traffic engineering shall be performed to provide different priority to different users, applications, or data flows, and to guarantee a minimum level of performance for a data flow. For example, the Enterprise may define critical communications as data needed to keep the network running and as command and control communications, and normal communications as daily communications such as email and instant messaging. Information shall be leveraged from the Know the Enterprise Capability area to help determine priorities, and there is a strong coupling with the Understand Mission Flow Capability to understand mission flows. How an Enterprise determines what shall be a priority is considered a business decision.

The Utilization and Performance Management Capability shall provide reports of network utilization covering several metrics. Thresholds shall be established (percentage and deviations). When exceeded, an alert shall be triggered and prompt intervention. Alerts and notifications shall be sent out when SLAs are not met. Notification alerts shall be sent to local Network Operations for evaluation and to the Incident Response Capability where the incident shall be further evaluated at an Enterprise level. Situational awareness personnel shall perform trend analysis to determine whether the incident involves more than the obvious. In addition, information may need to be shared with peer Organizations to ensure a complete picture for Understand Mission Flow.

The Utilization and Performance Management Capability shall securely enforce automated reconfiguration through Digital Policy Management and Configuration Management. Where possible, policy management decisions shall be allowed to automate reconfigurations, if necessary.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are



CGS Utilization and Performance Management Capability



Version 1.1.1

services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Network resources have different Utilization and Performance baselines.
2. Network availability requirements are clearly defined.
3. Service delivery depends on an underlying infrastructure of people, process, technology, and environment.
4. The system is adequately designed to support Utilization and Performance needs.
5. SLAs are established that drive the baseline.
6. Network Operations focuses on the component parts (people, process, technology, and environment) and monitors these for Utilization and Performance.

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 primary priority is not on one asset, but on the ability of that asset to produce expected results.
2. Utilization and Performance affects the effectiveness and efficiency of service delivery.
3. Provided services (e.g., automated services, web services, service-oriented architecture [SOA] services, or any of many other services) may be manual (e.g., Help Desk).
4. Minimum and maximum effective Utilization and Performance thresholds are clearly identified.
5. Target levels, including acceptable variances, are defined in this Capability.
6. When a threshold is exceeded, it provides the necessary alerts for response.
7. An effective service or system provides the expected result (i.e., the service or system works as intended).
8. An efficient service or system provides the expected result within specified performance parameters.

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



CGS Utilization and Performance Management Capability



Version 1.1.1

Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Utilization and Performance Management is employed correctly, the Organization will possess the ability to reactively and proactively discern operational impact on service delivery within the scope of the components of the underlying infrastructure that support service delivery.

The Organization, more specifically Network Operations, will be able to do following:

1. Design resources to enable the Utilization and Performance Management Capability
2. Implement additional tools within the network or environment to employ Utilization and Performance Management activities where possible, if preexisting resources are incapable of performing Utilization and Performance Management
3. Know business and mission needs, leveraging information from the Understand Mission Flow Capability
4. Determine how many and for which resources to implement for Utilization and Performance Management
5. Establish Utilization and Performance schema to determine what data (based on business need) needs to be collected
6. Understand baseline and threshold parameters
7. Understand what actions need to be taken based on which thresholds are met
8. Provide reporting

An Organization will design its systems to incorporate existing target performance levels. For each legacy resource that does not meet stated Utilization and Performance targets, the Organization will ensure that additional tools (e.g., hardware/software) are in place to ensure targets can be met.

Each Organization will recognize the specific characteristics for Utilization and Performance, develop applicable thresholds for each, and determine appropriate responses when particular issues occur. Organizations will define Utilization and Performance baselines, as well as the target Utilization and Performance levels and thresholds for each resource on the network or within the Enterprise. The Organization will determine thresholds including resource limitations (e.g., available power), as well as service requestor expectations such as SLAs. Contributors to Utilization and Performance Management determination will include resource owners, resource operators, and users.



CGS Utilization and Performance Management Capability



Version 1.1.1

The Organization will also establish target baselines. In addition, the Organization will perform modeling and simulation and revisit the baseline as needed based on experience gained from additional performance exercises, mission need, and trend analysis.

Proactive and reactive Utilization and Performance Management will be performed. The Organization will establish monitoring of appropriate resource characteristics, including anything that would generate an alert on performance, such as the system, CPU utilization, and activity levels. As an end goal, the Organization will also provide situational awareness of Utilization and Performance. This information will be used to react and reconfigure resources to appropriately manage Utilization and Performance Management. Moreover, the Organization will establish manual or automated procedures for intervention (through the Incident Response Capability) upon exceeding defined thresholds by analyzing business policy business drivers. Systems will be monitored and will provide alerts, and the Organization will securely enforce automated reconfiguration based on policy decisions, leveraging the Digital Policy Management and Configuration Management Capabilities.

Organizations will provide periodic and ad hoc reports on Utilization and Performance characteristics including trending. Scheduled reports will be generated based on the Organization's operational and business drivers, and ad hoc reports will be generated on demand based on consumer needs. Content of the reports will change based on the consumer; thus, Organizations will need to define a schema of items needed per consumer. Report data will be maintained to perform trend analysis, and Organizations will analyze reports and trends over time to reestablish the baseline. The goal will be to provide an effective, efficient service provision to understand the Utilization and Performance characteristics. From there, the Organization can determine what needs to be done. The Organization will use a standard reporting format for distributing reports to consumers and sharing situational awareness information with peer Organizations.

Consumers of Utilization and Performance Management reports from an Enterprise layer perspective may include the following: government to review and modify policy on service provision; management for resource planning and allocation to maintain SLAs; operations for tactical movement of resources to maintain SLAs; and users for SLA reports to ensure efficient support of user activity.



CGS Utilization and Performance Management Capability



Version 1.1.1

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.

- Understand Mission Flows—The Utilization and Performance Management Capability relies on the Understand Mission Flows Capability for information that is used to provide for the efficient allocation of network resources.
- Understand Data Flows—The Utilization and Performance Management Capability relies on the Understand Data Flows Capability for information that is used to provide for the efficient allocation of network resources.
- Hardware Device Inventory—The Utilization and Performance Management Capability relies on the Hardware Device Inventory Capability for information that is used to provide for the efficient allocation of network resources.
- Software Inventory—The Utilization and Performance Management Capability relies on the Software Inventory Capability for information that is used to provide for the efficient allocation of network resources.
- Digital Policy Management—The Utilization and Performance Management Capability relies on the Digital Policy Management Capability to enforce automated reconfiguration based on alerts received.

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 Utilization and Performance Management 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 Utilization and Performance Management 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 Utilization and Performance Management Capability



Version 1.1.1

- IA Awareness–The Utilization and Performance Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Utilization and Performance Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Utilization and Performance Management 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 Utilization and Performance Management Capability relies on the Network Security Evaluations Capability for information that is used to fill any gaps that may have been overlooked.
- Risk Mitigation–The Utilization and Performance Management Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

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> | |
| PL-6 SECURITY-RELATED ACTIVITY PLANNING | Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals. Enhancement/s: None Specified |
| PM-6 INFORMATION | Control: The organization develops, monitors, and reports on the |



CGS Utilization and Performance Management Capability



Version 1.1.1

| | |
|--|--|
| <p><i>SECURITY MEASURES OF PERFORMANCE</i></p> | <p>results of information security measures of performance. Enhancement/s: None Specified</p> |
| <p>SC-6 RESOURCE PRIORITY</p> | <p>Control: The information system limits the use of resources by priority. Enhancement/s: None Specified</p> |
| <p>SC-24 <i>FAIL IN KNOWN STATE</i></p> | <p>Control: The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.</p> <p>Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.</p> <p>Control Enhancements: 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.

Utilization and Performance Management Directives and Policies

| Title, Date, Status | Excerpt / Summary |
|---|--|
| Intelligence Community (IC) | |
| IC Policy Memorandum for Uniform Data Standards, 7 March 2007 (Draft) | Summary: This draft Intelligence Community Policy Memorandum (ICPM) established a Director of National Intelligence (DNI) policy, which defines the uniform standards of data, metadata, and resource utilization data |



CGS Utilization and Performance Management Capability



Version 1.1.1

| | |
|---|--|
| | that is to be shared within the IC. Final document not located. |
| | |
| ODNI/CIO-2009-012, Assistance to the CNCI 7 Top Secret Environment Tiger Team..., 28 January 2009, Classified | Summary: This document is classified. See the document for details. |
| | |
| Comprehensive National Cybersecurity Initiative (CNCI) | |
| NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified | 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. |
| | |
| Department of Defense (DoD) | |
| Nothing found | |
| | |
| Committee for National Security Systems (CNSS) | |
| Nothing found | |
| | |
| Other Federal (OMB, NIST, ...) | |
| Nothing found | |
| | |
| Executive Branch (EO, PD, NSD, HSPD, ...) | |
| Nothing found | |
| | |
| Legislative | |
| Nothing found | |
| | |



CGS Utilization and Performance Management Capability



Version 1.1.1

Utilization and Performance Management 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 800-55 Rev 1 Performance Measurement Guide for Information Security, July 2008, Unclassified | This special publication (SP) is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs. |
| | |
| Executive Branch (EO, PD, NSD, HSPD, ...) | |
| Nothing found | |
| | |
| Legislative | |
| Nothing found | |
| | |
| Other Standards Bodies (ISO, ANSI, IEEE, ...) | |
| Nothing found | |
| | |



CGS Utilization and Performance Management 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. Solution used for implementation—Additional hardware/software may be needed to manage legacy resources not otherwise capable of being monitored.
2. Scope of work—The number of devices and breadth of hardware/software will contribute to the complexity of this Capability's functions.
3. Network bandwidth availability and consumption—As more network connections are needed to satisfy the Capability's bandwidth requirements, there will be less bandwidth available for other systems to use. Bandwidth will need to be balanced among all Capabilities to satisfy mission needs based on priority.
4. Number of service environments and service providers—The number of environments and providers used by the Enterprise will contribute to the complexity of monitoring and management.

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 Network Mapping Capability.



CGS Utilization and Performance Management Capability



Version 1.1.1

- The Enterprise shall ensure availability and reliability of resources that directly or indirectly provide support to mission functionality such that they are accessible and usable on demand by an authorized entity.
- All utilization and performance target levels shall be defined and managed by the Enterprise.
- Networks shall be designed to incorporate target performance levels and be managed at the target levels that shall help to ensure the reliability of resources.
- The Enterprise shall establish target utilization and performance baselines based on performing modeling and simulation in a test environment.
- The Enterprise shall establish target baselines based on running exercises to measure actual performance in an operational or semi-operational environment.
- The Enterprise shall establish target baselines based on exercise results.
- The Enterprise shall reestablish baselines based on mission need and trend analysis as experience is gained through running the network.
- The Enterprise shall establish target baselines based on iteratively revisiting the definition of target levels as experience is gained.
- The Enterprise shall identify characteristics of resource utilization and network performance.
- The Enterprise shall gather data on resource utilization and network performance characteristics.
- The Enterprise shall analyze data to articulate a target operational utilization and performance level.
- The Enterprise shall define utilization and performance thresholds that when exceeded shall trigger corrective action (e.g., escalation to incident response, operations support, or other to SME for analysis and potential intervention).
- The Enterprise shall identify network utilization anomalies and generate useful alerts of the identified anomalies.
- The Enterprise shall balance demand for resources (performance) and consumption of those resources (utilization).
- The Enterprise shall employ both reactive and proactive management for utilization and performance.
- The Enterprise shall employ reactive utilization management for responding to real-time resource consumption in operations.
- The Enterprise shall employ proactive utilization management for network simulation and examination to plan for resource consumption before that consumption occurs in real-time operations.



CGS Utilization and Performance Management Capability



Version 1.1.1

- The Enterprise shall employ reactive performance management for responding to unforeseen difficulties in real-world operations.
- The Enterprise shall employ proactive performance management for network simulation and examination to mitigate operational risks before they occur in real-world operations.
- The Enterprise shall systematically monitor and evaluate service delivery for performance management to ensure effective and efficient operations (e.g., with respect to network performance management—network throughput, service response times, path utilization, priority, and preemption).
- The Enterprise shall measure and track end-to-end performance of applications and missions.
- The Enterprise shall ensure that applications perform efficiently, that systems have sufficient capacity to support them, and that networks that deliver application functionality can meet SLAs.
- SLAs shall define the obligations and expectations between the service provider and the service user to provide a range of support services, how they shall be monitored, and how deviations shall be rectified.
- The Enterprise shall support QoS and priority of resources.
- Traffic engineering shall be performed to provide different priority to different users, applications, or data flows, and to guarantee a minimum level of performance for a data flow.
- The Enterprise shall leverage and prioritize information from other systems within the Enterprise.
- The Enterprise shall provide reports of network utilization covering several metrics.
- For all exceeded thresholds, an alert shall be triggered and prompt an intervention.
- Alerts and notifications shall be sent out when SLAs are not met.
- Notification alerts shall be sent to local network operations for evaluation and incident response systems for further evaluation at an Enterprise level.
- Situational awareness personnel shall perform trend analysis to determine whether an incident is a potential risk.
- The Enterprise shall securely employ automated reconfiguration through digital policy and configuration management.
- Where possible, policy management decisions shall be allowed to automate reconfigurations, if necessary.