



Enabling Grids for E-science

# Grid Incident Response Planning

*Operational Security Coordination Team meeting  
EGEE-4, Pisa  
Ian Neilson, CERN.*

[www.eu-egee.org](http://www.eu-egee.org)



- **Overview**
  - Incident Response Planning
    - Recap
    - Handbook
  - Role of OSCT
    - Now / EGEE-I
    - EGEE-II

- **At EGEE-3**
  - Grid Security Incident Handling and Response Guide
    - [https://edms.cern.ch/file/428035/3/OSG\\_incident\\_handling\\_v1.0.pdf](https://edms.cern.ch/file/428035/3/OSG_incident_handling_v1.0.pdf)
    - Replaces LCG Agreement on Incident Response
    - Needed EGEE/LCG context.
      - *Generalised for OSG/LCG/EGEE*
  - Contact management
    - GOCDB
      - *Integrate with site registration process*
      - *Preserve JSPG role-based access*
  - Basic IR planning and model plans
    - *Use-case and role-play useful tools for creating these*
    - *Should be tested in future security exercises*
    - *OSCT is the group to organise this*

- **EGEE-3 to EGEE-4**
  - Grid Security Incident Handling and Response Guide
    - ☹ Little discussion from GDB, OSCT, ROC Managers
    - ☹ Yet to make its way through the approval process
    - 😊 But: no serious disagreement
  
  - Contact Management
    - 😊 Site registration process working
      - *But it is rigorous enough ?*
    - 😊 GOCDB roles and role-base access implemented
    - ☹ Waiting for management interface
      - *GOCDB Advisory Group*
    - 💣 Manual synchronisation of CSIRT data
    - ! Duplicated VOMS functionality ?

- **EGEE-3 to EGEE-4**
  - Basic IR planning and model plans
  - Proposed: *Incident Response Handbook*
    - Make procedures out of policy
      - Quick to update
    - Framework for planning
  - 4 Sections
    - Quick Start
      - *The basic process*
    - Grid resources
      - *References for contacts*
    - Services Reference
      - *Threat and impact by service*
    - Playbook
      - *Worked examples*

- **Incident Response Handbook**
  - ☹️ Almost no comment from OSCT
    - .....?
  - Should we continue ?
    - Need some framework
    - Links in with monitoring and SSC

- **EGEE4 onwards**
  - Incident Response Handbook
  - Quick Start and Resources reasonably ‘complete’
    - First draft
  - Service reference
    - Take a look at each service
      - *‘Assets’, Risks, Impact, Propagation*
      - *Site and Grid effects*
      - *Recovery*
    - Need a suitable encoding
  - Playbook
    - Critical to understanding and debugging process
    - Need broad participation
      - *Regional variations: support, VOs, ...*
    - Feedback to other sections
    - How and what to play ?

- **Operational Security Coordination Team**
  - Formed to provide ROC level support for security activities
  - What is its operational role?
    - “The OSCT .....
  - How is this implemented
    - What structures should be in place
    - What communications etc.
    - Links to operations e.g. CIC-on duty, ROC, GOC, GGUS
    - Time coverage
- **EGEE-II**
  - Dedicated resources for this at ROCS
  - Should lay foundations now
  - So we are ready
- **Meetings**
  - Face to face
  - Phonecon





Enabling Grids for E-scienceE

**Thank You**

[www.eu-egee.org](http://www.eu-egee.org)



INFSO-RI-508833