

Promoting security best practice

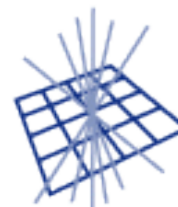
Romain Wartel

3rd EGEE conference, Athens, 18-22 April 2005



CCLRC

Rutherford Appleton Laboratory



GridPP

UK Computing for Particle Physics



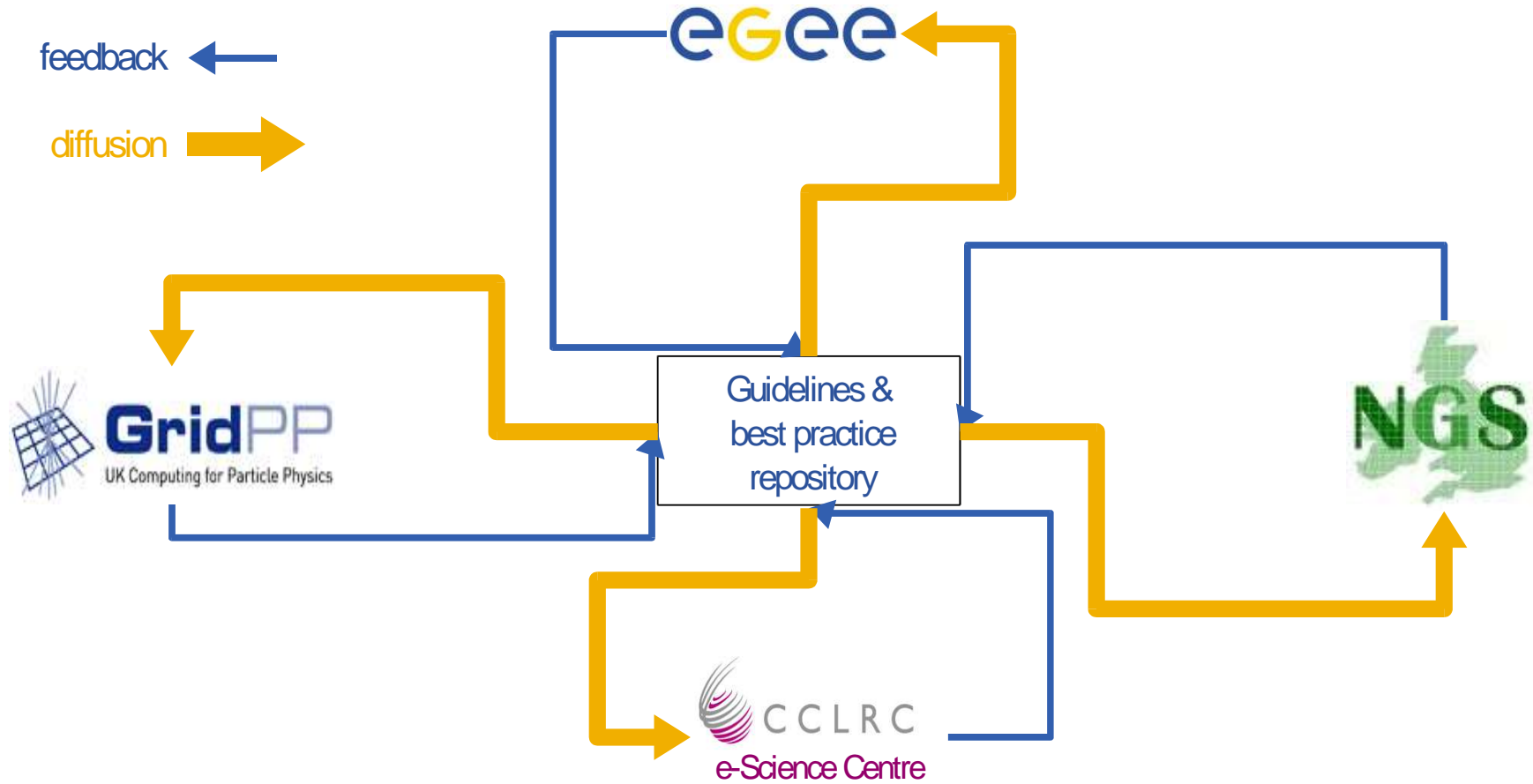
Information Society

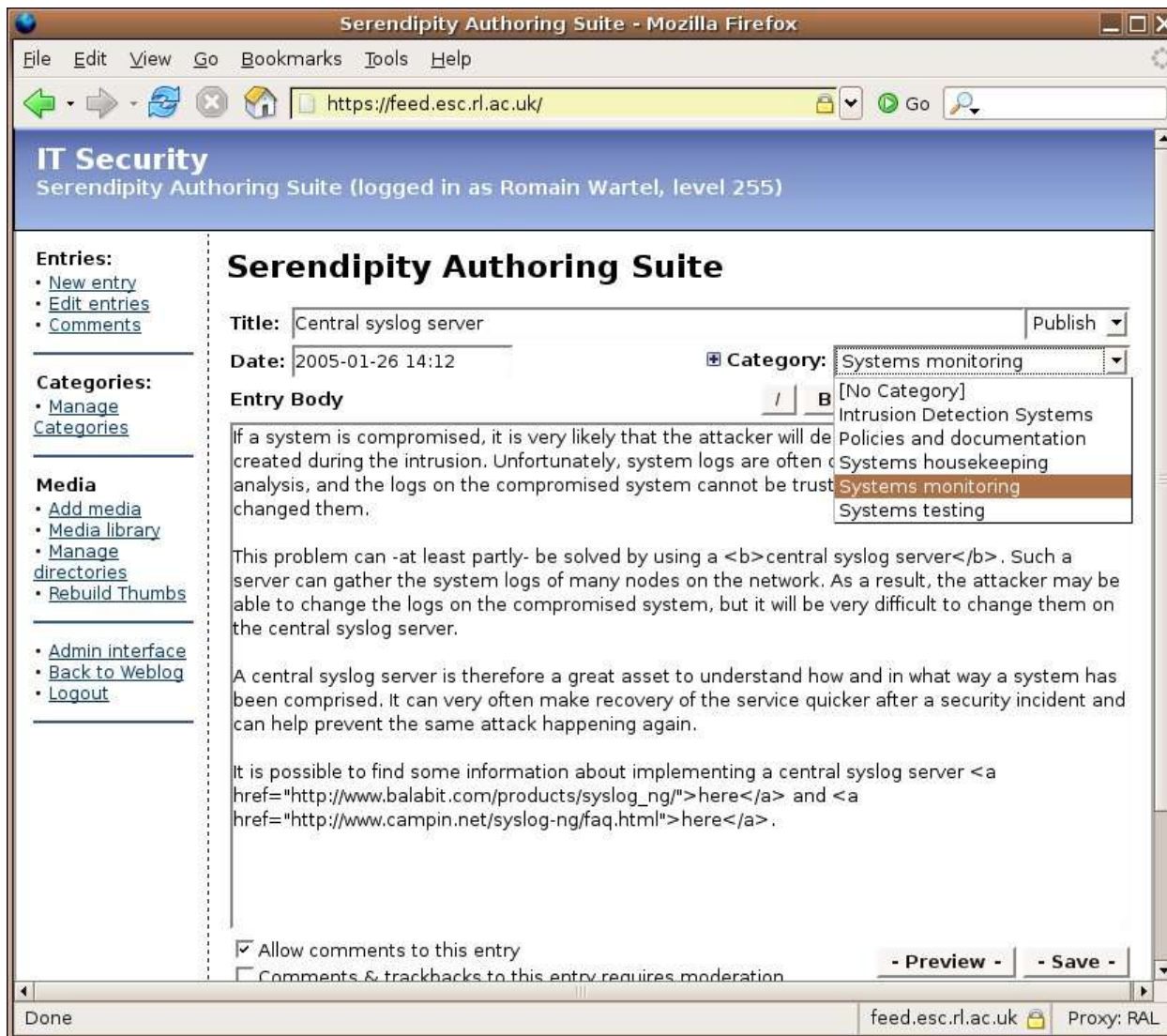


- Most sites have similar security issues
- Heterogeneous groups of systems administrators
- Experience from security incidents is extremely useful
- Good ideas should be spread amongst the community
 - Guidelines & best practice should be advertised

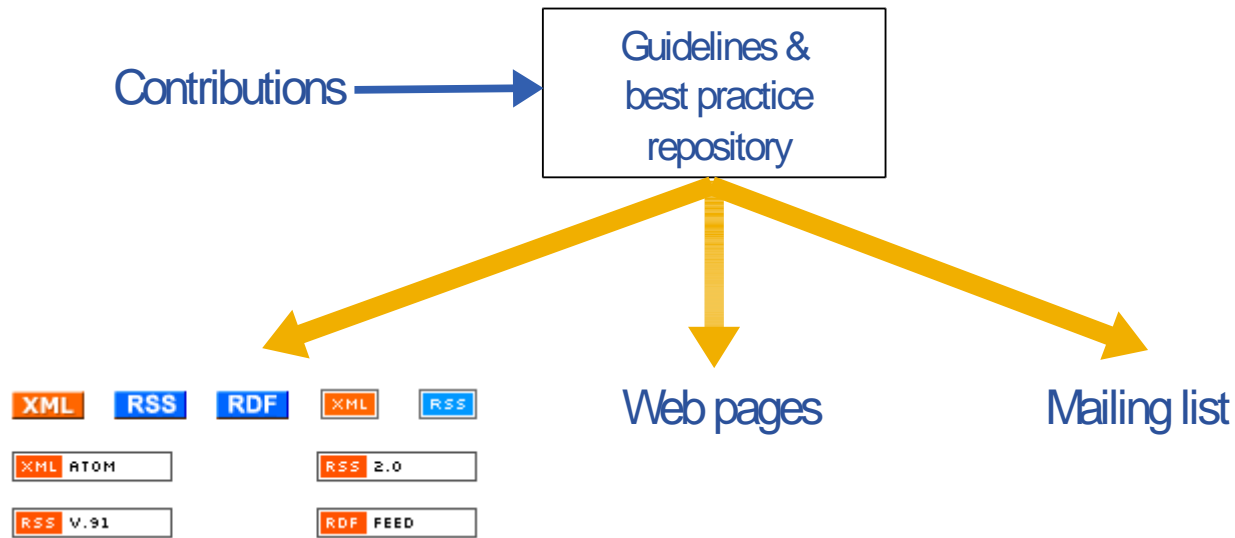
BUT

- Information must be kept up-to-date
- A single source of information is not enough
- Maintaining coherent information amongst many sites is difficult

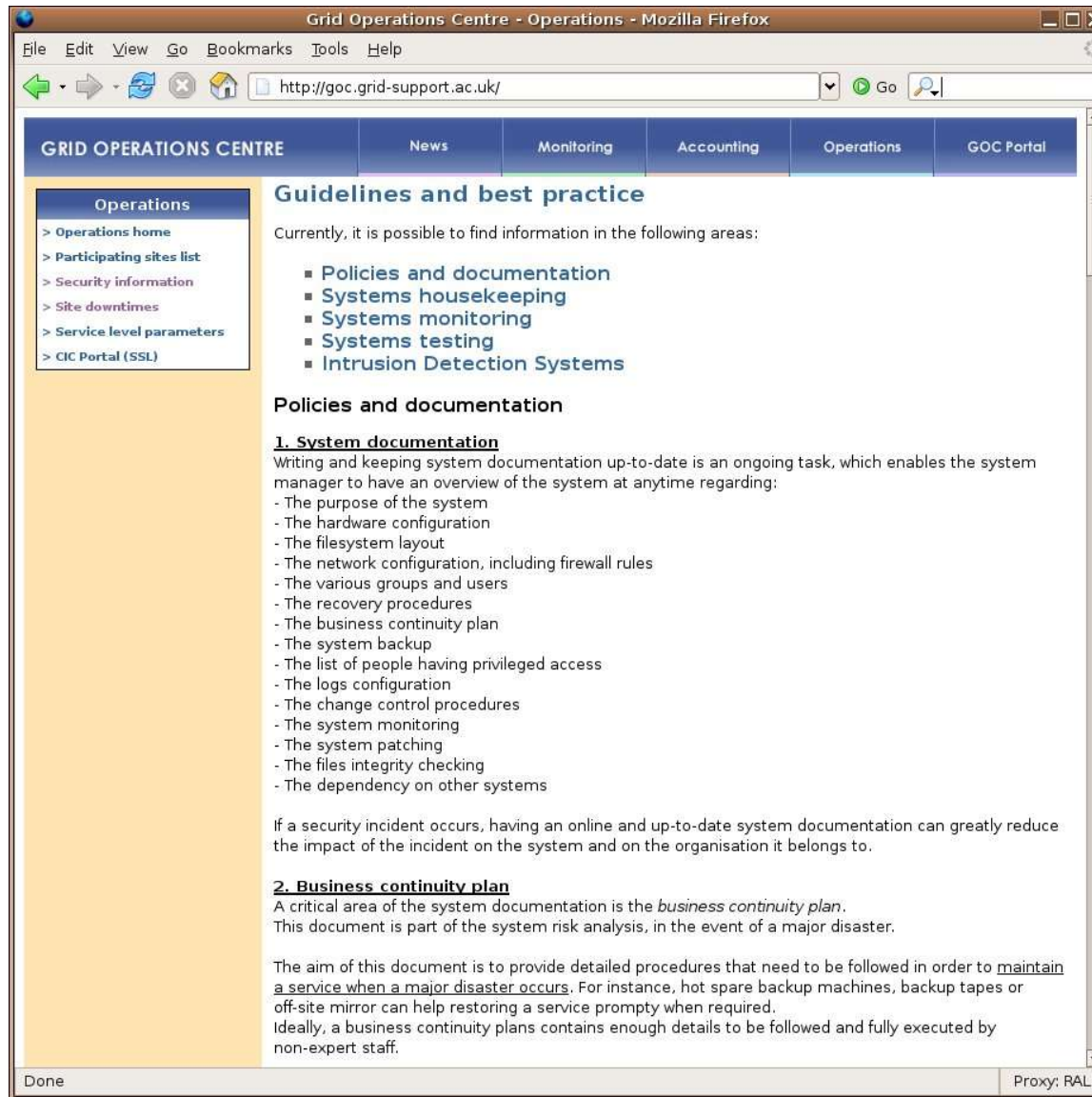




- Web interface, currently using Serendipity
- Using Gridsite authentication (x509 certificates)
- Contributions centralized and published by “trusted” people



- **The information is published via:**
 - Web pages
 - email
 - RSS feed



Grid Operations Centre - Operations - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://goc.grid-support.ac.uk/

GRID OPERATIONS CENTRE News Monitoring Accounting Operations GOC Portal

Operations

- > Operations home
- > Participating sites list
- > Security information
- > Site downtimes
- > Service level parameters
- > CIC Portal (SSL)

Guidelines and best practice

Currently, it is possible to find information in the following areas:

- Policies and documentation
- Systems housekeeping
- Systems monitoring
- Systems testing
- Intrusion Detection Systems

Policies and documentation

1. System documentation

Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:

- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

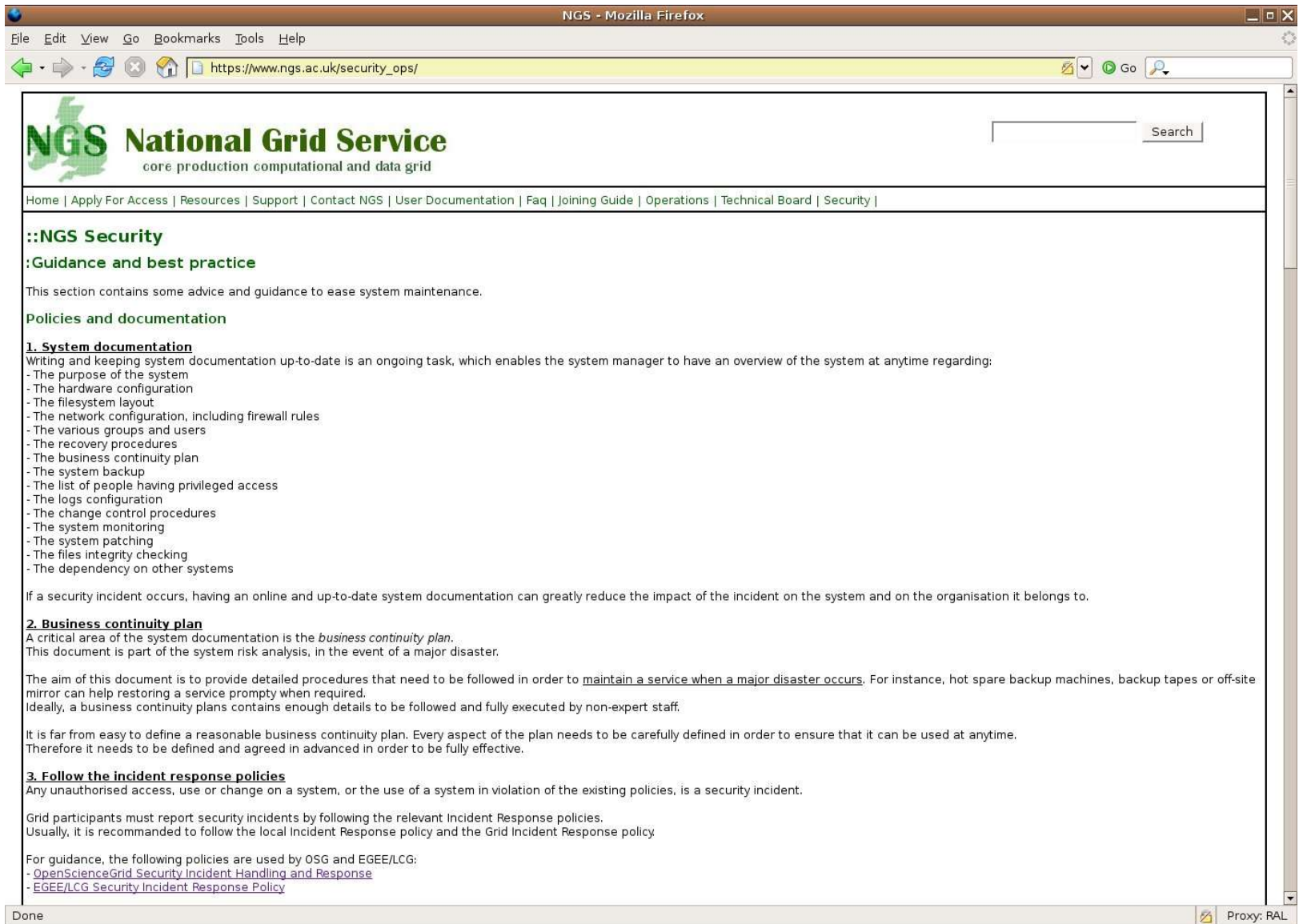
2. Business continuity plan

A critical area of the system documentation is the *business continuity plan*. This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service promptly when required.

Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

Done Proxy: RAL



NGS - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://www.ngs.ac.uk/security_ops/

NGS National Grid Service
core production computational and data grid

Home | Apply For Access | Resources | Support | Contact NGS | User Documentation | Faq | Joining Guide | Operations | Technical Board | Security |

::NGS Security
:Guidance and best practice

This section contains some advice and guidance to ease system maintenance.

Policies and documentation

1. System documentation
Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:

- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

2. Business continuity plan
A critical area of the system documentation is the *business continuity plan*. This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service promptly when required. Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

It is far from easy to define a reasonable business continuity plan. Every aspect of the plan needs to be carefully defined in order to ensure that it can be used at anytime. Therefore it needs to be defined and agreed in advanced in order to be fully effective.

3. Follow the incident response policies
Any unauthorised access, use or change on a system, or the use of a system in violation of the existing policies, is a security incident.

Grid participants must report security incidents by following the relevant Incident Response policies. Usually, it is recommended to follow the local Incident Response policy and the Grid Incident Response policy.

For guidance, the following policies are used by OSG and EGEE/LCG:

- [OpenScienceGrid Security Incident Handling and Response](#)
- [EGEE/LCG Security Incident Response Policy](#)

Done Proxy: RAL

GridPP - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.gridpp.ac.uk/deployment/security/guidelines/index.html

Welcome page : Current status : How to use the Grid : Website Help

GridPP
UK Computing for Particle Physics

Search

Deployment

- Overview
- Planning
- News
- Meetings
- Status
- Work in Progress
- Links
- Contact us
- UK Testzone

User Area

- Certificates
- User interface
- Run a job
- Join a VO
- FAQs
- Getting support

Admin Area

- Installations
- Joining LCG2
- Site tests
- Maintaining a site
- Monitoring

Security

- Security Policies
- Best Practice
- Security incidents
- Security challenges

Guidance and best practice

This section contains some advices and guidance to ease system maintenance. It is provided without any warranty and GridPP shall not be liable for any damage the following may cause.

Currently, it is possible to find information in the following areas:

- [Policies and documentation](#)
- [Systems housekeeping](#)
- [Systems monitoring](#)
- [Systems testing](#)
- [Intrusion Detection Systems](#)

Policies and documentation

1. System documentation

Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:

- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

2. Business continuity plan

A critical area of the system documentation is the *business continuity plan*. This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service promptly when required. Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

It is far from easy to define a reasonable business continuity plan. Every aspect of the plan needs to be carefully defined in order to ensure that it can be used at anytime.

Done Proxy: RAL

Date	Headline
24/02/05 14:23:09	Using SSH keys
26/01/05 14:12:12	Central syslog server
21/01/05 18:08:38	Configuring a system-level firewall

Feed: [IT Security for Grid Projects](#)
Item: [Central syslog server](#)

If a system is compromised, it is very likely that the attacker will delete the log files that have been created during the intrusion. Unfortunately, system logs are often critical during the post-incident analysis, and the logs on the compromised system cannot be trusted as the attacker could have changed them.

This problem can -at least partly- be solved by using a **central syslog server**. Such a server can gather the system logs of many nodes on the network. As a result, the attacker may be able to change the logs on the compromised system, but it will be very difficult to change them on the central syslog server.

A central syslog server is therefore a great asset to understand how and in what way a system has been comprised. It can very often make recovery of the service quicker after a security incident and can help prevent the same attack happening again.

It is possible to find some information about implementing a central syslog server [here](#) and [here](#).

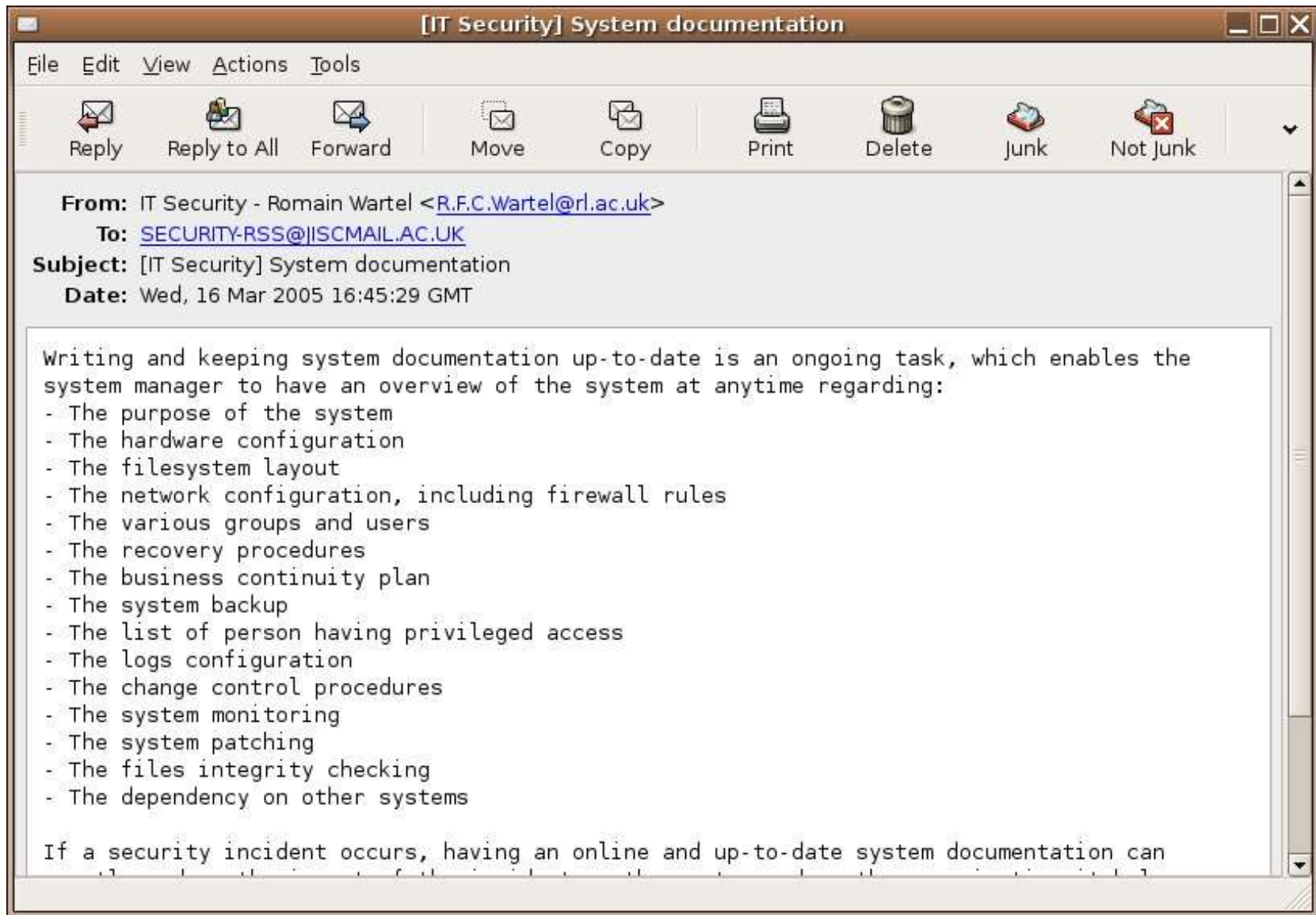


IT Security: 19 new items
[System documentation](#)
[Business continuity plan](#)
[Follow the incident response policies](#)

SharpReader

P Professional
 (Service Pack 1)

16:44



- XML based, recognized standard
- Widespread technology: many clients and APIs
- Enables injecting security information within existing Websites
- Enables filtering of the information
- Any webmaster can use the feed
- Coherent, up-to-date information is available
- Design up to Webmasters, but some layout can be pushed

However:

- RSS requires a server-side mechanism
- Webmasters need to trust the authors or perform manual updates

We need to:

- Provide better, more targeted content
- Provide a second layer of information, via external Web pages
- Receive contributions from the community
- Deploy the mechanism amongst more sites
- Improve the way the information is sorted

Questions?