Open Science Grid

Document Name	OSG Security Plan
Authors	D. Petravick, I. Gaines, R. Cowles, D. Olson, G. Garzogolio, E. Berman, S. Fuess, P. Canal
OSG Document #	389

Version	**Date**	**Comment**
001	September 7, 2006	First draft with the header
002	September 15, 206	First vulnerability prose
003	September 15,2006	Incorporate feedback from security matters meeting.
004	October 2, 2006	Written Vulnerability section
005	October 27	Cut at data operational controls, clipped out the rest of the document.
006	December 5, 2006	Remove section 1, clean up other sections. Add new sections.
007	December 10th 2006	Editing, RP
008	December 11, 2006	Major editing – EB, IG, DLP…
009	December 13, 2006	Changed section 2.3.1.3 to Accountability of Sites, Users, and VO's Changed "OSG Limited" to OSG limited distribution only.
010	Dec 27, 2006	Edits per EB review of Dec 21.

1 OVERVIEW

This document describes the core OSG Security Plan to be accepted by the OSG Executive Board and ratified by the Council. Three types of operating entities collaborate to provide a secure grid computing environment for the OSG: Resource providers (facilities and peer grids), Virtual Organizations, and the OSG Facility itself.

The OSG has two kinds of effort: Assets with a computer realization – for example, its software stack and its software distribution system; And assets that have no such realization – examples are good will and credibility of its facilities, or more generally trust in Grid computing. The scope of the security plan includes the protection of both types of assets.

Integrated cyber security management refers to the notion that each provisioner of an asset is responsible for providing the asset with sound security characteristics and documenting these characteristics. It requires that each provisioner has an identified security role that is defined by the management plan.

2 CONTROLS

The OSG Risk Assessment document describes the risk assessment process addressing site wide threats and mitigations. This security plan for OSG identifies the controls developed in response.

2.1 Risk Assessment and Management

A risk assessment [OSG-488] has been performed on OSG to identify specific risks and mitigations.

2.2 Overview of OSG Security Control Clusters

The security control clusters for OSG are analyzed and described briefly in the Risk Assessment for OSG. In the Security Plan we give more specific details about each of our security controls and discuss the means by which each control will be assessed. The three types of assessment mechanisms used for security controls are Interview (I), Examine (E), and Test (T). As explained in NIST publication 800-53A "Guide for Assessing the Security Controls in Federal Information Systems", these three types of assessment mechanisms can be described as follows:

- **Interview**: this involves asking a selected set of individuals, based on their roles, specific questions about configurations, their actions, etc. For Interview assessments, we indicate who will be interviewed (not a full list of names, but the roles involved, and whether it is all of those individuals or some statistical sample), what questions you will ask them, and where the results are recorded.
- **Examine**: this involves doing an analysis of some existing data sample and recording the results of the analysis. For Examine assessments, we give a pointer to the data set being analyzed, a description of what analysis is done, and the locations of the results of the analysis.
- **Test**: this involves performing some specific test (or fire drill) of the security control to verify that it is performing as expected. For Test assessments we describe the test, the test frequency, and the location where the test results are recorded.

2.3 Management Controls

Management controls include those policies which support and describe the planning, organizing, monitoring, and controlling of OSG core activities.

2.3.1 Integrated Computer Security Management

The overarching security management control is the concept of Integrated Computer Security Management (ISM). The line managers of the OSG are primarily responsible for the computer security aspects of their work. This work is governed by OSG computer Security process. Some degree of expert help is available from the OSG security staff. This philosophy ensures that computer security, like safety, is not an arbitrary set of prescriptive rules imposed from the outside, but rather a part and parcel of all core OSG activities.

Each area of the core OSG has an individual to act as their OSG Security Coordinator. This individual aids the computer security team in transmitting policies and information to the other participants and contributors, brings the concerns from the area to the attention of the security team, and aids the incident response team to identify the locale and response to an incident.

There are clearly defined security roles and responsibilities that are part of the OSG management chain, including the OSG Security Officer (and deputy), the Facility Coordinator (and deputy), the Executive Director (and deputy) and Operations and Software Coordinators. Each resource (and VO) that is registered as a member of the OSG has a Security Contact who serves as a liaison to the computer security team.

The specific controls in this control cluster are:

2.3.1.1 Roles and Responsibilities – Line Organization

The set of individuals as of December 2006 is –

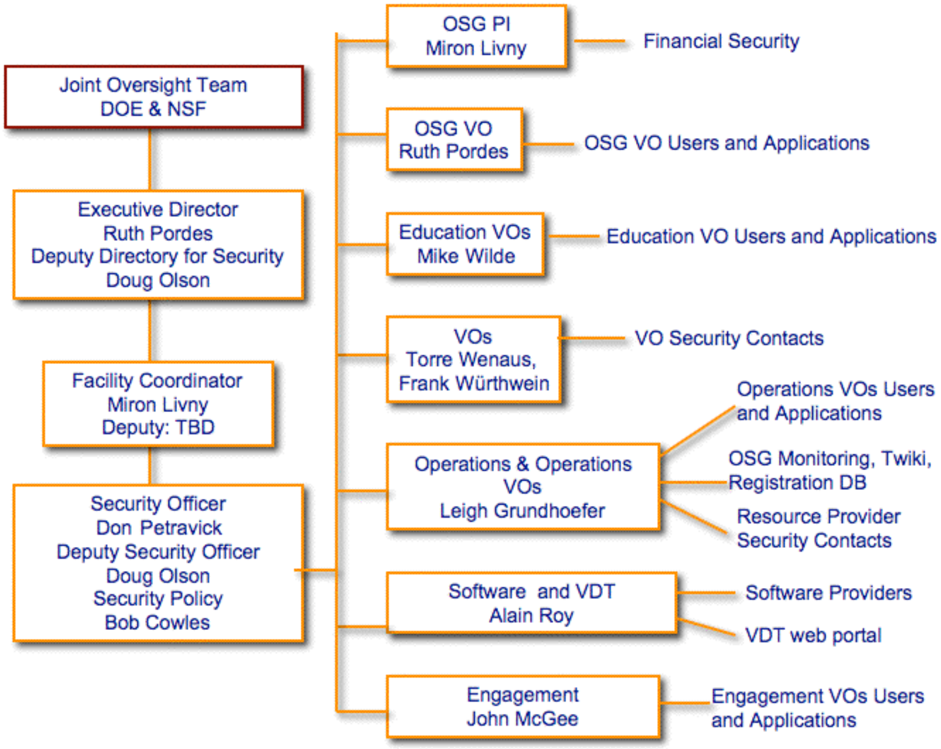

Figure 1: OSG Security Organization

- The OSG Executive Director is responsible for the security of the OSG core assets.
- The OSG Facility Coordinator is responsible for the security of the OSGF assets.

- The OSG Security Officer is responsible for coordinating, monitoring, responding to, and supporting the security of the OSG infrastructure. The Security Office leads the Security Team. The Security Officer promotes the mechanisms of integrated security management and ensures that the OSG Staff know their responsibilities and implement them. The Deputy Security Officer and the OSG Security Policy Officer are members of the Security Team. The Security Officer organizes the assessment of the security controls, drawing upon others as necessary to evaluate the operation of the security office itself.
- The Software Coordinator is a member of the security team. The Software Coordinator is responsible for the security of the VDT assets and as contact for all aspects of security related to the providers of software in the VDT and OSG software caches.
- The Operations Coordinator is a member of the OSG Security Team. The Operations Coordinator is responsible for the security of the core OSG operational services – monitoring, databases etc. – as well as communications with and training of the Resource Security Contacts.
- The Applications Coordinators are members of the OSG Security Team. They are responsible for communicating with and training the Virtual Organization Security Contacts.
- The Operations Coordinator is the security contact for the Operations VOs.
- The Education Coordinator is the security contact for the Education VOs.
- The Engagement Security Contact is the security contact of the Engagement VOs.
- The Executive Director is the security contact of the OSG VO.

Control Assessment: Examination. An examination shall be made every 6 months of the current organizational chart for completeness and accuracy.

2.3.1.2 Awareness for OSG Managers

The OSG Security Office prepares awareness materials describing the Integrated Security Management Responsibilities to the OSG Security awareness program.

Control Assessment: Examination. An annual examination of the awareness materials chart for completeness and accuracy is done.

2.3.1.3 Accountability of Sites, Users, and VO's

The OSG only has management control over the core OSG assets and staff.

Users of OSG resources are given authority to use the OSG through a trust relationship with the managers of the Virtual Organization(s) of which they are a member. In the OSG, the organization responsible for establishing the trust relationship with a user also holds responsibility for the associated management controls for that user, hence Virtual Organizations stand accountable for the actions of their users.

Virtual Organizations face the possibility of losing their privilege to access resources through the OSG if they fail to exercise the requisite controls. The OSG Executive Director can bar a VO from accessing resources by means of the OSG.

Providers of OSG resources must abide by the OSG service AUP. If the AUP is violated, the OSG Executive Director can bar the responsible party from offering services via the OSG.

Control Assessment: Interview. Annual the OSG Operations Coordinator is interviews to determine that the OSG has the capability to bar a user, a VO or a site. Examination. Annually, the OSG awareness materials are examined to see that roles and responsibilities for Accountability are presented.

2.3.2 Security Processes

The OSG runs security processes that assess and enforce its security policies. A good portion of this work consists of preparing and executing its policies, plans, and procedures.

The specific controls in this control cluster are:

2.3.2.1 Computer Security Lifecycle Meeting.

The OSG Security Officer holds periodic meetings. The purpose of the meeting is to discuss operational security matters, to assess the security status of the OSG, and to assess and execute change control of the OSG's security policies, plans, procedures. Agendas for the meeting are prepared, and meeting notes are kept and distributed on the security-discuss-l mailing list.

Control Assessment: Examination. Meeting notes are inspected annually.

2.3.2.2 Briefing of the Executive Board

The OSG Security Officer periodically briefs the OSG Executive Board on the status and plans for OSG security efforts.

Control Assessment: Examination. An examination is done of the minutes of the Executive Board meeting annually.

2.3.2.3 Risk Assessment

The OSG Security Officer maintains a risk assessment document. The document analyzes risks at a high level, and forms the basis for OSG security planning. The analysis shall include:

- Threats to OSG
- OSG vulnerabilities
- OSG security control clusters
- Residual risk to the OSG

The OSG Executive Director approves the risk assessment document and formally accepts the residual risks.

Control Assessment: Examination. The risk assessment is inspected annually for appropriate content and signatures.

2.3.2.4 Policies, Plans and Procedures

The OSG Executive Director approves OSG security policies. OSG policies are normally drafted under the oversight of the OSG Security Officer.   The OSG Security Officer approves OSG wide security plans and procedures.

The OSG Security Officer oversees the ISM based security planning process for OSG processes and services.   OSG services are individually responsible for their own plans and procedures, and approve their own plans. However the OSG Security Officer may determine the adequacy of any such plan.

These documents can be found in the OSG document repository.

Control Assessment: Examination. These documents are inspected annually for appropriate signatures.

2.3.2.5 Self Assessment

Annually, the OSG Security Officer organizes a self assessment of the OSG security program.

Control Assessment: Examination. The date and the results of the review are inspected annually.

2.3.2.6 Peer review

The OSG Executive Director organizes a peer review of OSG security no less frequently than every two years. At the Executive Director's discretion the peer review may be combined with a self assessment.

Control Assessment: Examination. The date and the results of the review are inspected annually.

2.3.3 Trust relationships

Authorization to operate Core Services, VO services, Support Centers, and Resources (Resource Providers) for the Open Science Grid is based on established Trust Relationships. Historically, these trust relationships have been established via several methods:

- Default – the operational body of security and operational plans, policies, and methods will be abided by based on prior collaborative work (typically over an extended period).
- Detailed – there are additional written agreements defining the trust relationships between the parties.

In general, Trust Relationships within the Open Science Grid are granted and revoked by the OSG Executive Director (or their designee) and reviewed by the OSG Executive Board.

OSG maintains the following controls for the set of Trust Relationships:

2.3.3.1 Approval

Participants that operate Core Services, VO services, Support Centers and Resources (Resource Providers) must establish a Trust Relationship via the procedures given in -

http://osg.ivdgl.org/twiki/bin/view/Operations/StandardOperatingProcedures

The procedures define the appropriate level of trust for different categories of relationships.

Control Assessment: Examination. The approval records shall be examined annually.

2.3.3.2 Documentation

All Trust Relationships for the Open Science Grid shall be documented in the OSG registration database.

Control Assessment: Examination. The set of trust relationships shall be compared to the documented list.

2.3.3.3 Clear Roles and Responsibilities

All roles and responsibilities necessary to carry out the duties of the corresponding Trust Relationship shall be documented; said documentation shall list the precise role and/or responsibility and the personnel (by name) who are authorized to perform that function.

Control Assessment: Examination, Test. An examination shall be performed of the documented roles and responsibilities for completeness. A test of a sample of contact mechanisms shall be performed.

2.3.3.4 Review

All Trust Relationships for the Open Science Grid shall be organized by the OSG Executive Director (or their designee) and the date of that review shall be documented. A review shall be performed –

- On a yearly basis
- Or when it is deemed necessary by the OSG Security Office

Control Assessment: Examination. The list of OSG Trust Relationships shall be reviewed for the date of latest trust relationship review.

2.4 Operational Controls

Operational controls are security mechanisms implemented and executed by people as opposed to by machines. They often interact with management controls and may require technical controls to be implemented.

2.4.1 Security Training and Awareness

OSG Core staff has security responsibilities not covered by the OSG VO or User AUP. The principal of Integrated Security Management requires that individuals in particular roles assume computer security responsibilities commensurate with those roles, and that they are provided sufficient training, both formal and informal, to carry out those responsibilities. In addition, the core staff must maintain sufficient awareness to allow them to react to unanticipated situations. Controls in this cluster provide these key individuals with knowledge of their responsibilities and appropriate technical expertise, and ensures that they acknowledge their roles.

The specific controls in this control cluster are:

2.4.1.1 Formal Role-Based Training

OSG organization charts identify those individuals who play key roles in the various components of core OSG. Each of these individuals is required to participate in formal training that ensures they are aware of:

- the responsibilities of their role
- the principles of Integrated Security Management as they are applied to core OSG
- OSG security policies and procedures
- the current grid security threat environment

In addition, many of these key staffers also participate in other external grid projects which provide them additional formal training opportunities.

Control Assessment: Examination. Examination of the training material and records of individuals participating in the training shall be done:

- every 6 months
- when new roles are filled
- when individuals take on a role

2.4.1.2 Regular OSG Core Security Phone Conference

A regular phone conference (currently held weekly on Friday mornings) among core OSG staffers is used to discuss security policies and procedures, review recent incidents or reports of vulnerabilities, and exchange information. This provides the main ongoing tool to provide continuing awareness of security information and status. Minutes are circulated to those with core security responsibilities.

Control Assessment: Examination. Examination of minutes of these meetings shall be done annually.

2.4.1.3 OSG and Other Security Mailing Lists

Core OSG staff are members of dedicated OSG security mailing lists, one for discussion of security issues relevant to OSG, and one for reporting vulnerabilities and security incidents. In addition, key OSG personnel also subscribe to a variety of additional national and international mailing lists dealing with grid security, keeping them up to date and aware.

Control Assessment: Examination. Examination of the membership of these mailing lists and of the list archives shall be done annually.

2.4.1.4 Security Briefings and Discussions at Consortium Meetings

OSG consortium meetings provide an opportunity for face to face meetings and presentations suitable both for core OSG staff and for the larger consortium. Presentation of security issues is a standard agenda item at these meetings, as are smaller parallel session discussions among core OSG security personnel.

Control Assessment: Examination. Examination of presentations at and agendas of OSG Consortium meetings.

2.4.2 Incident Response

It is unrealistic to expect that there will never be a computer security incident within the OSG, in spite of the security controls noted elsewhere in this document. The OSG maintains an Incident Response Plan (Ref: OSG Document #19, "Grid Security Incident Handling and Response Guide", OSG Document #51, "Incident Response Plan for the Open Science Grid", and OSG Document #76, "Security Incident Handling and Response Communications Plan") that sets the guidelines on when an incident is declared and the steps that are followed in response to the incident.

A summary of the controls noted within the Incident Response Plan and the assessments of these controls follows.

2.4.2.1 Incident Planning

The Incident Response Plan document(s) provide(s) the plan under which the OSG responds to a computer security incident. This plan acts as a control by which the effect of an incident is minimized, and lessons learned to minimize the likelihood of subsequent incidents.

Control Assessment: Examination. Examination of the Incident Response Plan documentation is done. The examination shall be performed annually by the OSG Security Officer or designee, with the notes/comments/results distributed to the OSG Security mail list.

2.4.2.2 Incident Discovery and Mandatory Reporting

The Incident Response Plan states:

"Incidents will be discovered through a variety of means including users, system administrators, engineers, and peers; operations center monitoring of infrastructure, services, and resources; and through monitoring of intelligence channels. When an incident is discovered that relates to grid resources, services or identity, it MUST be reported to the local institution incident handling process AND the discovering/reporting party MUST ensure that the incident is reported to the grid security contacts."

The Incident Response Plan specifies the mail list to be used to report the incident, and the information that should be supplied in the report. This mail list is monitored by the OSG Grid Operations Center (GOC).

Control Assessment: Interview, Test. There are several assessments associated with the Incident Reporting mechanism. The education and training of users, operators, and administrators can be assessed by random interview. The interview shall be performed annually by the OSG Security Officer or designee, with the notes/comments/results distributed to the OSG Security mail list. The mail list reporting mechanisms can be assessed by periodically invoking a Test incident from different locations.

2.4.2.3 Invocation of the Incident Response Plan

Upon report of a possible incident to the OSG GOC, a decision to invoke the Incident Response Plan is made by the security officer on duty. The Incident Response Plan references security contact lists maintained by the OSG GOC. The contact lists include site security contact points, VO security contact points, and coordination points with other Grid Operations Centers. These contact mechanisms operate by email and/or phone.

Control Assessment: Examination, Test. There are several assessments associated with the Invocation phase of the Incident Response Plan. The documentation referenced by the GOC to determine if an incident should be declared can be periodically examined. The examination shall be performed annually by the OSG Security Officer or designee, with the notes/comments/results distributed to the OSG Security mail list. A Test incident with specified attributes can be reported to the GOC and the reaction noted. The GOC can initiate a Test incident to be reported to the site, VO, and peer GOCs and the notification chain evaluated.

2.4.2.4 Incident Handling

During an incident the Security Officer reports to the Executive Director.

Once an incident is declared by the GOC and the sites, VOs, and peer GOCs notified, then the response to the incident begins. The incident is analyzed and classified according to a High/Medium/Low scheme specified in the Incident Response Plan. This specification dictates whether a response team leader needs to be specified for the duration of the incident.

The incident responders act to contain the attack, notify other organizations and escalate the matter if appropriate, analyze the attack vector, and respond to the attack with appropriate palliatives and repairs.

The Incident Handling phase of the Incident Response Plan is complex, with many possible variations in required actions. Perhaps the best assessment of the quality of this phase of this control is the evaluation of the actions taken during a real incident. The assessment is coupled with a mandatory incident analysis phase, discussed in the following section.

Control Assessment: Examination. An assessment of the potential to perform adequate Incident Handling can be made by Examination of the raw material that might be needed, including operating system, application, and network logs. Sites, VOs, and GOCs can be randomly and periodically requested to provide such information, with the quality and timeliness of the response evaluated. The examination shall be performed annually by the OSG Security Officer or designee, with the notes/comments/results distributed to the OSG Security mail list.

2.4.2.5 Incident Analysis and Reporting

The incident responders are also charged with collecting evidence and making a complete post-incident analysis and report.

The Incident Response Plan specifies the level to which specific and detailed incident information can be shared outside of a local site, within the OSG, to other peer grids, to supporting agencies, to law enforcement, and to the general public. Safeguards to sensitive and/or privacy-related information must be maintained. The OSG core public disclosures must be handled by the Fermilab public relations office.

Control Assessment: Examination. This control is assessed by examination of the reports created for actual incidents. The examination shall be performed/initiated annually by the OSG Security Officer or designee, with the notes/comments/results distributed to the OSG Security mail list.

2.4.3 Data Integrity

The Security of data has three aspects: Integrity, Availability, and Confidentiality

Integrity is the protection of data from unauthorized change. Availability refers to the ability to access data when it is needed. Confidentiality refers to protection of the data from unintended audiences.

The OSG also provides information classes which define levels of confidentiality. There are four classes, sensitive personal information, restricted data, limited data, and public data. Two methods of dissemination are permitted: Dissemination via document exchange or dissemination via service.

Clearly within OSG, we want to create managerial and operational controls such that an owner can assume the level of trust in an OSG person accessing the data. When passing information outside of the OSG, we need to state the diligences to assess the trustworthiness of the outsider.

Information Classes:

- **Sensitive personal information** has challenging security requirements and is incidental to planning, provisioning or using grid computing. Examples are social security numbers and credit card numbers

- **OSG restricted data** has more restrictive access requirements. Recipients may not disclose information that cannot be discovered elsewhere and the data are available only to individuals white-listed by the data owner.

- **OSG limited data** are used for OSG business purposes. The use covers when there is a need to know, by either core OSG staff or OSG partners. An important expected use case for information is operational information which is not intended to be disseminated publicly, such as the dissemination of vulnerability information between grids. Holders of the data are expected to protect any information which is only available from the OSG.

- **OSG public data** is data that has no privacy requirements. Data that is not explicitly classified is presumed to be public.

OSG Management is able to view all OSG data regardless of information class. The author of a document and the provider of a service are responsible for the categorization of the associated information.

Dissemination Mechanisms:

The OSG makes a distinction between two ways of disseminating information: Dissemination via documents and dissemination via services.

- **Dissemination by document** has the nature of a single transaction, as where a document is passed on from one person to another. The parties reach an understanding of the practices required to protect the confidentiality of the data being exchanged. Documents can be labeled in some way that makes their information classification evident.

- **Dissemination by service** differs from dissemination by document. It allows for automated and ongoing dissemination to current and future data. There is no requirement that a pair of humans are aware of any particular data access transaction

The specific controls in this control cluster are:

2.4.3.1 Integrity and Availability

In core OSG, services holding data are responsible for planning for the integrity and availability of data they hold. Service plans must characterize the maximal expected data loss, and maximal expected unavailability of data. For many services, this should be a statement of backup frequency and retention; a statement of on-call support (e.g. “5x7”), and consideration of the “vandal” threat, as defined in the OSG risk analysis. The OSG Security Officer can state the maximal expected data loss and maximal unavailability for any data in Core OSG.

Control Assessment: Examination.

- A sample of service plans are inspected annually for proper treatment of data integrity and availability.
- Awareness materials are inspected annually for proper representation of roles and responsibilities of service owners.

2.4.3.2 Identification and Handling of Sensitive Personal Data

Sensitive personal information is barred from core OSG systems. The OSG uses member institutions or vendors to handle such data. The OSG Security Officer maintains a list of information in this class, and OSG insiders are made aware of the list. OSG core insiders are aware of the kinds of information belonging to this class, and bring new candidates for the list to the attention of the Security Officer. The list is continuously reviewed in the security lifecycle process.

Control Assessment: Examination, Interview.

- The list of forbidden business data is inspected annually.
- Awareness materials are inspected annually for proper representation of the roles and responsibilities of OSG staff with respect to sensitive personal information.
- A sample of OSG staff is interviewed annually to determine that sensitive personal data are handled according to plan.

2.4.3.3 Identification and Handling of Restricted Data

The author or service owner maintains a list of authorized recipients and defines a purpose for which the information can be used. The recipients are informed that information is to be used for its intended purpose. Recipients agree to use reasonable care holding copies, and to hold only as long as business purposes require. The author evaluates the trustworthiness of each non-OSG core recipient.

Documents are to be marked with the phrase "OSG Restricted – OSG business only -- Do not redistribute" or equivalent.

Dissemination services have a documented plan and implement

- Are able to receive and enforce the author's white-list, by having authentication and authorization mechanisms.
- Services authorize recipients as individuals.
- Services Log access to the data.
- Respond to Termination of rights incidents.

Control Assessment: Examination, Interview.

.

- Awareness materials are inspected annually for proper representation of the roles and responsibilities of OSG staff with respect to restricted information.
- A sample of OSG staff is interviewed annually to determine that restricted data are handled according to plan.

2.4.3.4 Identification and Handling of Limited Distribution Data

The decisions to share data in this class are delegated to persons holding the data. Protection occurs because that people holding this data are made aware of the OSG's confidentiality requirements and are deemed trustworthy. Documents are to be marked with the Phrase "OSG Limited Distribution– OSG Business Only" or language with equivalent meaning by the author. Recipients agree to use reasonable care with their copies. The trustworthiness of OSG core staff and services may be presumed. The disseminator evaluates the trustworthiness of each any non-OSG recipient.

Dissemination services have a documented plan and implement

- The service owner creates awareness within the OSG of the confidentiality of the data it serves.
- The roles and responsibilities for handling OSG Limited data are communicated to non-OSG recipients. The service owner retains these communications, in a way that allows auditing. Non-OSG core recipient's access to the service is for a bounded amount of time, the duration related to risk. Non OSG recipients may be individuals or service owners.
- Access controls on limited data are adequate for, and accessible to incident response.
- Services log access to the data and retain logs for a reasonable amount of time, no less than one year.
- Services are responsive to termination of rights incidents.

Control Assessment: Examination, Interview.

- Awareness materials are inspected annually for proper representation of the roles and responsibilities of OSG staff with respect to limited information.
- A sample of OSG staff is interviewed annually to determine that sensitive data are handled according to plan.

2.4.3.5 Classification By the OSG Security Officer

OSG insiders know of the information classification system, and the responsibilities and diligences associated with it. Based on the policy of ISM, OSG insiders bring cases of suspected misclassification to the attention of the document author, service owner or the OSG Security Officer.

The OSG Security Officer can classify any data in Core OSG, and issue a plan for dealing with extant copies of the data.

Control Assessment: Examination. Awareness materials are inspected annually for proper representation of the roles and responsibilities of OSG staff with respect to handing matters involving potential misclassification of data.

2.4.4 Configuration Management

OSG has two classes of configurations to be managed. First is configuration of services owned and operated by OSG (the core) and the second is the recommended or reference configurations for the services which are downloaded and installed from the OSG software stack. For both of these types of configurations the basic controls that can be employed are; monitoring for unexpected changes, version management, and security review of proposed changes. Since a large part of the security profile of the OSG comes from the configuration of services which are installed on resources not owned by OSG it is important that the documentation provided about how to install and configure those services is included in the scope of "configuration data" considered in this section.

The specific controls in this control cluster are:

2.4.4.1 Monitoring

Monitoring configuration data is a periodic process of scanning configuration data in place, comparing it to a reference set, and sending notification when differences are detected. To the extent possible the scanning process should be conducted on a machine which is distinct from the target so that a compromise of the target does not affect the integrity of the scanning procedure.

Control Assessment: Examination, Test. The primary means to evaluate the effectiveness of monitoring is to check that it detects expected changes to configuration. For this, the person(s) making the authorized changes to configuration should receive the notification of changes having been made from the monitoring procedure. Any authorized change that does not trigger a notification message indicates a failure of the monitoring procedures.

Another means of evaluation is to apply periodic changes to configuration data that trigger a change notification without affecting the functionality of the service. These notifications can be directed to automate processing that can actively detect a missing change notice.

A third means to evaluate the monitoring process is to do a manual audit to verify that the scanned and reference configuration data are correctly compared.

2.4.4.2 Version Control

Configuration management data should be maintained in a version control system that keeps a history of changes with a record of who made a change, when, associated comments, tagging of changes to apply a common label across several related pieces of configuration data (a release tag). An example is to maintain files in a CVS system.

Control Assessment: Examination. The primary means to evaluate version control is to have the version numbers and difference changes appear in the change monitoring notifications sent to service administrators described in the section above. A secondary means to evaluate version control is a manual audit.

2.4.4.3 Security Review of Proposed Changes

This is a procedure where an analysis of the security implications of a proposed change to a service configuration is carried out before the change is applied. The depth and breadth of the security analysis depends on the "significance" of the proposed change. It may be that guidelines need to be developed to help service administrators estimate the "significance" of a change. The procedure for authorizing changes to configuration includes recording a statement about the security implications of the change.

Control Assessment: Examination. Notice of proposed changes should be sent to the security team and include the service administrators evaluation of the security implications of the proposed change. On some occasions a member of the security team or the Security Officer should participate in the security analysis for changes where the "significance" of the change would not normally trigger such additional analysis.

2.4.5 Vulnerability Management

A vulnerability is a flaw in a system which leaves it open for exploitation. All systems possess vulnerabilities. A prime goal of the OSG Security processes is to remove vulnerabilities presenting unacceptable residual risk to the OSG. When the OSG becomes aware of a vulnerability in its core it determines whether the vulnerability presents an unacceptable risk. If the risk is above threshold, the vulnerability is mitigated or eliminated.

The OSG communicates vulnerability information to other parties - without taking on responsibility. Communications may be to VO's, software providers, users, and others when this is deemed to be in the OSG's interest.

The OSG Security Officer keep a vulnerability log, which records vulnerabilities reported via all methods (listed below) and vulnerabilities involved in incidents. The log is used to assess the effectiveness of the vulnerability system.

The specific controls in this control cluster are:

2.4.5.1 General Vulnerability Reporting

Anyone can notify OSG of a vulnerability via security@opensciencegrid.org. Such vulnerability contacts are forwarded to the OSG Security Officer.

Control Assessment: Interview. Annual interview of GOC supervisor, who leads the staff reading the email, is done.

2.4.5.2 Primary Vulnerability Reporting

Because the OSG's organizing principle is Integrated Security Management, entities operating a service or running a process for the OSG have primary responsibility for identifying vulnerabilities.

The OSG requires services and processes to report vulnerabilities that are inconsistent with acceptable residual risk as discussed in the OSG risk analysis to the OSG Security Officer.

Control Assessment: Examination. This control is evaluated annually by inspection of the vulnerability logs.

2.4.5.3 Secondary Vulnerability Awareness

The Security Officer has a secondary responsibility for awareness of vulnerabilities. This provides some measure of depth in vulnerability detection; forms a basis for assessing the primary vulnerability awareness process and provides expertise that may be available to provide vacation-time assistance for the awareness programs that processes and services must run.

Control Assessment: Examination. This control is evaluated annually by inspection of the vulnerability logs.

2.4.5.4 Primary Vulnerability Mitigation

Because the OSG's management controls are based on Integrated Security Management, services and processes work autonomously to mitigate vulnerabilities. The OSG expects the routine elimination of vulnerabilities in a process of routine maintenance services and processes shall notify the OSG Security Officer when a vulnerability inconsistent with acceptable residual risk to the OSG is present in their systems

Control Assessment: Examination. Annually, a sample of services or processes is selected. Their running systems are inspected for vulnerabilities which:

- Should have been reasonably removed by maintenance.
- Would present an unacceptable risk to the OSG.

The record of primary vulnerability reports is inspected to determine if vulnerabilities presenting unacceptable risk to the OSG were reported in a timely fashion.

2.4.5.5 Special Roles of the OSG Security Officer

On occasion, when the OSG Security Officer deems so, the officer may:

- authoritatively determine the risk associated with vulnerabilities,
- articulate and oversee the execution of a vulnerability mitigation plan.

These actions are documented in the security lifecycle process.

Control Assessment: Examination. Inspection of the minutes of the security process meetings is done.

2.4.5.6 Vulnerabilities, Vulnerability Communications and the OSG Security Life-cycle

Selected vulnerabilities are discussed in the security life-cycle process.

Vulnerability Communications are discussed in the security lifecycle process.

Control Assessment: Examination. Vulnerability mitigation is assessed by inspecting the minutes from the computer security lifecycle discussion.

2.4.5.7 Vulnerability Awareness

Information about the OSG Vulnerability awareness plan is included in appropriate OSG awareness materials, and disseminated in the awareness process.

Control Assessment: Examination. Vulnerability awareness is evaluated by inspecting the awareness material relevant this plan annually.

2.4.6 Physical Access Control and Site Management for Production Services.

A series of operational controls are in place to assure that the core OSG resources are only physically accessed by authorized staff.

The specific controls in this control cluster are:

2.4.6.1 Physical Access

All production core OSG systems shall be located in an area which is access protected - either via possession of a physical key, keycard access, or other similar access control method.

Control Assessment: Interview. A sample of core OSG resources shall be verified to be in an access controlled area by interview of the respective administrators.

2.4.6.2 Console Access

Any offered production core OSG service must maintain a security plan that includes protection against unauthorized access from a local console. This plan must consider such items as: default user accounts or passwords; use of live sessions not protected by a screensaver; and booting from a Trojan floppy.

Control Assessment: Examination. A sample of plans will be examined to determine compliance.

2.4.6.3 Network Access

Network login or command access to a production core OSG system shall be permitted only to a client via secure authorization and authentication mechanisms.

Control Assessment: Interview. Administrators will be asked the method for storing their secure authorization and authentication credentials.

2.4.6.4 Network Service Restrictions

All production core OSG systems shall run the absolute minimum set of network services required for their functions.

Control Assessment: Interview. A sample of system administrators for core OSG services will be interviewed to determine that the running network services on their systems are only those services necessary for the system operation.

2.4.6.5 Redundancy

All production core OSG service providers must have a plan describing redundancy or other mechanisms used to maintain service availability in case of operational disruption or emergencies.

Control Assessment: Examination. A sample of plans will be examined to determine compliance.

2.4.6.6 Data Retention

On each production core OSG system, a copy of the system and service logs shall be saved on line for at least 30 days.

Control Assessment: Interview. An interview of a sample of production core OSG system administrators will be done to determine the presence of the logs for the previous 30 days.

2.5 Technical Controls

Technical controls are security mechanisms that are executed by machines. They provide automated protection against unauthorized access and misuse, facilitate detection of security violations, and are used to implement management and operational controls.

2.5.1 Monitoring

The Open Science Grid gathers and publishes information from services and resources on the Grid. This information is used for several different purposes, including monitoring, usage accounting, service discovery, and resource selection..

Most of the information currently available through the OSG monitoring and accounting services consists of real-time or historical records of resource usage. Therefore, this control cluster focuses on the usage of computing, storage, and network. Controls should be available for relevant entities on the grid, including Virtual Organizations (VO), VO-groups, sites, and users.

In general, our focus on resource usage could be complemented by anomaly detection on software services usage (computing node processes table, local and grid job schedulers, data handling services, etc.). Such data could help detect attempts to carry denial of service attacks and would be useful in conjunction with traditional network usage alarms. In principle, it could also help detect malicious dormant processes.

The specific controls in this control cluster are:

2.5.1.1 Recording of Resource Usage Using Accounting Records

The OSG usage accounting infrastructure (Gratia) holds the usage information for each site regarding CPU usage, storage usage and possibly network usage. This information is detailed down to the VO and the individual user or service.

Gratia is a resource usage accounting framework that focuses on reliably collecting accurate usage information. It is composed of several parts: 'probe' which send the information regarding the usage of a particular service, 'collector' which gather the information and 'reporter' which can present the information in different format: graphics, text, attachment, web services.

The resulting information is a comprehensive record of all VOs use of OSG resources. This information can be queried in the context of forensics, anomaly detection, and misconfigurations.

Variance in pattern of use by VOs and individual users is expected. For example a user may have been testing her algorithm for several weeks and finally schedule the run of her analysis over the whole dataset or a VO may have a spike of use in the days leading to a conference. Hence each suspected anomaly should be checked with the individual user or VOs to know whether these changes were expected or not.

Control Assessment: Examination. Examination of the accounting records for comprehensiveness and accuracy will be done.

2.5.2 Access Control for Core OSG Administrators/Users

Access to core OSG resources must be restricted to individuals with proper authentication and authorization.

The specific controls in this control cluster are:

2.5.2.1 Authentication for Privileged Access

Any access to core OSG resources for privileged access must be done using a supported cryptographically strong authentication mechanism that is tied to an individual identity. All such accesses must be logged and the logs retained for at least 30 days. Individuals can be denied access to core OSG resources based on an OSG blacklist maintained by the OSG Security Officer.

Control Assessment: Test. Access will be attempted without valid credentials for a sample of services on a yearly basis.

2.5.2.2 Authorization for Privileged Access

At all times there is a specific limited set of individuals authorized to make a privileged access.

Control Assessment: Examination. An examination of a sample of users will be made on a yearly basis.

2.5.2.3 Non-privileged User Access

Core OSG services need to be widely available. There are in general no restrictions on the authentication of non-privileged access to these services. However, great care must be taken to ensure that non-privileged access cannot be elevated to privileged access. This implies great care in configuration management, patching, administration etc.

Control Assessment: Interview. An interview of a sample of service administrators will be done to verify the control.

2.5.3 Scanning

OSG core services participate in the security plan and the associated security infrastructure. The security infrastructure provides common tools for local administrators to execute their responsibilities with respect to the security plan. This includes tools to enable the local administrator to perform site vulnerability and intrusion detection scans on their local systems. Scanning is done to enable timely detection of –

- Vulnerabilities – to identify and remove the vulnerabilities before a risk occurs
- Intrusions - to identify and respond to risks that have occurred allowing identification and removal of the associated vulnerability

When a critical vulnerability is declared, the site vulnerability scanning programs will be augmented in order to detect any devices that are sensitive to the declared vulnerability.

The specific controls in this control cluster are:

2.5.3.1 Web Service Vulnerability Scanning

A common tool will be provided to allow web service administrators to perform vulnerability scanning on their locally provided web services. It is the responsibility of the local web service administrators to be knowledgeable in the interpretation of the scanning reports. Assistance is available from the OSG security office when needed. These web service vulnerability scans will be performed when any of the following occur –

- The last scan is 6 months old.
- When the operating system is upgraded.
- When the web services application is upgraded.
- When infrastructure (e.g. cgi scripts) is changed.

The scanning results should be examined and any identified vulnerabilities fixed.

Control Assessment: Examination. Examination of vulnerability scanning reports and logs will be done after each scan.

2.5.3.2 Web Intrusion Detection Scanning

A common tool is provided to allow web service administrators to perform web intrusion detection on their locally provided web content. It is the responsibility of the local web service administrators to be knowledgeable in the interpretation of the intrusion detection reports. Assistance is available from the OSG security office when needed. These web intrusion detection scans should be performed –

- every 15 minutes for critical services
- once a day for other highly visible content

Any detected intrusion will result in immediate notification of the local system administrator (via paging for example). The system administrator will perform an immediate assessment, with a minimum of intervention, to determine if the incident is the result of unauthorized intrusion and follow the OSG policy for alerting the OSG incident response team. Care will be maintained to perturb the compromised system as little as possible.

Control Assessment: Examination. Examination of the intrusion detection reports and logs is done -

- When an intrusion is detected
- Every 6 months to insure the detection is examining the correct content

2.5.3.3 Vulnerability Scanning

Local system administrators institute a policy of vulnerability scanning on machines that offer OSG core services. Particularly urgent security threats are classed as critical vulnerabilities which must be immediately remediated. Periodic scans are performed to search for these vulnerabilities, with new detectors being added to the scan as new critical vulnerabilities are announced. The results of this scan are used to warn system administrators that their machines are vulnerable.

Control Assessment: Examination. This control is assessed by examination of scanning records.

3 References

NIST Documents http://csrc.nist.gov/publications/nistpubs/index.html
The docs most likely to be of use are

800-53	security controls
800-30	risk management
800-18	security plans

OSG documents are numbered and kept in a controlled document repository at –

http://osg-docdb.opensciencegrid.org/cgi-bin/DocumentDatabase/

Some documents are restricted to members of the OSG Consortium, members of the OSG staff, and/or security teams.