GWD-I
Enterprise Grid Requirement (EGR) RG
http://forge.gridforum.org/projects/egr-rg/

Authors
Ravi Subramaniam, Intel
Toshiyuki Nakata, NEC
Satoshi Itoh, AIST
Yoshio Oyanagi, Kogakuin University
Atsuko Takefusa, AIST
Tokuro Anzaki, Hitachi, Ltd.
Ken-ichi Mizoguchi, Toshiba Solutions Corporation
Hideaki Tazaki, Fujitsu Limited
Takuya Mori, NEC Corporation
Toshihiro Suzuki, Oracle Corporation Japan
Masahiko Hamada, IBM Japan, Ltd.
Takashi Maeshiro, First Riding Technology Inc.
Hiroyuki Takashima, Novartis Pharma K.K.
Masahiro Yoshioka, Mazda Motor Corporation

September 21, 2008

Guidelines of Requirements for Grid Systems v1.0

Status of This Document

This memo provides information to the Grid community on guidelines of requirements for Grid systems. It has recommendations on the designing grid systems. Distribution is unlimited.

Copyright Notice

Abstract

This document describes the requirements for construction and operation of grid systems. This document does not say “Grid Systems must satisfy these requirements”. It says “These requirements shall be considered when someone designs / constructs / operates on Grid Systems”.

Contents

1. Introduction

This standard describes requirements to be considered in integration and operation of grid systems that effectively provide services by virtualizing and flexibly assigning, collaborating and using various resources including computers, storages and networks in accordance with different purposes. In order for the systems to effectively function, clarification and operational management of many related activities are required. In grid systems suppliers provide services to consumers, and in many cases consumers themselves may become suppliers and provide services to other consumers.

Coordinated construction and operation of grid systems generate opportunities for ongoing management, greater efficiency and continual improvement.

This standard is assumed to target people who use and operate grid systems.

1.1 Scope of the document

This standard specifies requirements for construction and operation of grid systems of an acceptable quality for customers.

This standard may be used by the following business enterprises, organizations and applications.

a) Organizations who design, construct and operate grid systems

b) Commercial Data Centers that provide hosting and housing services as their business.

c) Service providers who provide applications, IT resources and others.

d) Organizations that mediate various information services

This standard, as Figure 1 shows, defines a grid system as a hierarchical structure that consists of four layers. The first layer is the physical environment layer that consists of hardware components associated with servers, storages and networks. The second layer is the operating environment layer that consists of a number of software such as an operating system and a file system that makes the first layer operable. The third layer is the platform layer that consists of a number of softwares to achieve operations over multiple components such as database and grid middleware. The forth layer is the application service layer that consists of applications and portals. Consumers who use the forth layer are called end-users.

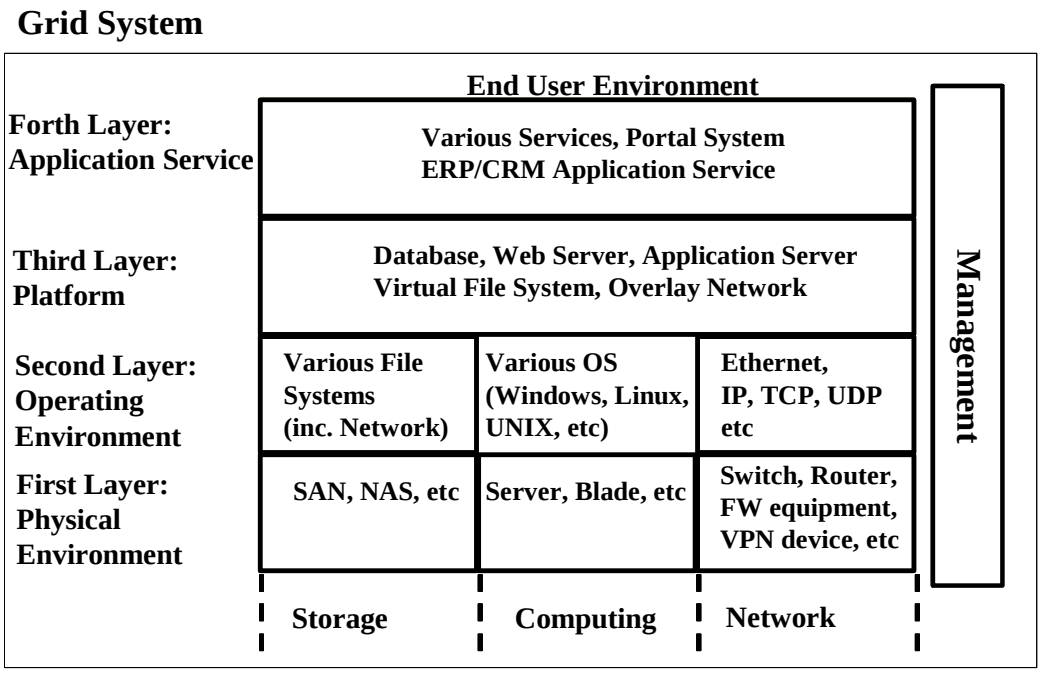

Figure 1: Hierarchy Diagram of the Grid System

Suppliers operate the entire or a part of grid system and provide them as services to consumers. Consumers may add components of hardware or software where needed. In this case consumers become suppliers who provide services with added components to other consumers. As Figure 2 shows, such pairs of suppliers and consumers are concatenated to form a chain and the consumers at the end are called end-users. Although end-users access to services through the forth layer, there may be services without the forth layer. This standard applies to a pair of a supplier and consumer and the service provided between them.

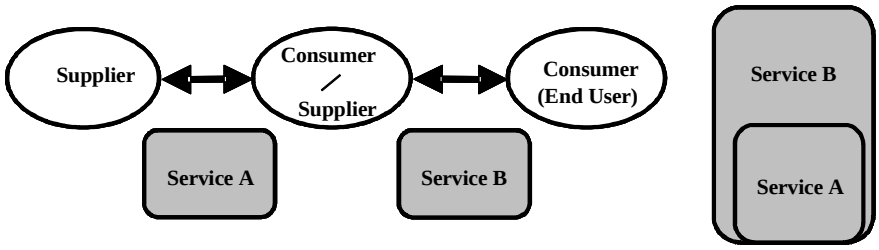

Figure 2: Chain of Supplier and Consumer

Requirements included in this standard are limited to minimal and therefore, addition of any requirement that is needed to satisfy the needs of a specific business may be considered. The way requirements in this standard are implemented to achieve the entire objective depends on the characteristics of the relations between suppliers and consumers.

2. Terms and Definitions

Terms those are used in this document is explained in this chapter.

2.1 Service

A system provided by a supplier is called a service.

Note: A service may corresponds to both the entire grid system and a part of grid system. In other words, multiple services provided by multiple suppliers may be integrated to form one grid system.

2.2 Supplier

A supplier is a person who provides either the entire or a part of a grid system as a service.

Note: Suppliers include system operators and they use this standard from the standpoint of designer and operator of systems. Multiple suppliers are present in a grid system that consists of multiple services.

2.3 Consumer

A consumer is a person who makes use of a service provided by a supplier.

Note: The consumer may refer not only to a person but a part of a system. This means that services provided in the layers below the forth layer may be accessed directly by the components in the upper layer that a consumer has added. Furthermore, consumers may not necessarily be the members of a single organization and members of a virtual organization that consists of multiple organizations are also treated as consumers.

2.4 Access

Access is an operation for consumers to directly use the services under their privileges.

Note: Submissions of jobs to computing resources and writing records to database resources correspond to this operation, for example.

2.5 Agreement

Agreement is an operation of consumers that enable indirect use of services by making requests to suppliers to implement processes that consumers have no privilege to implement.

Note: Change of priorities of job submissions to computing resources and retrieval of log data of submitted jobs and database access correspond to this operation, for example.

2.6 Control

Control is an operation by suppliers to manage/operate services.

Note: Allocation of resource for each consumer, setting of priority and configuration of consumer access privilege to resources correspond to this operation, for example.

2.7 Usability

This term indicates the characteristics related to ease of use from the viewpoint of consumers.

Note: This does not only mean "availability".

2.8 Controllability

The term indicates the characteristics related to ease of use and control from the viewpoint of supplier.

Note: This does not only mean "ability to control".

2.9 Confidentiality

The term indicates the property that information or information processing/storing system is not made available or disclosed to unauthorized consumers.

2.10 Integrity

The term indicates the property of safeguarding the accuracy and completeness of information or information processing/storing system.

2.11 Availability

The term indicates the property of being accessible and usable to information or information processing/storing system upon demand by an authorized consumer.

2.12 Policy

The term refers to the content specified for the way of allocating services in advance.

Note: This is used for the purpose of data sharing that do not have effect on the load distribution, prioritized processing for each consumer, prioritized processing for each access and other consumers of the service. Policies include operation policies for suppliers to manage and operate services and usage policies for consumers to use services.

3. Grid System Model

Types of operations performed between suppliers, consumers and services are shown in Figure 3. Actions that suppliers implement against services are operations to manage services and therefore called "control". Actions that consumers implement against services are classified two ways. One is the direct operation performed using consumers' own privileges and this is called "access". The other is the indirect operations performed by making requests to suppliers to implement some process and this is called "agreement". This "agreement" includes disclosure of service information and prioritization of executions.

Requirements for "access", "agreement" and "control" are described in 4.1, 4.2 and 4.3 respectively.

There is a case where a grid system is used in cooperation with other external grid systems. Requirements for grid systems in such case are described in 4.4.

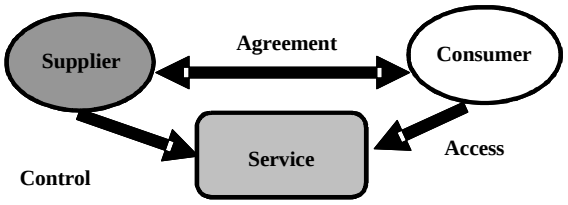

Figure 3: Operations between Supplier, Consumer and Service

4. Requirements for Grid System

This section describes requirements those are required to be investigated for Grid System. Requirements are categorized by kinds of players and operations.

4.1 Access

4.1.1 Usability

The following items shall be considered as requirements from a usability point of view when consumers access services.

* a: Consumers can access services without being aware of the lower level layers (including location, OS and middleware) (layer 4)
* b: Services are accessible using a uniform interface (layer 3, 4)
* c: Access protocols to services are selectable where there is more than one access protocol present (layer 2, 3)
* d: Existing applications are operable without any change (layer 3, 4)

* e: When more than one authentication mechanism is present, only a minimal authentication mechanism is required (layer 3, 4)

* f: Expected performance of the system is estimated in advance. (layer 2, 3, 4)

4.1.2 Security

The following items shall be considered as requirements from a security point of view when consumers access services.

* a: Consumers and services are mutually authenticated (layer 3)

* b: Confidentiality, completeness and availability of accesses to services by consumers are guaranteed (layer 3, 4)

* c: Confidentiality, completeness and availability of contents such as data generated by accesses to services by consumers is guaranteed (layer 3, 4)

* d: Logs of access to services by consumers can be recorded (layer 3, 4)

* e: Confidentiality, completeness and availability of access logs to services by consumers can be guaranteed (layer 2, 3, 4)

4.2 Agreement

4.2.1 Usability

The following items shall be considered as requirements from a usability point of view when consumers perform agreement-related operations against services according to service levels.

* a: Static information including configuration information and performance of services is disclosed to consumers (layer 2, 3)

* b: Dynamic information including load status, processing capacity and failure of services is disclosed to consumers (layer 2)

* c: Consumers can configure usage policies for each service individually at the time of usage (layer 2, 3)

* d: Consumers can view a record of service level (layer 2, 3)

4.2.2 Accounting

The following item shall be considered as a requirement from the accounting point of view when consumers perform agreement-related operations against services.

* a: Accounting information such as log data of services used by consumers are disclosed to consumers (layer 3)

4.2.3 Security

The following items shall be considered as requirements from the security point of view when consumers perform agreement-related operations against services.

* a: Confidentiality, completeness and availability of operations related to agreements implemented by consumers to services can be guaranteed (layer 3)

* b: Confidentiality, completeness and availability of information including usage history and accounting generated by operations on agreements implemented by consumers to services can be guaranteed (layer 3)

4.3 Control

4.3.1 Controllability

The following items shall be considered as requirements from the controllability point of view when suppliers perform control-related operations against services.

* a: Priorities configured by and for each consumer are configurable. (layer 3)
* b: Services have the mechanism that users can access services without being aware of lower level layers (including location, OS and middleware) (layer 3)
* c: Resource allocation is dynamically altered according to suppliers' operation policy (layer 3)
* d: Management items required to construct and operate upper level layers are configurable (layer 2, 3)
* e: Suppliers can monitor status of services (including failure and risk) by inquiry or notification (layer 1, 2, 3)
* f: Suppliers can view access status of consumers (layer 2, 3)
* g: Policies for service allocation are configurable with regard to consumer access(layer 2, 3)
* h: Services include a mechanism to easily perform maintenance (layer 2, 3)
* i: Configuration change, expansion and destroy of services can be performed according to service levels without halting the whole system (layer 2, 3)
* j: Suppliers can easily monitor status of the whole services (layer 1, 2, 3)

4.3.2 Accounting

The following item shall be considered as a requirement from the accounting point of view when suppliers perform control-related operations against services.

* a: Usage history of consumers is viewable by suppliers (layer 2, 3)

4.3.3 Security

The following items shall be considered as requirements from the security point of view when suppliers perform control-related operations against services.

* a: Suppliers and services can be mutually authenticated. (layer 3, 4)
* b: Confidentiality, completeness and availability of services can be guaranteed (layer 2, 3)
* c: Confidentiality, completeness and availability of operations related to controls implemented by suppliers to services can be guaranteed (layer 2, 3)
* d: Confidentiality, completeness and availability of contents generated by operations related to controls implemented by suppliers to services can be guaranteed (layer 2, 3)
* e: Logs for controls implemented by suppliers to services can be recorded (layer 2, 3)
* f: Confidentiality, completeness and availability of operation logs related to controls implemented by suppliers to services can be guaranteed (layer 2, 3)
* g: Suppliers can configure security policy of services (layer 2, 3)

4.4 Cooperation between Systems

The following items shall be considered as requirements when a service cooperates with an external grid system.

* a: Ways to establish mutual trust relations are specified(layer 2, 3)
* b: Each other's services are cooperable(layer 2, 3)

5. Contributors

This document was originally developed by “Grid Computing Industrial Guidelines Standardization Committee” on February 2008. The committee was organized in 2005 by AIST and was funded by METI through INSTAC from FY 2005 to FY 2007.

AIST: National Institute of Advanced Industrial Science and Technology

METI: Ministry of Economy, Trade and Industry

INSTAC: Information Technology Research and Standardization Center, JSA (Japanese Standards Association)

6. Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

7. Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

8. Full Copyright Notice

Appendix

The requirements described in this document were extracted from several grid systems. The following grid systems were investigated for this purpose.

* In-house technical computing grid (Computing grid - cluster -)

  semiconductor, automobile, construction

* In-house technical computing grid (PC grid)

  novartis (pharma)

* In-house data grid

  Financial company

* Academic collaborative grid (Computing grid)

  APGrid (Asia Pacific Grid testbed)

* Commercial data center grid (Business computing grid)

  Mazda operates Business Grid PJ in Japan on a trial basis

* Commercial data center grid (Commercial storage service)

  FRT(Data Center Company)

In addition, the following use cases were picked up for applying the guideline. These use cases were presented in the past EGR-RG sessions of OGF/GGF.

* Fleet Numerical by Platform Computing
  - "US Navy's Fleet Numerical Meteorology and Oceanography Center", Nick Werstiuk, (Platform Computing) @ GGF18
* Financial Service by HP and Hartford
  - "Grid for Financial Services", Larry Ryan, (Hewlett-Packard), and Robert Nordlund, (Hartford) @ GGF18
* SURAgrid (regional cooperative grid)
  - "Building a Campus Grid: Concepts & Technologies", Mary Fran Yafchak (SURA)@GGF18

Examples of requirements for typical grid systems are summarized in the following tables. This table is expected to be used as a reference.

Note: Even though the table is not fully filled, it is attached for a reference.

		Item No.	Layer	Requirement	Technology to satisfy requirements	1. Enterprise Technical Computing Grid (Computing Grid)	1.1 Fleet Numerical by Platform Computing	1.2 Financial Service by HP and Hartford	2. Enterprise Technical Computing Grid (PC grid)	3. Academic Cooperative Grid (Computing Grid)	3.1 SURAgrid (regional cooperative grid)	4. Business Computing Grid (Provision of server resources to business systems)	5. Storage Infrastructure Service (Storage Grid)	6. Enterprise Data Grid (Database Federation)
Access	Usability	4.1.1-a	4	Consumers can access services without being aware of the lower level layers (including location, OS and middleware)	virtualization technology	Job submission to execute application and retrieval of result are possible without being aware of the location of resources to be executed and the OS used. (necessary)	Multi site, heterogeneous platform	Multi site	Job submission to execute application and retrieval of result are possible without being aware of the location of resources to be executed and the OS used. (necessary)	Job submission to execute application and retrieval of result are possible without being aware of the location of resources to be executed (compute server, data) and the OS used. (necessary)	Across Departments on a campus or Across Institutions for access to other campuses' resources	It is available without being aware of the location of services. (necessary)	Storage resources are virtualized, and the way of accessing their logical location and interface is provided. Namespace and access method of resources are logically provided and therefore they will not be recognized by consumers when physical resources are changed.	Job submission to execute data reference and retrieval of result are possible. (necessary)
		4.1.1-b	3,4	Services are accessible using a uniform interface	Standard interface	Job execution can be requested from the same interface without relying on the OS and middleware of compute resources.	single 'console' across locations		N/A	Uniform interface to heterogeneous computer is provided (necessary)	Portal accessibility	Uniform interface to the services is provided. (necessary)	Either data and files to storages, and access and control of database are standardized or they are provided by the interface that aims to be industry standard.	Access to database is possible from a uniform interface. (optional)
		4.1.1-c	2,3	Access protocols to services are selectable where there are more than one access protocols present		N/A			N/A	N/A	Portal test scripts (https://gridportal.sura.org/gridsphere/dist/sgGridTest.html) represent several Globus based protocols.	N/A	Access methods of storage provided are virtualized and multiple selections are possible. Specifically, the following access methods are possible. <Block> <FILE> *iSCSI *NFS *FC-SAN *CIFS *SATA *SMB *SAS : :	N/A
		4.1.1-d	3,4	Existing applications are operable without any change		It can be used without changing commercial applications.		Ability to minimize application changes to take advantage of a Grid-based infrastructure	N/A	Programs by users can be used. (necessary) It can used without changing commercial applications. (preferable)	Once an application has been grid-enabled and deployed to a SURAgrid site, it should be able to run at other sites which have appropriate environment (cf. libraries or versions.) Should also be able to minimize applicatiions changes to take advantage of campus grid infrastructures that are inter-connected (moving smoothly between campus grid and regional grid).	N/A	Compatible systems for each system of DB, contents, files and block that existing applications use are provided and they are available for use without restructuring applications.	It can be used without changing commercial applications.
		4.1.1-e	3,4	When more than one authentication mechanisms are present, only a minimal authentication mechanism is required	Realized by single sign-on technology (Proxy certificate and delegation)	Access to multiple computer systems is possible without multiple signing-in.(necessary)			Access to multiple computer systems is possible without multiple signing-in.(necessary)	Access to multiple computer systems is possible without multiple signing-in.(preferable)	Use of cross-certification processes and SURAgrid BridgeCA leverages campus identity systems, enabling consumers to use their campus ID for access and faciltiating scalable inter-institutional authentication.	Access to multiple services and management systems is possible without multiple signing-in.(necessary)	When multiple systems are involved in authentication, authorization and signature of access to storage system, it can collaborate with multiple authentication systems or with a system that integrates them.	Access to multiple computer systems is possible without multiple signing-in.(necessary)
		4.1.1-f	2,3,4	Expected performance of the system is estimated in advance.				Real-time calculation is a competitive advantage			No performance estimates are provided to consumers at this time but this is desirable and tools to provide this exist/are emerging.			
	Security	4.1.2-a	3	Consumers and services are mutually authenticated			Military Security				GSI security identifies both hosts (suppliers) and consumers. Systems (cluster resources, portals, user management store) and end users require authentication using PKI credentials.			
		4.1.2-b	3,4	Confidentiality, completeness and availability of accesses to services by consumers are guaranteed	Policy control	To which computers consumers are accessing is not open to other consumers. Range of computers available to consumers is controllable.	Military Security		Range of computers available to consumers is controllable.	Communication channels of accesses are encrypted. (preferable) Range of computers available to consumers is controllable. (necessary)	secure (uses Globus Grid Security Infrastructure)		Encryption mechanism which complies with SLA is provided to the interface that provides storage infrastructure service. Policy on storage access can be configured in accordance with SLA contract.	Content of Requirements is protected on the server (management node) which distribute requirements to database resources (database node). (necessary) Range of computers available to consumers is controllable.
		4.1.2-c	3,4	Confidentiality, completeness and availability of contents such as data generated by accesses to services by consumers is guaranteed	VM technology, VLAN technology	Jobs and data are protected from other consumers on the server (management node) which distributes jobs to compute resources (compute node). (necessary)	Military Security		Jobs and data are protected from other consumers on the server (management node) which distributes jobs to compute resources (compute node). (necessary)	Jobs and data are protected from other consumers on the server (management node) which distributes jobs to compute resources (compute node). (preferable)	secure	Business programs and data of consumers in grid systems are protected from other consumers. (necessary)	Completeness of access control, encryption and electronic signature which can maintain confidentiality of information in storage between consumers and between consumers and suppliers is guaranteed in the scope of SLA.	Requirements and data are protected on the server (management node) which distribute requirements to database resources (database node). (necessary)
		4.1.2-d	3,4	Logs of access to services by consumers can be recorded			Military Security				secure			

		4.1.2-e	2,3,4	Confidentiality, completeness and availability of access logs to services by consumers can be guaranteed	Access control, Encryption technology	Other than administrators can not access to logs of job manager and portal servers.	Military Security		Other than administrators can not access to logs of job manager and portal servers.	Other than administrators can not access to logs of job manager and portal servers.	secure	Other than administrators can not access to logs of business management systems and middleware.	Other than administrators can not access to logs of storage management systems and middleware.	Other than administrators can not access to logs of database management systems and middleware.
Agreement	Usability	4.2.1-a	2,3	Static information including configuration information and performance of services is disclosed to consumers	Monitoring	Static information such as configuration information and performance of services is disclosed to consumers.(preferable)			Static information such as configuration information and performance of services is disclosed to consumers.(preferable)	Static information such as configuration information and performance of services is disclosed to consumers.(necessary)	Allow consumer or application to choose resource (based on availability, load, type of resource)	Static information such as configuration information and performance of services is disclosed to consumers.(necessary) Service level, indent information, problem management information and annual operation schedule are provided.	Static information of storage is disclosed. Static information of storage includes the following. *Object type *Volume *functional performance *availability :	Static information such as configuration information and performance of services is disclosed to consumers.(preferable)
		4.2.1-b	2	Dynamic information including load status, processing capacity and failure of services is disclosed to consumers	Monitoring	Load status of job manager queue is disclosed to consumers.			N/A	Load status of job manager queue is disclosed to consumers. (preferable)	Allow consumer or application to choose resource (based on availability, load, type of resource)	Load status and performance status of services can be viewed in real time or information is provided by suppliers.	Dynamic information of storage is disclosed. Dynamic information of storage includes the following. *Volume *free space *statistical performance *underlying index (performance, location…) :	N/A
		4.2.1-c	2,3	Consumers can configure usage policies for each service individually at the time of usage	Policy control	Prioritization can be performed between multiple consumers or by a consumer himself. (optional)			Prioritization can be performed between multiple consumers or by a consumer himself. (optional)	Prioritization can be performed between multiple consumers or by a consumer himself. (preferable)	Usage policies managed by site contributing resource (supplier). Consumer can inspect usage policies. Prioritization may be performed between multiple consumers or by a consumer himself (preferable).	Prioritization of multiple tasks can be performed by a consumer himself. (necessary)	Access policy such as use rights is freely configurable against the domain provided by a storage supplier in the scope of SLA with the supplier.	Prioritization can be performed between multiple databases consumers or by a database consumer himself (optional)
		4.2.1-d	4	Consumers can view a record of service level	Service-level management Monitoring	N/A				N/A	Grid portal tracks and views services from the consumer perspective, leveraging data from back-end usage and accounting mechanisms.		Consumers can view number of access, access speed and access frequency of storage.	N/A
	Accounting	4.2.2-a	3	Accounting information such as log data of services used by consumers are disclosed to consumers	Logging Monitoring	Usage volume of services by consumers are made available to consumers. (necessary)			Usage volume of services by consumers are made available to consumers. (necessary)	Usage volume of service by consumers are made available to consumers. (preferable)	Usage volume of service by consumer is made available to that consumer in process).	Usage volume of services by consumers are made available to consumers. (necessary)	Consumers of storages can access to dynamic information of system when needed. *Current remaining volume *Usage rate *Back up…	Usage volume of services by consumers are made available to consumers. (necessary)
	Security	4.2.3-a	3	Confidentiality, completeness and availability of operations related to agreements implemented by consumers to services can be guaranteed	Access control	Priority set by consumers are not referenced by other than administrators and manipulated by administrators.	Military Security			Access privilege set by consumers are not referenced by other than administrators and manipulated by administrators.(preferable)	Minimal…relies upon proper service file-system protections		Suppliers of storage system can implement similar encryption, authorization and acknowledgement to security (authentication, authorization and auditing) according to SLA.	Access privilege set by consumers are not referenced by other than administrators and manipulated by administrators.
		4.2.3-b	3	Confidentiality, completeness and availability of information including usage history and accounting generated by operations on agreements implemented by consumers to services can be guaranteed	Access control	Usage volume of services by consumers are not referenced by other than the corresponding consumers. (necessary)	Military Security		Usage volume of services by consumers are not referenced by other than the corresponding consumers. (necessary)	Usage volume of services by consumers are not referenced by other than the corresponding consumers. (preferable)	Usage volume of service by consumer is made available to that consumer (in process).	Usage volume of services by consumers are not referenced by other than the corresponding consumers. (necessary)	Access history of storage remains. Access history, accounting and security system of storage are associated.	Usage volume of services by consumers are not referenced by other than the corresponding consumers. (necessary)
		4.3.1-a	3	Priorities configured by and for each consumer are configurable	Priority management	Configuration method, in which suppliers can control job execution sequence in accordance with priority set by consumers, is available.			N/A	Configuration method, in which suppliers can control job execution sequence in accordance with priority set by consumers, is available. (preferable)	Local policy and technology components factor first in determination of consumer priority. Priority may then be influenced by regional grid participation objectives, MOUs or service agreements.	N/A	Use rights, encryption and signature for each consumer are configurable to storage environment that storage infrastructure services provide.	N/A
		4.3.1-b	3	Services have the mechanism that users can access services without being aware of lower level layers (including location, OS and middleware)	virtualization technology						Not at this time.		It is only available with interfaces of storage infrastructure services.	N/A

Controllability	4.3.1-c	3	Resource allocation is dynamically altered according to suppliers' operation policy	Policy control	Load allocation such as allocating jobs to compute resources is configurable according to job load.	NWP(Numerical Weather Prediction) jobs to be executed within a strict schedule		Ranges between servers, which distribute jobs, and PCs are recognized by administrators and control program, and allocation by job size is possible. (preferable) Grid jobs that operate on PC/workstation resources do not affect PC consumers. (necessary)	Annual or automatic load distribution is possible depending on load status of compute servers.(preferable)	Locally managed via various means. Often done in conjunction with running the specific application (application monitors resources and makes appropriate decisions).	Load distribution is possible depending on load status of services. (necessary)	Volume, type, performance and availability of storages are dynamically allocated according to SLA. This enables provision of storage infrastructure that realizes wide-area distributed RAID and distributed FS.	N/A
	4.3.1-d	2,3	Management items required to integrate and operate upper level layers are configurable		N/A			N/A	N/A	N/A	N/A	Storage infrastructure provided is virtualized, independent from lower level systems and consumers can change access privilege of storage domain.	N/A
	4.3.1-e	1,2,3	Suppliers can monitor status of services (including failure and risk) by inquiry or notification	Monitoring	Status of each computer system which become a compute resource is monitorable by suppliers through a simple interface.(necessary)			Status of each computer system which become a compute resource is monitorable by suppliers through a simple interface.(necessary)	Status of each computer system which become a compute resource is monitorable by suppliers through a simple interface.(necessary)	Portal provides a level of status monitoring. Minimum status reporting preferred for all systems, but not enforced.	Status of each computer system which become a compute resource is monitorable by suppliers through a simple interface.(necessary)	Dynamic information such as usage volume of storage infrastructure provided is monitorable.	Status of each computer system which become a database resource is monitorable by suppliers through a simple interface.(necessary)
	4.3.1-f	2,3	Suppliers can view access status of consumers	Monitoring	Distribution and status of jobs submitted by consumers can be viewed by suppliers.(necessary)			Distribution and status of jobs submitted by consumers can be viewed by suppliers.(necessary)	Distribution and status of jobs submitted by consumers can be viewed by suppliers.(necessary)	Distribution and status of jobs submitted by consumers can be viewed by suppliers locally (necessary) but not necessarily at level of SURAgrid.	N/A	Access statistics and evidence of access can be viewed while maintaining confidentiality of access contents of storage infrastructure provided.	Distribution and status of jobs submitted by consumers can be viewed by suppliers.(necessary)
	4.3.1-g	2,3	Policies for service allocation are configurable with regard to consumer access	Access control Policy control	Conditions for job allocation in each computer system which becomes a compute resource is configurable by suppliers.(preferable) Prioritization between multiple consumers is possible. (optional)	NWP(Numerical Weather Prediction) jobs to be executed within a strict schedule	Comprehensive fair-use policies	Conditions for job allocation in each computer system which becomes a compute resource is configurable by suppliers.(preferable) Prioritization between multiple consumers is possible. (optional)	Conditions for job allocation in each computer system which becomes a compute resource is configurable by suppliers.(preferable) Prioritization on allocation of performance of the system to be used, usage time, number of units and so on is possible in provision of systems per user or per group. (preferable)	Suppliers configure conditions for job allocation, user privileges. Preemption or other prioritization schemes are possible upon agreement of suppliers.	Use condition and performance assurance of services by consumers are configurable by suppliers. (necessary) Prioritization of tasks of multiple consumers is possible. (necessary) Tasks that share the same server do not affect one another. (necessary)	Volume of allocatable domain that storage infrastructure provides and policy of availability are freely configurable.	Conditions for allocating requirements in each database system which becomes a database resource are configurable by suppliers. (preferable) Prioritization between multiple database consumers is possible. (optional)
Control	4.3.1-h	2,3	Services include a mechanism to easily perform maintenance	Agent	Maintenance of environment such as deploying applications to compute resources is easy to perform.			Installation/maintenance of PC grid middleware to PC/workstations, to which grid jobs are executed, is possible.(necessary) Maintenance of PC grid middleware is performed automatically. (optional)	Maintenance of environment such as deploying applications to compute resources is easy to perform. (necessary)	Performance of maintenance is managed by each supplier; there is a capability (via portal) for verification of basic common services and service status notification to consumers.	N/A	Maintainable environment in back up, mirroring and RAID mechanism of storage infrastructure is provided without affecting consumers.	N/A
	4.3.1-i	2,3	Configuration change, expansion and destroy of services can be performed according to service levels without halting the whole system		Addition and deletion of compute resources can be performed without halting the whole system.			Addition and deletion of compute resources can be performed without halting the whole system.	Addition and deletion of compute resources can be performed without halting the whole system. (Preferable)	SURAgrid is loosely coupled; there are generally alternative sites in the event service at one site is being modified.	N/A	The followings are possible for storage infrastructure environment without affecting consumers. *Change of configuration, expansion and withdrawal of partial storage *Operation and halting of partial system *Change of system configuration	N/A
	4.3.1-j	1,2,3	Suppliers can easily monitor status of the whole services	Monitoring	Compute resources in operation and wait status of queues are easily recognized.				Compute resources in operation and wait status of queues are easily recognized. (necessary)	System-wide status (SURAgrid as a whole) is viewable through the SURAgrid portal – basic at this time but advanced monitoring tools exist/are emerging.		Function to recognize configuration, usage status and failure of storage infrastructure is provided.	Compute resources in operation and wait status of queues are easily recognized.

Accounting	4.3.2-a	2,3	Usage history of consumers is viewable by suppliers	Logging Monitoring	Accounting information on usage per job can be retrieved by suppliers. (necessary) Statistical information on jobs executed is available to suppliers. (preferable) Usage of service by consumers are recognized by suppliers. (necessary)			Accounting information on usage per job can be retrieved by suppliers. (necessary) Statistical information on jobs executed is available to suppliers. (preferable) Usage of service by consumers are recognized by suppliers. (necessary)	Accounting information on usage per job can be retrieved by suppliers. (necessary) Statistical information on jobs executed is available to suppliers. (preferable) Usage of service by consumers are recognized by suppliers. (necessary)	Common record format has been defined based on Job Usage Record standard currently progressing through the OGF User Record Working Group http://forge.ggf.org/sf/projects/ur-wg). Data gathering and formatting must be implementable using a wide variety of local schedulersis and is under investigation.	Accounting information for task operations by consumers can be retrieved by suppliers. (necessary) Statistical information for tasks performed is available to suppliers. (necessary) Usage volume of services by consumers is recognized by suppliers. (necessary)	Information required for accounting such as usage status of consumers is collected without conflicting security. *Frequency of access, usage rate (volume) *Allocation status of storage domain to consumers	Accounting information on usage per request can be retrieved by suppliers. (necessary) Statistical information on requests executed is available to suppliers. (preferable) Usage of service by consumers is recognized by suppliers. (necessary)
Security	4.3.3-a	3,4	Suppliers and services can be mutually authenticated	Authentication technology	Uniform ID management (authentication, authorization, attribute management) in multiple computer systems is performed.(necessary)	Military Security		Uniform ID management (authentication, authorization, attribute management) in multiple computer systems is performed.(necessary)	Uniform ID management (authentication, authorization, attribute management) over multiple sites is performed. (necessary)	Centralized ID management (uses Globus Grid Security Infrastructure)	Uniform ID management (authentication, authorization, attribute management) is performed. (preferable)	Uniform ID management (authentication, authorization, attribute management) is performed. (preferable)	Uniform ID management (authentication, authorization, attribute management) over multiple database systems is performed. (necessary)
	4.3.3-b	2,3	Confidentiality, completeness and availability of services can be guaranteed	Redundancy Autonomous control	A job manager is made high fault-tolerance by duplication. Job execution is operated with the remaining resources even when a part of computing node is unavailable due to some failure.			It can continue job executions using alternate PCs and workstations in the case where PCs and workstations that handle job executions stop operating due to some failure. (preferable)	A job manager is made high fault-tolerance by duplication. (optional) It can continue job executions using alternate PCs and workstations in the case where PCs and workstations that handle job executions stop operating due to some failure. (preferable)(Optional)	Fault handling, error recovery & reporting; based on local resource supplier implementations; applications can implement mechanisms for availability and completeness across suppliers.	Businesses are not stopped due to some failures.(necessary) It can continue businesses of consumers using alternate services in the case where services stop operating due to some failure. (necessary)	There is a mechanism that a partial failure of storage infrastructure does not affect the entire infrastructure. It possesses a complex system and prompt recovery from system failure is possible. Rollback to the transaction status of a certain period is possible using backups.	N/A
	4.3.3-c	2,3	Confidentiality, completeness and availability of operations related to controls implemented by suppliers to services can guaranteed										
	4.3.3-d	2,3	Confidentiality, completeness and availability of contents generated by operations related to controls implemented by suppliers to services can be guaranteed										
	4.3.3-e	2,3	Logs for controls implemented by suppliers to services can be recorded										
	4.3.3-f	2,3	Confidentiality, completeness and availability of operation logs related to controls implemented by suppliers to services can be guaranteed										
	4.3.3-g	2,3	Suppliers can configure security policy of services	Policy control		Military Security				Local policy and technology components factor first in determination of security policy. Regional grid policy and technonolgy components have secondary influence on implementation.		Suppliers can configure security policies including authentication, authorization, signature, encryption, logging and backups of storage infrastructure in accordance with SLA.	Suppliers can configure data access privileges and others.
Cooperation between Systems	4.4-a	2,3	Ways to establish mutual trust relations are specified	PMA(Policy Management Authority)	N/A			N/A	User certificate issued by Certificate Authority which has set Operational Policy is used. (necessary)	SURAgrid BridgeCA approach provides mechanism for cross-trust relations; higher level of trust being implemented to be consistent with major initaitives in globally-scalable trust for HE (e.g., HEPKI, www.educause.edu/Higher+Education+PKI/931; IGTF, www.igtf.net)	N/A	N/A	N/A
	4.4.-b	2,3	Each other's services are cooperable	Resource reservation	N/A	Expansion of solution across other geographical locations outside of the Navy requirements		N/A	Resource reservation is possible. (preferable)	SURAgrid is being designed and developed to provide grid infrastructure (currently Globus-based) that enables common services to access and use heterogeneous resources across organizational and aministrative domains. Applkication-level cooperation/coordination of resources at separate sites is desirable but not implemented/assisted through centralized tools or services. Metascheduling is likely to be a primary means to implement this. Performance limitations due to WAN connections will also be a significant factor in which applications can benefit.	N/A	N/A	N/A