

|  |  |
| --- | --- |
| **Document Name** | Computer Security Risk Assessment for Core OSG |
| **Authors** | Mine Altunay, Alain Roy, Dan Yocum, Don Petravick, Doug Olson, Leigh Grundhoefer, Irwin Gaines, Philippe Canal, Robert Cowles, Robert Gardner, Ruth Pordes, Vikram Andem, Kevin Hill |
| **OSG Document #** |  |

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Comment** |
| 001 | June 17, 2006 | First draft with the header |
| 002 | June 17, 2006 | After phone conf, rough notes |
| 003 | June 26, 2006 | June 28th Meeting |
| 004 | July 11, 2006 | Risk Mitigation contents |
| 005 | August 1,2006 | Identified core Risks for core components |
| 006 | August 8,2006 | Presented the core risks for core components with grading |
| 007 | August 14,2006 | Added section “Appendix: Detail explanation of risks identified and mitigations” |
| 008 | August 15,2006 | Added Trust relationship processes section |
| 009 | August 17,2006 | Final edits for first version |
| 010 | May 14, 2009 | Updated out-of-date information and the risk grades |
| 011 | December 11, 2014 | Annual update |
| 012 | December 15, 2015 | Annual update |

# IDENTIFICATION

# System Name/Title

The Open Science Grid is a nationwide distributed computing infrastructure that supports scientific computing via an open collaboration of science researchers, software developers, and computing, storage and network providers.

The OSG does not provide computing centers; rather it facilitates access to computing and storage facilities and thus the researcher’s use of the facilities. It does this by providing a number of core services, a common software stack, and training and education.

# Responsible Organization

The Open Science Grid Consortium goals are to support the use of and operate a secure fabric of services providing access to more than 100 computing and storage sites; distribute and support a robust, evolving middleware stack for use on the distributed resources; education, outreach and training activities to enable new participants in the use and support of Grid infrastructures; and usage and extensions to the fabric of services driven by the science needs of the stakeholders.

In particular, the OSG is committed to deliver production distributed infrastructure for the US LHC experiment and for the LIGO data grid core infrastructure components, as well as for other scientific research communities—including the STAR experiment, the Tevatron Run II and Astrophysics experiments. While currently the majority of the stakeholders are physics and computer science computing facility organizations and research collaborations, OSG is strongly committed to engage a broader set of communities. OSG priorities include interfacing and interoperating with other grid infrastructures — especially XSEDE in the US, the EGI in Europe and a diverse set of campus and regional grids.

***The Open Science Grid Consortium governance is described in the by-laws and management plan. The program of work for OSG is executed by an Executive Team and Executive Board reporting to the Consortium Council.***

The organization of the program of work for the OSG is described in its project management plan. The Open Science Grid Executive Director is responsible for the management of the project. The Technical Director guides the technical direction of the OSG as the technologies that are used to implement the OSG services and middleware change and the stakeholder needs evolve. The Security Officer coordinates and monitors the operational security of the OSG infrastructure. The Operations Coordinator coordinates, monitors and supports the operation and running of the OSG infrastructure. The software coordinator coordinates the packaging, distribution, and support of OSG infrastructure middleware. The Executive Director takes decisions to the OSG Council for Endorsement.

Resources made accessible through the OSG infrastructure are registered with the Grid Operations Center (GOC). Similarly new user groups (VOs) register with the GOC. Each VO and/or resource is supported by a Support Center and has an identified Security Contact. Support Centers may support multiple sites, resources, services and VOs.

# Information and Security Contact(s)

|  |  |  |  |
| --- | --- | --- | --- |
| Title | **Name** | **Email** | **Telephone** |
| Executive Director | Lothar Bauerdick | bauerdick@fnal.gov | (630) 840 6804 |
| Technical Director | Miron Livny | miron@cs.wisc.edu | (608) 262-0856 |
| Security Officer | Mine Altunay | maltunay@fnal.gov | (630) 840-6490 |
| Operations Coordinator | Rob Quick | rquick@iupui.edu | (317) 274-5260 |
| Software Coordinator | Tim Cartwright | cat@cs.wisc.edu | (608) 262-4002 |

*Table 1: Information and Security Contacts*

# System Operational Status

The OSG is in the Operational phase of its life cycle.

# Information Gathering Technique

This assessment is done using interviews and document review.

# General Description/Purpose

The OSG is a collection of assets and processes, listed below:

**Software stacks and release process**:

OSG provides a software stack that is conceptually composed of three pieces:

1. The Virtual Data Toolkit (VDT).
2. Configuration software and data. For example, this includes the list of VOMS servers used for authorizing users in OSG.

There is a wide variety of software including job management software, data management software, authentication and authorization mechanisms, web service containers, and various utilities.

OSG software is stored on web servers at University of Wisconsin (VDT team) and Indiana University (GOC). Usually the software is pre-compiled. Access to the complete software stack is unrestricted, and no authorization is required, nor is membership in the OSG. However, OSG will only support the software used on the registered OSG resources and VOs.

OSG software stack has been developed by a wide variety of individuals and institutions. The VDT and OSG both have release processes for building, packaging, and testing the software. OSG software releases come in two varieties: Integration and Production. Integration software releases are more frequent and deployed on a smaller set of sites for testing. Production software releases are less frequent and are installed on OSG sites that expect to do production for end users.

Both the VDT and OSG have processes to release incremental updates of the software as needed for high priority fixes, particularly security updates.

Both the VDT and OSG have pre-release automated testing mechanisms to catch problems before users experience them.

**Communications and Web presence process:**

The primary and general OSG presence consists of production information repositories; some utilize open source content management systems, such as twiki.

The OSG productions web presence, at <http://www.opensciencegrid.org> has a mix of static and dynamic content. Within the OSG there are many groups and activities that require a global location for meeting minutes, publication of reports and plans, and an information repository, which is easily editable by each OSG contributor. To meet this need the Twiki web environment has been deployed and is available at https://twiki.grid.iu.edu/twiki/bin/view/Main/WebHome.

Another area where web repositories are present is the software repositories which are deployed and maintained for the purpose of software distribution and the installation of OSG software components. There are three separate services. The first is the VDT site at <http://vdt.cs.wisc.edu/vdt_cache> residing with the VDT team at the University of Wisconsin. The remaining two are deployed on the same server at IU. The Production OSG cache is at <http://software.grid.iu.edu/pacman> and the Integration cache is at <http://software.grid.iu.edu/itb>. The OSG distributes its web presences among several sites. (At the time of this writing, IU, UWisc and FNAL)

OSG also distributes applications and data via the CVMFS distributed file system, maintained at the GOC. CVMFS uses web servers and a network of cache servers to provide a read-only file system, which can be used to publish application software or small data or configuration files, which will be available to jobs running on worker nodes with the CVMFS client software installed.

The OSG provides coordinating communications via a multitude of mailing lists. The mail lists range from open – anybody may subscribe with an open archive, to closed and un-archived. The mail list service is provided by FNAL.

The OSG provides a trouble ticket system that has restricted login access. Weekly reports are generated from the ticket information.

The VDT team maintains another ticketing system, <http://vdt.cs.wisc.edu/rt/>, that only contains issues related to VDT software stack, such as software bugs. GOC tickets are general in nature that they cover all trouble issues from installation to production problems. Software specific GOC tickets are forwarded to VDT system for resolution

**VO/End User process:**

The OSG has an interest that OSG users abide by the OSG AUP. It does this by ensuring that its VOs AUPs are no more permissive than the OSG AUP, and relying on the VOs to enforce their AUPs. Therefore, VOs are primarily responsible for enforcing the OSG AUP. VOs are the mechanism for interacting with end users.

In keeping with the OSG interest in supporting the grid infrastructure as reliable, usable and secure, OSG provides assistance with digital identity management for people and services. The deployed infrastructure requires X509 certificates as the identity token for all entities and the OSG operates a Registration Authority (RA) in conjunction with Digicert-grid CA (operated by Digicert) to provide users and service providers with X509 certificates of sufficient quality to be acceptable by the resource providers in OSG and partner grid infrastructures around the world.

The OSG RA:

* Authorizes personnel in the VOs to act as agents for the CA to perform authentication procedures for issuance and revocation of certificates
* Provides education and training for agents
* Provides some user support and problem solving activities related to using the certificates with the OSG infrastructure
* Ensures that suitable logging information of certificate-related actions are maintained by the OSG RA or by the agents in the VOs

The primary aspects of certificate quality to be maintained are to ensure that the subject name (DN) is issued only to a valid owner of the DN, so that the same DN is not issued to different people (owners for service certificates).

# OSG hosted VO process:

The core OSG hosts a number of VOs such as MIS, OSG, and OSGEDU VOs. Occasionally a support center and accompanying VO request that they place their membership information on an OSG hosted VO membership service. When granted, the Support Center and VO admin maintain control and authority toward all policies related to the VO membership service.

OSG also hosts VOs for its core staff access. The VOs for core OSG staff are fully featured and used for various OSG purposes. The OSG core VOs are given no special privileges at the sites.

**OSG Validation Monitoring and Accounting Process:**

OSG Software contains several components which are installed as part of the base functional set which is used either by executing a daemon on the installed compute element or run from a cron type entry on the installed compute element. Other validation software is run from off site using the default (fork) job-manager that is a standard piece of the Grid Middleware. Such jobs have no special privileges. The collected information is returned to the services that are part of the OSG core facility. The information is used for OSG operational purposes, and is protected on a best effort basis. The information has to be accurate enough to meet OSG’s operational needs.

# Inter-grid operation process:

The OSG seeks to interoperate with XSEDE and is part of the WLCG, while preserving its security. The OSG deploys a BDII. This allows the WLCG to see OSG resources.

The OSG trusts the WLCG VOs and Users. WLCG VOs are registered with OSG in the usual way. However, their users sign a WLCG AUP, which is the same as the OSG AUP and is also trusted. From the OSG perspective WLCG VOs are not “special”.

# Security Processes:

Primarily, the OSG implements integrated security management, the notion that primary responsibility for security rests with entities performing processes for the OSG.

Within this context the security process leads the overall security effort with the OSG facility.

Elements of the process include:

* Provides an overall security plan and process for the OSG.
* Assists process owners with security matters.
* Provides for incident response.
* Provides in-house assessment of OSG security.
* Speaks for the OSG on security matters.
* Reports internally about OSG security matters.

The planning and incident response functions have data (for example, plans and mailing lists) whose security must be planned for. The in-house assessment of security assess the security of OSG services. The assessment results contain data that must be secured.

**Trust Relationship Process:**

OSG systems can be secure when all of the various parties (OSG sites managing computing and storage facilities, OSG member virtual organizations managing users, and core OSG services) are operating in a secure manner that can be relied upon by other parties.

Much of the security functionality belongs to the sites and the VOs, and cannot be controlled by core OSG staff or services. However, OSG maintains and manages a set of trust relationships, defined by signed agreements, among these parties.

OSG will be responsible for creating and maintaining drafts of the trust agreements, and creating and managing a process whereby the trust agreements will be signed and distributed to the various OSG parties so that the expected behavior is understood by all concerned.

# METHODOLOGY

The methodology we use for our risk assessments is as follows. A risk is a function of a threat (someone knocking on our door) and a vulnerability (an insufficiently protected or unlocked door). A “vulnerability without a corresponding threat”, or a “threat that cannot exploit a vulnerability”, does not present a risk. Each risk is associated with an impact: we have adapted the qualitative assessment to conduct the impact analysis to prioritize the risks and identify the areas for immediate improvement in addressing the vulnerabilities. The set of security controls are designed to mitigate the risks so that the expected level of impact is sufficiently low to be accepted as a residual risk. The residual risks that cannot be dealt with security controls may be dealt with in contingency plans.

In this document we will outline our current perception of the threat environment, describe the potential vulnerabilities in OSG, and discuss the security controls in place to mitigate the risks that these threats and vulnerabilities present. We will assess what residual risks remain after the imposition of these controls.

Two other points should be cited:

1) This risk assessment is not static, since the threat environment is constantly changing and evolving. This risk assessment document must be revisited and updated regularly, at a minimum on an annual basis.

2) An additional component of the risk assessment is the evaluation of the risks associated with OSG processes. This is performed by the process owners and includes an inventory of the services and applications used by the processes and an evaluation of the security controls for the OSG processes.

# Threat Source Identification, Motivation and Threat Actions

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised.

We identify the following threat sources based on their motivations:

1. Careless or uninformed authorized person
2. Squatter (unauthorized persons who use our resources, but not at an economically significant level)
3. Vandals (web page defacers, data destroyers, malicious code, vandalize reputation )
4. Thief (take services, money, things of value)
5. Author who writes malware
6. Spy
7. Alarmist

In more detail, these threats are represented by the following examples:

1. Authorized person who does not abide by the OSG AUP, or makes a mistake and causes harm to the operational grid or posts improper content on OSG web sites (Careless person)
2. Resource exploiter. The ensemble computing power of the OSG is quite large; Misuse of the OSG might seem attractive to a variety of groups. The threats include denial of service and a very large indirect threat of public embarrassment because of improper use of resources (Thief)
3. Disgruntled insider. A present or former insider or user, with the combination of computer skills, knowledge of our systems and operations, and a perceived grievance, and lacking in normal psychological inhibitions to destructive behavior. (Vandal or a Thief).
4. Script Kiddie. These persons use scripts they easily download from the network and exhibit adolescent behavior. In general, motivations are divided between keeping score and boasting to friends and using high capacity computers and network links for other attacks. (Vandal, Squatter)

1. Skilled crackers. There exist a number of extremely talented and skilled break-in “artists”. These people may be attracted to the novel technology in the OSG. (Vandal, Squatter, Spy, malware author)
2. Loud person who forgets that risk requires both a threat and vulnerability. Internal over-reaction can effectively cause a denial of service on our own operations and restrict our ability to do our science mission in the open academic environment it requires. (Alarmist)

# Vulnerability Identification

Our vulnerabilities fall into the following categories,.  
  
I. Reliance on third parties for the services our processes rely on. (Relying on non- OSG entities for platforms, etc) – We cannot directly manage their processes and diligence.  
  
Risks associated with these vulnerabilities are mitigated by controls involving formal agreements between the parties mandating certain procedures and behaviors, and by technical controls that limit the impact of any violation of these agreements.  
  
II. Improper or inappropriate OSG core staff actions (basis for assessing and controlling Behavior, like diligence.)  
  
Risks associated with these vulnerabilities are mitigated by controls involving training of personnel to minimize these actions, and technical controls that limit the impact of these actions.  
  
III. Improper or inappropriate OSG user actions.  
  
Risks associated with these vulnerabilities are mitigated by controls  involving training of personnel to minimize these actions, and technical controls that limit the impact of these actions.  
  
IV. Remote Access  
   The OSG Core activities are conducted on the open public internet.   
   i. Sniffing of passwords   
   ii. Hijacking   
   iii. Denial of Service exposure on an open network  
  
Risks associated with these vulnerabilities are mitigated by controls involving authentication and authorization to limit remote access and network controls to limit unauthorized and improper connections.  
  
V. Exploits latent in vulnerable software.   
   i.    OS holes.  
   ii.   Application security holes  
   iii.  Lack of protection against malicious code (viruses, worms, trojans, etc.) introduced through mail enclosures, browser web accesses involving Java, ActiveX, etc  
  
Risks associated with these vulnerabilities are mitigated by controls involving patching and system configuration, scanning for vulnerabilities, virus scanning, and network access limitations.  
  
VI. Physical access  
  
Certain OSG assets could be vulnerable if an intruder obtains physical access to computing and networking equipment.  
  
Risks associated with these vulnerabilities are mitigated by controls that regulate and limit such physical access.

# IMPACT Analysis

VOs rely on the OSG as part of their computational infrastructure. The impact of a computer security event primarily derives from its consequences seen by the OSG VO’s and Sites. Other sources of impact are the draining of resources associated with even trivia incident response and damage to the OSG’s reputation.

The impact of a risk is considered in terms of damage to individuals, loss of property, or resultant downtime of services and processes.

A security event has LOW impact if it occurs less than 10 times per year and does not disrupt the perception of the OSG as a computational facility that can be relied on AND no single occurrence of the event disables service availability for more than two days.

A security event has MODERATE impact if it occurs less than 20 times/ year disables service availability for up to a week.

A security event has SEVERE impact if it occurs 20 or more times/year or disables service availability for more than a week.

# Control Analysis

The OSG implements Management, Operational and Technical Security Controls.

The controls in each of these classes are organized into families. An overview of these control families is provided below:

## **6.1. Management Controls**:

#### 6.1.1 Integrated Security Management

Integrated cyber security management refers to the notion that each custodian of an asset is responsible for providing the asset with sound security characteristics and documenting these characteristics.

#### 6.1.2 Security Processes

The OSG supports integrated cyber security management by defining basic processes, providing common methods and services. These processes include:

* Security process life cycle
* Self assessment/peer review
* Computer security roles and responsibilities
* Identification of critical single points of failure.

6.1.3 Trust relationships

OSG members work with each other by agreements. Controls on the trust relationships for OSG family provide confidence that these parities will mutually operate securely. The needs for security change over time and parties they provide for security in the matters they in turn delegate, and for mutual auditing of security.

## **6.2. Operational Controls:**

### 6.2.1 Security Training and Awareness

OSG Core staff has security responsibilities not covered by the OSG VO or User AUP.

The principal of Integrated Safety management provides that individuals assume computer security responsibilities appropriate to their roles. Controls in this family provide that this information is composed, communicated and understood.

6.2.2 Incident Response

The OSG provides for an incident response plan covering all aspects of its core. The OSG provides for Mandatory Incident, reporting, distributed organized response, maintenance and assessment of the response organization.

6.2.3 Data Integrity

Controls in this family provide that OSG data receive appropriate care for its availability, integrity and privacy. This family of controls includes an information classification system for OSG, and provides for system backup and recovery.

6.2.4 Configuration Management

This family provides for Configuration Baselines for OSG-prescribed software and configuration guidelines for other systems. The Configuration management family provides for processes that update software quickly enough that the residual risk is acceptable.

6.2.5 Vulnerability Identification

This control family provides for continuous assessment of software in a baseline for vulnerabilities, and the timely deployment of mitigations if the presents unacceptable risk.

6.2.6 Physical access control and site management

This control family provides for sufficient physical controls over tangible assets.

### 6.3. Technical Controls:

#### 6.3.1 Monitoring

The OSG has operational processes that monitor and assess the general health and status of the OSG. These processes also necessarily assess the security of the OSG and are coupled to the security process.

### 6.3.2 Control of administrators/user

### These controls provide the technical means to enumerate OSG core staff and provide authentication and authorization that are consistent with acceptable residual risk.

### 6.3.3 Scanning

Controls in the scanning family specifically assess the security of the OSG services. Scanning includes comparison to the baselines.

### VII. RISK MITIGATIONS AND RESIDUAL RISK LEVEL

The integration and use of new technologies always involves risk. The goal of OSG risk assessment and mitigation is to understand the risks inherent to an integration project and to develop strategies to effectively manage the project in a manner that mitigates the associated risks. The elimination of all risk in the core OSG is usually impractical or close to impossible. Therefore, it is the responsibility of management to use the most cost effective approach and implement the most appropriate controls to decrease OSG risk to an acceptable level, with minimal adverse impact on the agency’s resources and mission

In this section we consider the various risks associated with the identified threats and vulnerabilities, and show how they are mitigated by the variety of security controls which constitute our defense in depth. We will not indicate every instance of mitigation (for example, protocol restrictions at the site border provide some protection against almost all types of risks). Instead we will indicate which security controls provide the main protections against particular risks, recognizing that many other components of our defense in depth also provide additional mitigation.

In particular, it should be pointed out that the fundamental security controls of integrated security management, network management, and incident handling provide mitigations for almost all types of risks. Responding to incidents and learning from them how the threat environment is evolving allows us to keep our mitigations up to date to counteract the latest threats.

The risks in the OSG are characterized by the probability of occurrence and the impact if they do occur. Each of the potential threats and vulnerabilities listed above are considered as they might

apply to each of the various components of the core OSG. Each resultant risk is then characterized in the below table. Occurrences are rated LOW if it happens less than 10 times per year; MEDIUM if it happens up to several times per month; and HIGH if it occurs more than once per week.

Using the ratings for occurrence and Impact we can then determine a current grading for each risk that in turn provides a measure of the OSG risk exposure at the time of the evaluation

*Table 3* provides the OSG method for calculating a grading for each risk based upon the combination of the occurrence and Impact ratings.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Occurrence** | **Impact** | | | |
|  | low | medium | high |
| low | E | D | C |
| medium | D | C | B |
| high | C | B | A |

*Table 3: OSG Risk matrix for grading risks*

*Key:*

|  |  |
| --- | --- |
| **Change in Grade since the last assessment** | |
| **NEW** | New risk (Just identified) |
| - | NO change to Grade of the risk since last assessment |
|  | Grade has been decreased since last assessment |
|  | Grade has been increased since last assessment |

So what this means in practice is:

**How OSG will manage or 'treat' the Risks?**

Risk mitigation strategies reduce the chance that a risk will be realized and/or reduce the Severity of a risk if it is realized**.** In OSGGrade C Risks should be continually monitored and have planned mitigation strategies ready to be implemented if appropriate. These plans need to be recorded in OSG *Risk Management Table*.

There are three broad types of risk mitigation strategies in OSG:

* **Avoid** the specific threat, usually by eliminating the root cause.
* **Mitigate** the specific threat by reducing the expected impact of the risk, or by reducing the probability of its occurrence.
* **Manage** (accept) the consequences of the risk.

For each action in the *Risk Management Table*, it is necessary to specify:

* Who will be responsible for implementing each action?
* When the action must be implemented?
* What are the costs associated with each action (if applicable)?

*Table 4* presents Risk management table for the OSG with the mitigation strategies for the risks mentioned in the *appendix A*

*Table 4: OSG Risk Management Table*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No** | **Description of Risk** | **O** | **I** | **G** | **Status** | **Date** |
| 1 | Disclosure of sensitive security information: incident reports, vulnerability tickets, comm. on incident-discuss email lists | M | H | B |  | 6/6/15 |
| 2 | Subversion of security process | L | L | E | **-** | 6/6/15 |
| 3 | Withholding security notification: such as attack alerts, patches | M | M | C | **-** | 6/6/15 |
| 4 | CVMFS exploited to provide corrupt software | L | H | C | - | 6/6/15 |
| 5 | Software auto-update feature exploited to provide corrupt software | L | H | C | **-** | 6/6/15 |
| 6 | Software in the stack has flaws that could be exploited in deployments | L | M | D | **** | 6/6/15 |
| 7 | Corruption of the software stack by authorized person | L | H | C |  | 6/6/15 |
| 8 | Corruption of software stack by outsider | L | H | C | **** | 6/6/15 |
| 9 | Release process is unavailable, but is needed by the security process | L | M | D | **-** | 6/6/15 |
| 10 | Users unaware of OSG AUP, may violate policies out of ignorance, may fail to report security incidents | M | M | C |  | 6/6/15 |
| 11 | User violates AUP willfully and circumvents security controls to access resources | L | M | D | **-** | 6/6/15 |
| 12 | VO has incorrect user information in VOMS server, may provide hole for malicious user to exploit | L | M | D | **-** | 6/6/15 |
| 13 | VO insider authorizing mis-use of resources | L | H | C | **** | 6/6/15 |
| 14 | OSG staff manipulating OSG-hosted VO authorization | L | H | C | **** | 6/6/15 |
| 15 | OSG staff publicizing false information about User Process | L | M | D |  | 6/6/15 |
| 16 | Careless 3rd party mistakenly granting agent privilege to incorrect person, possible impact on OSG since all agents of DOE Grids have privilege for all certificates | L | M | D | **-** | 8/14/15 |
| 17 | Malicious authorization of agent privilege for illegitimate person, by impersonating a valid RA, malicious agent can revoke all certificates causing DOS | L | H | C | **-** | 8/14/15 |
| 18 | Hack into CA website and perform malicious actions, install fake agents, revoke certificates, cause DOS | L | H | C | **-** | 8/14/15 |
| 19 | Careless or incomplete training for agents, agents do not follow correct procedures, potential exploit for malicious user if combined with exploit of VOMS server | L | M | D | **-** | 8/14/15 |
| 20 | Malicious mis-information provided for agent training, like 10 but implies intent to exploit | L | H | C | **** | 8/14/15 |
| 21 | Careless or incomplete user training for PKI, user may not handle private key correctly | M | M | C |  | 8/14/15 |
| 22 | Accidental corruption of RA process audit log, leads to incomplete of lack of audit ability | L | L | E | **-** | 8/14/15 |
| 23 | Intentional corruption of RA process audit log to disguise audit trail, potential privacy compromise | L | M | D | **** | 8/14/15 |
| 24 | Malicious disruption of PMA process, potential damage to credibility of PKI, potential delays in handling authentication and revocation requests | L | H | C | **** | 8/14/15 |
| 25 | Careless or incomplete identity vetting in certificate process, potential exploit for malicious user can permit abuse of resources if identity theft occurs | L | M | D | **-** | 8/14/15 |
| 26 | Malicious abuse of identity vetting, insider participation in identity theft by agents | L | H | C | **** | 8/14/15 |
| 27 | Careless management of CA services, potential DOS caused by CRL lack of availability | L | H | C | **-** | 8/14/15 |
| 28 | Loss of CA integrity due to physical access to CA, potential compromise of CA key and need for re-issuing thousands of certificates | L | H | C | **-** | 8/14/15 |
| 29 | Reliance on third parties to ensure user compliance with OSG AUP(Some users unaware of AUP, may violate policies out of ignorance, may fail to report security incidents) | M | L | D | **-** | 8/14/15 |
| 30 | User carelessness violation of AUP | M | L | D | **-** | 8/14/15 |
| 31 | User willful violation of AUP (User circumvents security controls and exercises unauthorized use of resources) | L | M | D | **-** | 8/14/15 |
| 32 | OSG misrepresenting user AUP compliance data (AUP verification audited in 2014) | L | L | E | **-** | 8/14/15 |
| 33 | VO careless violation of AUP (Errors in VOMS, incorrect info for users, May provide hole for malicious user to exploit) | L | M | D |  | 8/14/15 |
| 34 | VO malicious violation of AUP (VO mis-representing purpose of resource usage, VO insider authorizing mis-use of resources, embarrassment to OSG) | L | M | D | **-** | 8/14/15 |
| 35 | OSG staff careless violation of AUP for OSG-hosted VOs | L | L | E | **-** | 6/6/15 |
| 36 | VO malicious software exploit | L | H | C | **** | 6/6/15 |
| 37 | VO physical access, applies to OSG-hosted VOs (OSG staff vandal interfering with hosted-VO authZ) | L | M | D | **-** | 6/6/15 |
| 38 | VO OSG staff alarmist – for OSG-hosted VOs (OSG staff claiming incorrectly that OSG-hosted VO violates AUP and abuses resources. Potential embarrassment for OSG) | L | L | E | **-** | 6/6/15 |
| 39 | Third party careless agent authorization (CA managers mistake)Risk of mistaken agent authorization, potential damage to trust of grid PKI if it happens too often | L | H | C | **** | 6/6/15 |
| 40 | Third party agent authorization (impersonate OSG RA to install malicious agent) Risk that malicious agent is authorized via impersonation of legit RA, immediate impact is low, potential threat to PKI trust, potential DoS by revocation of certificates | L | H | C | **-** | 6/6/15 |
| 41 | OSG RA careless authZ of agent (Accidental authorization of agent that does not want agent access, low impact unless agent also exploits VOMS) | L | H | C | **** | 6/6/15 |
| 42 | Software exploit agent authZ (CA managers issue) | L | H | C | **-** | 6/6/15 |
| 43 | Agent authZ physical access (CA managers issue) Malicious physical access to CA machines | L | H | C | **-** | 6/6/15 |
| 44 | OSG staff alarmist – removal of agent authZ (Agent authorization is removed due to incorrect OSG staff complaints , may delay some certificate requests) | L | L | E | **-** | 6/6/15 |
| 45 | 3rd party careless agent training (Agents in VOs give incorrect info to other agents, requests handled incorrectly) | L | M | D | **** | 6/6/15 |
| 46 | 3rd party malicious agent training (Intent to give agents incorrect instructions, low impact unless malicious person also has access to VOMS) | L | L | E | **-** | 6/6/15 |
| 47 | OSG staff careless agent training (OSG RA provides incorrect training info to agents, agents do not follow correct procedures) | L | M | D | **** | 6/6/15 |
| 48 | Malicious remote access agent training (change web instructions)Hacker modifies agent instructions and post bad info | L | M | D | **** | 6/6/15 |
| 49 | Physical access & agent training (OSG staff trashing training materials) | L | L | E | **-** | 6/6/15 |
| 50 | Careless 3rd party user PKI training (Users don’t get proper instructions on how to handle private keys) | M | L | D | **-** | 6/6/15 |
| 51 | 3rd party careless user support for PKI (Users get mad, try to circumvent controls that are not working) | M | L | D | **** | 6/6/15 |
| 52 | Malicious remote access user support (N/A, or trashing trouble ticket) | L | L | E | **-** | 6/6/15 |
| 53 | OSG staff alarmist user support(OSG staff mis-represent user support issues) | L | L | E | **-** | 6/6/15 |
| 54 | 3rd party careless logging, (incorrect mail sent to RA logging list) | L | L | E | **-** | 6/6/15 |
| 55 | 3rd party malicious logging (Intentional incorrect log entries, potential to confuse audit trail) | L | L | E | **-** | 6/6/15 |
| 56 | OSG staff careless log entries (Incomplete log entries, incomplete audit trail) | L | L | E | **-** | 6/6/15 |
| 57 | Software exploits log entries, corruption of email archives, damage to audit trail | L | M | D | **** | 6/6/15 |
| 58 | Physical access to log info | L | M | D | **** | 6/6/15 |
| 59 | PMA 3rd party carelessness(Disruption of PMA process) | L | L | E | **-** | 6/6/15 |
| 60 | PMA 3rd party vandal( plus intentional damage to PMA repository) | L | L | E | **-** | 6/6/15 |
| 61 | PMA physical access (Vandal damaging PMA repository) | L | L | E | **-** | 6/6/15 |
| 62 | PMA OSG staff alarmist (OSG staff impugning PMA) | L | L | E | **-** | 6/6/15 |
| 63 | ID vetting 3rd party carelessness(Accidental incomplete ID verification, or accidental duplicate DN issuance, impact on PKI trust if happens too often) | L | L | E | **-** | 6/6/15 |
| 64 | ID vetting 3rd party vandal(Malicious sponsor or agent violates authentication process, issues incorrect DN, low impact unless malicious party has access to VOMS admin) | L | M | D | **-** | 6/6/15 |
| 65 | ID vetting malicious remote access (Hacker access to Registration Manager server, DNS potential from installing vandal agent doing revocation or certificates) | L | H | C | **-** | 6/6/15 |
| 66 | ID vetting physical access | L | H | C | **-** | 6/6/15 |
| 67 | ID vetting OSG staff alarmist (OSG staff making incorrect statements about quality of ID vetting, potential damage to trust in PKI) | L | L | E | **-** | 6/6/15 |
| 68 | CA integrity 3rd party carelessness (Potential disruption of services, such as CRL’s, and delays in request processing) | L | M | D | **-** | 6/6/15 |
| 69 | CA integrity 3rd party vandal (Potential disruption of services, like CRL distribution, or violation of CA key) | L | H | C | **-** | 6/6/15 |
| 70 | CA integrity malicious remote access(Potential disruption of services like CRL distribution, potential DNS from certificate revocation) | L | H | C | **-** | 6/6/15 |
| 71 | CA integrity physical access(Potential loss of PKI) | L | H | C | **-** | 6/6/15 |
| 72 | CA integrity OSG staff alarmist(Mis-statements about PKI may damage trust inPKI) | L | M | D | **-** | 8/14/15 |
| 73 | Incorrect and or out of date instructions or information on the collaborative development space, on the OSG twiki | M | L | D | **↓** | 6/6/15 |
| 74 | Web information updated (defacement) | M | H | B | **** | 6/6/15 |
| 75 | OSG information gives away OSG private/sensitive information | L | H | C | **** | 6/6/15 |
| 76 | Injection of operational instructions from OSG Ops to information channels by unrelated third parties. | L | H | C | **-** | 6/6/15 |
| 77 | Service compromised, DOS, DNS redirect | M | H | B | **-** | 6/6/15 |
| 78 | User addition, policies for addition/removal not followed | M | M | C |  | 6/6/15 |
| 79 | 'Stealing' un-authorized accounting information | L | L | E | **-** | 6/6/15 |
| 80 | Insertion of 'fake' accounting information | L | M | D | **-** | 6/6/15 |

*Note: Different colors are used in the “no” field to categorize individual OSG components, Columns O,S,G represent Occurrence (O),Severity (S), Grade (G)*

**Monitoring and reviewing risks in OSG**

The OSG *Risk Management Table* should be visited with re-evaluation of the risks occurring on an annual basis. If OSG prevention strategies are being effective, some the OSG Grade A and B Risks should be downgraded. Risk Status is reported to the OSG management on an agreed regular basis.

# OSG Residual Risk Analysis

Residual risks are divided into categories based on expected frequency of occurrence after full implementation of all security controls. We consider an occurrence rate to be low if it is expected to happen <10 times per year, very low if it is expected to happen less than once/year, and extremely low if it is expected to happen less than once every five years. With these definitions, our residual risks are:

* Very low rate of virus/worm infection due to late virus signatures and poor user behavior
* Very low rate of unauthorized access through physical access
* Extremely low rate of damage due to disgruntled insider with specialized knowledge
* Extremely low rate of loss of important data
* Extremely low rate of penetration of servers and central systems due to totally unexpected occurrences

### CONTROL RECOMMENDATIONS

No additional controls are required.

### IX. RISK MITIGATION

### No additional mitigation action is planned at this time and the risk levels identified above are accepted.

### Appendix: Detail explanation of risks identified and mitigations

**Software stacks and release process**: **(Alain Roy)**

1) Software auto-update feature exploited to provide corrupt software

Threat: Skilled crackers corrupt auto-update software cache

Vulnerability: Software that performs auto-update

Comments: This is unlikely to occur because the only software with an auto-update feature (MonaLISA) has the auto-update disabled. However, some users manually enable it, so there is some risk.

Mitigation: None needed, other than warning users not to enable auto-update

2) Software in the stack has flaws that could be exploited in deployments.

Threat: Script kiddie, skilled crackers

Vulnerability: Reliance on third parties for software.

Mitigations:

A) VDT needs ability to provide security fixes in a timely fashion

B) VDT needs to have security discussion with providers, when possible.

C) VDT needs to watch for security patches for software

D) VDT should suggest local configuration to provide some protection against security problems. (Firewalls,

Permissions, etc.)

E) Default VDT installation should only enable needed features. (That is, software might provide more features

Than are needed, and some can be turned off.)

Comment: We distribute software based on millions of lines of code, and the VDT team cannot do complete security audits on all of it. The best we can do is reacting as quickly as possible to problems, and to provide recommendations on keeping a secure environment.)

3) Corruption of the software stack by authorized person

Threat: Careless authorized person

Vulnerability: Improper actions by VDT/OSG software developer or a system administrator could corrupt software

Mitigation: Careful software development and system administration procedures

Comment: It's unlikely that a security problem will be introduced by carelessness. It is more likely that software is removed or rendered inoperable.

4) Corruption of software stack by outsider

Threat: Skilled cracker

Vulnerability: There are several places where a skilled cracker could inject malicious code into the VDT:

A) Modifying software as distributed by third-parties

B) Gaining access to VDT development computers and editing code directly.

C) Gaining access to NMI Build and Test infrastructure (where VDT builds happen) and corrupting the build process

D) Gaining access to VDT web server and corrupting distributed files directly.

Mitigation:

A) Careful testing by the VDT team

B) Reliance on system administrators to provide a secure facility.

5) Release process is unavailable, but is needed by the security process.

Threat: Skilled cracker or script kiddy

Vulnerability: A denial of service attack could prevent distribution of new software

Mitigation: We rely on our system administrators to provide a secure hosting environment for our software distribution. We could consider mirroring the software distribution to lessen the risk of a failure at a single-site causing this situation.

### Security Processes: (Don Petravick)

6) Disclosure of security information.

Vulnerability: Information systems which do not meet privacy requirements.

Threat – Accidental handling of information by **authorized person** resulting in it being place in a more visible location.

Threat – **Spy** subverting or breaking into an appropriate information system.

7) Subversion of Security processes – people taking action directed by an imposter acting as OSG security person.

Threat – Skilled cracker (actual damage), disgruntled insider.

Vulnerability – “Remote access” -- activities are conducted on the open internet by outside imposter, insider, and former insider.

8) Withheld notification of security event

Threat: **Authorized person** failing to report incident.

Vulnerability – Inappropriate actions.

**OSG Validation Monitoring and Accounting Process: (Dan Yocum)**

9) Distributed Denial of Service (DDOS)

Threats (Section 3): I, III, V, VII

Vulnerability: A bot-net could be configured to continually request information from the LDAP based servers (Gridcat, BDII,GIP).

Comment: none

Mitigation: Monitor for DDoS attacks and block at border routers.

10) Gridex user account (mis) compromised

Threats (Section 3): III, IV, VI

Vulnerability: The system Gridex is run from is compromised; someone watches Leigh type in her grid password and steals her key and cert.

Comment: This is no different than a normal user account being compromised.

Mitigation: The computer Gridex runs from is kept up-to-date with security patches are nobody watches Leigh's fingers ever.

11) Flaw in LDAP server software allowing arbitrary code to be executed.

Threats (Section 3): II-VI

Vulnerability: Software bug in OpenLDAP.

Mitigation: Keep OpenLDAP patches up-to-date; apply firewall rules to only allow ldap access from authorized set of systems.

12) Accounting system/software compromised allowing execution of arbitrary code.

Threats (Section 3): I, V, VI

Vulnerability: Bug in accounting service

Comment: Same risk as "Third Party Software," elsewhere.

Mitigation: Apply firewall rules to only allow access from authorized set of systems.

**Communication and Web presence (Leigh Grundhoefer)**

13) Incorrect and or out of date instructions or information on the collaborative development space, on OSG twiki

Threat: Careless authorized person, disgruntled insiders

Mitigation: Documentation reviewers?

14) Web information updated (defacement)

Threat: skilled crackers

Mitigation: Review Content Management System software, Keep all software patched and protected. Shell access only as necessary to Webmasters and administrators.

15) OSG information gives away OSG private/sensitive information

Threat: Skilled crackers

Mitigation: Security review of accessible information. Develop and employ access restrictions including data retention and storage standards.

16) OSG information gives away collaborators private/sensitive information

Threat: Skilled crackers

Mitigation: Security review of accessible information. Develop and employ access restrictions including data retention and storage standards.

17) Injection of operational instructions from OSG Ops or Core to information channels by unrelated third parties.

RSS, mailing lists, Ops to support centers communication, Security to security contacts communication

Threat: Skilled crackers

Mitigation: Controlled access to OSG registration information, use of signed emails for communication.

**OSG hosted VO (Leigh Grundhoefer)**

18) Service compromised, DOS, DNS redirect

Threat: Skilled crackers

Mitigation: Review Service framework connections to clients. Provide signed/encrypted information and data exchange.

19) User addition, policies for addition/removal not followed

Threat: Careless authorized person, disgruntled insiders

Mitigation: VO administrator and voms administrator training and understanding of accepted practices.

**OSG Accounting Process risk assessments (Philippe Canal)**

20) Denial of Service Attack

Threats (Section 3): I, III, V, VII

Vulnerability: Both the uploading of accounting and the downloading reports are 'web services' and as such could be the subject of DDoS attack.

Mitigation: Monitor for DDoS attacks and block at border routers. Software is designed to be resilient to loss of connection and prevent loss of data when this happen.

21)'Stealing' un-authorized accounting information

Threats (Section 3): I, VI

Vulnerability: A malicious user could try to poke at information there not entitled too, including information about

computing usage that can be linked to a specific user.

Mitigation: Access the information (except in a few case of aggregate information) require authentication via a DOEGrid certificate.

22) Insertion of 'fake' accounting information.

Threats (Section 3): III, IV, VI

Vulnerability: A malicious user could try to insert fake information or modify existing information, assumingly with the purpose of increase or decrease the apparent uses or contributions

Mitigation: Access the information (except in a few case of aggregate information) require authentication via a DOEGrid certificate. Origin of the information insert is tracked as much as possible. Access to the underlying database needs to be also protected using establish best practices.

**Responsible organization (Ruth Pordes):**

22) Defective operation of OSG interoperating software harms the Peer grid or the OSG

Threat: Authorized person not abiding by the AUP, Disgruntled insider, Resource Exploiter.

Controls: Control of Administrators, Physical Access control and Site management,

23) Defective use of OSG interoperating software harms the Peer grid or the OSG

Threat: Authorized person not abiding by the AUP, Resource Exploiter.

Controls: Security awareness and training, Configuration management.

24) Compromise of the interoperating software:

Threat: Script kiddies, skilled crackers.

Controls: Configuration Management, Vulnerability Identification.

25) Embarrassment to the OSG

Threat: Loud Person.

Controls: Trust relationships between grids, Administration of interoperation software available to incident response.

**User’s Process (Doug)**

Elements of User’s Process:

1. User compliance with OSG AUP
2. VO compliance with VO AUP and OSG Service Agreement
3. RA Agent authorization (includes gridadmin)
4. RA Agent training & education (includes gridadmin)
5. User training and education about PKI
6. User support
7. RA process logging
8. PMA activities
9. Identity Vetting – quality of certificates
10. CA integrity

Threat and vulnerability list

1. V.I & T.I – Third party - carelessness
2. V.I & T.II-V – Third party – squatter, vandal, thief, author
3. V.II & T.I – OSG staff – carelessness
4. V.III & T.I – Improper OSG user – carelessness
5. V.IV & T.II-IV; V.I,II & T.II,IV,VI; V.III & T.III  
   remote access – squatter, vandal, thief, author, spy  
   third party & OSG staff – squatter, thief, spy  
   improper OSG user – vandal
6. V.V,I,II,III & T.II-VI – software exploits from anyone – squatter, thief, vandal, spy
7. V.VI & T.I-VI – physical access – by anyone
8. add V.II & T.VII – OSG staff – alarmist

Occurrence – low < 1/mo; 1.mo. < med < 1/day; high > 1/day

Severity – low = few sites, << all OSG; few sites \* 2 days < med. < all OSG \* 2 days; high > all OSG \* 2 days

Risk analysis table for User Process

| **UP#** | **T&V** | **Risk** | **Occurrence** | **Severity** | **Grade** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | *Reliance on third parties to ensure user compliance with OSG AUP*  Some users unaware of AUP, may violate policies out of ignorance, may fail to report security incidents | medium | low | D |  |
| 1 | 2 | N/A |  |  |  |  |
| 1 | 3 | N/A (would be 1-8 if we measured user compliance) |  |  |  |  |
| 1 | 4 | *User carelessness violation of AUP*  Like 1-1 | Medium | Low |  |  |
| 1 | 5 | *User willful violation of AUP*  User circumvents security controls and exercises unauthorized use of resources | Low | medium | D | User authZ and user ID controls |
| 1 | 6 | (like 1-5) |  |  |  |  |
| 1 | 7 | N/A |  |  |  |  |
| 1 | 8 | *OSG misrepresenting user AUP compliance data*  If we had user compliance data this could be an embarrassment | Low | Low | E |  |
| 2 | 1 | *VO careless violation of AUP*  Errors in VOMS, incorrect info for users, May provide hole for malicious user to exploit, see 1-5 | Low | Low | E |  |
| 2 | 2 | *VO malicious violation of AUP*  VO mis-representing purpose of resource usage, VO insider authorizing mis-use of resources, embarrassment to OSG | Low | Medium | D | Means user authZ control not immediately effective. User ID control does not apply to mis-use, requires VO management intervention |
| 2 | 3 | *OSG staff careless violation of AUP for OSG-hosted VOs*  Like 2-1 but less frequent | Low | low | E |  |
| 2 | 4 | N/A |  |  |  |  |
| 2 | 5 | VO malicious remote access, like 2-2 |  |  |  |  |
| 2 | 6 | *VO malicious software exploit*, like 2-2 | Low | medium |  |  |
| 2 | 7 | *VO physical access, applies to OSG-hosted VOs*  OSG staff vandal interfering with hosted-VO authZ | Low | Medium | D | IU physical controls, IU & OSG management controls |
| 2 | 8 | *VO OSG staff alarmist – for OSG-hosted VOs*  OSG staff claiming incorrectly that OSG-hosted VO violates AUP and abuses resources. Potential embarrassment for OSG | Low | low | E | OSG management controls |
| 3 | 1 | *Third party careless agent authorization (CA managers mistake)*  Risk of mistaken agent authorization, potential damage to trust of grid PKI if it happens too often | Low | Low | E | 3rd party CA managers controls |
| 3 | 2 | *Third party agent authorization (impersonate OSG RA to install malicious agent)*  Risk that malicious agent is authorized via impersonation of legit RA, immediate impact is low, potential threat to PKI trust, potential DNS by revocation of certificates | Low | High | C | RA ID protections |
| 3 | 3 | *OSG RA careless authZ of agent*  Accidental authorization of agent that does not want agent access, low impact unless agent also exploits VOMS | Low | Low | E | 3rd party agent authZ controls |
| 3 | 4 | N/A (or 3-1) |  |  |  |  |
| 3 | 5 | *Remote access authZ of agent (CA managers issue)*  Like 3-2 |  |  |  |  |
| 3 | 6 | *Software exploit agent authZ (CA managers issue)*  Like 3-2 | Low | High | C | 3rd party CA managers controls |
| 3 | 7 | *Agent authZ physical access (CA managers issue)*  Malicious physical access to CA machines, like 3-2 | Low | High | C |  |
| 3 | 8 | *OSG staff alarmist – removal of agent authZ*  Agent authorization is removed due to incorrect OSG staff complaints , may delay some certificate requests | Low | Low | E |  |
| 4 | 1 | *3rd party careless agent training*  Agents in VOs give incorrect info to other agents, requests handled incorrectly | Low | Low | E | Proper instructions & trainingon web |
| 4 | 2 | *3rd party malicious agent training*  Intent to give agents incorrect instructions, low impact unless malicious person also has access to VOMS | Low | Low | E | Agents should not be VOMS admins |
| 4 | 3 | *OSG staff careless agent training*  OSG RA provides incorrect training info to agents, agents do not follow correct procedures | Low | Low | E | Control is to review training for compliance with CP/CPS |
| 4 | 4 | N/A |  |  |  |  |
| 4 | 5 | *Malicious remote access agent training (change web instructions)*  Hacker modifies agent instructions and post bad info | Low | Low | E | Web content controls, tell agents to report suspicious or confusing instructions |
| 4 | 6 | *Software exploits affect agent trainin*g (like 4-5) |  |  |  |  |
| 4 | 7 | *Physical access & agent training (OSG staff trashing training materials)*  Like 4-5 for OSG staff | Low | Low | E |  |
| 4 | 8 | OSG alarmist & agent training (N/A) |  |  |  |  |
| 5 | 1 | *Carelsss 3rd party user PKI training*  Users don’t get proper instructions on how to handle private keys | Medium | low | D | User ID controls when violation is discovered |
| 5 | 2 | *Malicious 3rd party user PKI training*  Like 5-1 |  |  |  |  |
| 5 | 3 | *Careless OSG staff user PKI training*  Like 5-1 |  |  |  |  |
| 5 | 4 | N/A |  |  |  |  |
| 5 | 5 | *Malicious remote access & user pKI training*  Like 5-1 |  |  |  |  |
| 5 | 6 | N/A |  |  |  |  |
| 5 | 7 | (like 4-7) |  |  |  |  |
| 5 | 8 | N/A |  |  |  |  |
| 6 | 1 | *3rd party careless user support for PKI*  Users get mad, try to circumvent controls that are not working | Low | Low | E | User ID controls |
| 6 | 2 | *Malicious 3rd party for user PKI support*  Like 6-1 |  |  |  |  |
| 6 | 3 | *Careless OSG staff for user PKI support*  Like 6-1 |  |  |  |  |
| 6 | 4 | N/A |  |  |  |  |
| 6 | 5 | *Malicious remote access user support* (N/A, or trashing trouble ticket) | Low | Low | E | OSG trouble ticket integrity |
| 6 | 6 | (like 6-5) |  |  |  |  |
| 6 | 7 | N/A |  |  |  |  |
| 6 | 8 | *OSG staff alarmist user support*  OSG staff mis-represent user support issues | Low | low | E |  |
| 7 | 1 | *3rd party careless logging*,  incorrect mail sent to ra logging list | Low | Low | E | Like spam, easily discounted |
| 7 | 2 | *3rd party malicious logging*  Intentional incorrect log entries, potential to confuse audit trail | Low | Low | E | Use signed email |
| 7 | 3 | *OSG staff careless log entries*  Incomplete log entries, incomplete audit trail | Low | Low | E | Control is agent training |
| 7 | 4 | N/A |  |  |  |  |
| 7 | 5 | (like 7-2) |  |  |  |  |
| 7 | 6 | *Software exploits log entries*, corruption of email archives, damage to audit trail | Low | Low | E | Controls on web email archive |
| 7 | 7 | *Physical access to log info*  Like 7-6 | Low | Low | E | Site physical access controls |
| 7 | 8 | N/A |  |  |  |  |
| 8 | 1 | *PMA 3rd party carelessness*  Disruption of PMA process | Low | Low | E | PMA governance rules |
| 8 | 2 | *PMA 3rd party vandal*  Like 8-1, plus intentional damage to PMA repository | Low | Low | E | PMA governance rules, PMA archive security controls |
| 8 | 3 | *PMA OSG staff carelessness*  Like 8-1 |  |  |  |  |
| 8 | 4 | N/A |  |  |  |  |
| 8 | 5 | *PMA 3rd party remote access vandal*  Like 8-2 |  |  |  |  |
| 8 | 6 | *PMA software exploits*  Like 8-2 |  |  |  |  |
| 8 | 7 | *PMA physical access*  Vandal damaging PMA repository, like 8-2 with physical access | Low | Low | E | Site physical controls |
| 8 | 8 | *PMA OSG staff alarmis*t  OSG staff impugning PMA | Low | low | E | OSG management controls |
| 9 | 1 | *ID vetting 3rd party carelessness*  Accidental incomplete ID verification, or accidental duplicate DN issuance, impact on PKI trust if happens too often | Low | Low | E | User ID controls, agent training |
| 9 | 2 | *ID vetting 3rd party vandal*  Malicious sponsor or agent violates authentication process, issues incorrect DN, low impact unless malicious party has access to VOMS admin | Low | Medium | D | User ID controls |
| 9 | 3 | *ID vetting OSG staff carelessness*  Like 9-1 but less frequent |  |  |  |  |
| 9 | 4 | *ID vetting user carelessness*  Like 9-1 |  |  |  |  |
| 9 | 5 | *ID vetting malicious remote access*  Hacker access to Registration Manager server, DNS potential from installing vandal agent doing revocation or certificates | Low | High | C | Reliance on CA controls |
| 9 | 6 | ID vetting software exploit  Like 9-5 |  |  |  |  |
| 9 | 7 | *ID vetting physical access*  Like 9-5 plus site physical access | Low | High | C | Reliance on CA controls |
| 9 | 8 | *ID vetting OSG staff alarmist*  OSG staff making incorrect statements about quality of ID vetting, potential damage to trust in PKI | Low | Low | E |  |
| 10 | 1 | *CA integrity 3rd party carelessness*  Potential disruption of services, such as CRL’s, and delays in request processing | Low | Medium | D | Rely on CA controls, would be good to make some services (CRL) redundant |
| 10 | 2 | *CA integrity 3rd party vandal*  Potential disruption of services, like CRL distribution, or violation of CA key | Low | High | C | CA controls |
| 10 | 3 | *CA integrity OSG staff carelessness*  N/A |  |  |  |  |
| 10 | 4 | *CA integrity careless user*  N/A |  |  |  |  |
| 10 | 5 | *CA integrity malicious remote access*  Potential disruption of services like CRL distribution, potential DNS from certificate revocation | Low | High | C | CA controls, CA key is not supposed to be accessible remotely? |
| 10 | 6 | *CA integrity software exploits*  Like 10-5 |  |  |  |  |
| 10 | 7 | *CA integrity physical access*  Potential loss of PKI | Low | High | C | CA controls, think about redundant services |
| 10 | 8 | *CA integrity OSG staff alarmist*  Mis-statements about PKI may damage trust inPKI | Low | low | E |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Risk Matrix Table for User Process (Table 4 in Risk Assessment document)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Description of Risk** | **Occurrence** | **Severity** | **Grade** | **Status (?), control in place, *possible control to implement*** |
| 1 | Users unaware of OSG AUP, may violate policies out of ignorance, may fail to report security incidents | Medium | Low | D | User AuthZ |
| 2 | User violates AUP willfully and circumvents security controls to access resources | Low | Medium | D | User AuthZ |
| 3 | VO has incorrect user information in VOMS server, may provide hole for malicious user to exploit | Low | Low | E | User AuthZ |
| 4 | VO insider authorizing mis-use of resources | Low | Medium | D | Requires intervention with VO manager |
| 5 | OSG staff manipulating OSG-hosted VO authorization | Low | Medium | D | Requires OSG management intervention |
| 6 | OSG staff publicizing false information about User Process | Low | Low | E | OSG management controls |
| 7 | Careless 3rd party mistakenly granting agent privilege to incorrect person, possible impact on OSG since all agents of DOEGrids have privilege for all certificates | Low | Low | E | CA managers controls |
| 8 | Malicious authorization of agent privilege for illegitimate person, by impersonating a valid RA, malicious agent can revoke all certificates causing DNS | Low | High | C | Identity protections for RA’s, requiring digitally signed email to CA managers |
| 9 | Hack into CA website and perform malicious actions, install fake agents, revoke certificates, cause DNS | Low | High | C | CA managers controls |
| 10 | Careless or incomplete training for agents, agents do not follow correct procedures, potential exploit for malicious user if combined with exploit of VOMS server | Low | Medium | D | *Correct agent training,* suitable VOMS user registration |
| 11 | Malicious mis-information provided for agent training, like 10 but implies intent to exploit | Low | Medium | D | *Validated agent training*, suitable VOMS user registration |
| 12 | Careless or incomplete user training for PKI, user may not handle private key correctly | Medium | Low | D | *Clearer user training material, for user’s and VOs,*  User ID control |
| 13 | Accidental corruption of RA process audit log, leads to incomplete of lack of audit ability | Low | Low | E | Log should be backed up normal information protection procedures |
| 14 | Intentional corruption of RA process audit log to disguise audit trail, potential privacy compromise | Low | Low | E | *(is it of value?),*  Privacy protections suitable for OSG internal information |
| 15 | Malicious disruption of PMA process, potential damage to credibility of PKI, potential delays in handling authentication and revocation requests | Low | Low | E | CA managers controls |
| 16 | Careless or incomplete identity vetting in certificate process, potential exploit for malicious user can permit abuse of resources if identity theft occurs | Low | Medium | D | Agent training, suitable VOMS registration |
| 17 | Malicious abuse of identity vetting, insider participation in identity theft by agents | Low | Medium | D | Agent validation, User ID control for agent certificate |
| 18 | Careless management of CA services, potential DNS caused by CRL lack of availability | Low | High | C | CA managers controls |
| 19 | Loss of CA integrity due to physics access to CA, potential compromise of CA key and need for re-issuing thousands of certificates | Low | High | C | CA managers controls, *consider redundant services* |

Description of Controls relevant to User Process

|  |  |  |
| --- | --- | --- |
| Control name | Exists | Description |
| User ID | Y | Certificate revocation |
| User AuthZ | Y | Communicate with VO to suspend user’s authorization |

### 