



Template for SMSCG Documents

Document info

| | |
|-------------------|---------------------------|
| Document Name | Security Audit Summary |
| Document Version | Version 0.1 |
| Date last updated | 02/01/10 |
| SMSCG Activity | WP5 Security and Policies |

Change history

| Version | Date | Author(s) | Comment |
|---------|----------|-----------|---------|
| V0.1 | 01/02/10 | P. Flury | Initial |
| | | | |
| | | | |

Abstract: This document summarizes the findings of the security audit (questionnaire) that was carried out for the SMSCG project.

Contents

| | |
|-------------------|---|
| Introduction..... | 2 |
| Section 1..... | 2 |

Introduction

The SMSCG-I has carried out a security audit. All sites providing infrastructure, i.e. those contributing with clusters or hosting core services, have answered a security questionnaire, that was custom-tailored from the ISO/IEC27002 security document. The objectives of the questionnaire were (i) to assess the sites, (ii) to identify weaknesses and thus prevent incidents, and (iii) to provide procedures for incidents handling.

This document summarizes the findings. Recommendations are provided in a separate document. few SMSCG specific recommendations. For the general recommendations we re on the sites own initiative (as these are beyond the scope of the SMSCG project).

1 Findings

1. **Assessing security risks:** two of the bigger sites have been, or are planning to be audited by some third party about information security. Another site does internal audits at regular time intervals.
The usage of security checklists to carry out security risk assessments isn't very popular, since most sites consider themselves too small to justify the overhead of such a practise. They rely instead on the judgement and initiative of their local site/system administrators.
All sites do however comply with the SMSCG checklist.
2. **Treating security risks:** All sites have decision makers for security risk treatment. Most sites do however not follow specific processes for treating security risks.
3. **Security policy:** All bigger sites have local security policies they adhere to. The Grid Security Policy are not necessarily covered by the local security policies, but they can be incorporated, by all sites according to the site's best practices.
4. **Organization of information security:**
 - a.) **internal:** every site has named a person or group that is in charge of information security and security incidents. (see recommendations).
All sites have a set of best practices in place, to ensure information security, e.g. adherence to data protection regulations, password polices of government, patching policies, network access control, backup policies, minimal set of service running etc..
 - b.) **external:** there is no explicit risk assessment for external parties who have access to the facilities deployed by SMSCG at any site. This is delegated to the AAI. Still, all sites enforce a user policy.
5. **Asset management:** All sites have a clear picture about their assets.
6. **Human resources security:** all sites have revocation procedures in place when people leave their institution.
7. **Physical and environmental security:** at all sites: rooms (in particular server rooms) are only accessible by authorized staff.
8. **Communications and operations management:** Only half of the sites do implement intrusion detection mechanisms (not necessarily for all services). All sites implement procedures for data backup. Again, not all data is backed up. Most sites have audit logs, but no sites specially protect them.

9. **Access control to Grid services:** UI's and Grid front-ends are mostly separated from the clusters and are installed on standalone machines. User mostly access the UI via ssh. (see recommendations)
10. **Vulnerability and Patching management:** most sites have a vulnerability management. Patching management is however most often delegated. (recommendation: coordinate this at grid-level).
11. **Information security incident management:** Major sites have specific guides and procedures about what measures should be taken when an incident happens (see also point 2). All sites know who to inform when an incident happens. Most of the sites do forensics when an incident happens (sometimes depending on the severity of the incident). Most sites do exchange information about the incidents with other (or other sites).
12. **Business continuity management:** all sites seem to be able to recover in reasonable time from any incident and disaster.

2 Recommendations

The security recommendations we deduced from above findings are provided into a separate document.