UKI ROC/GridPP/EGEE Security

Mingchao Ma

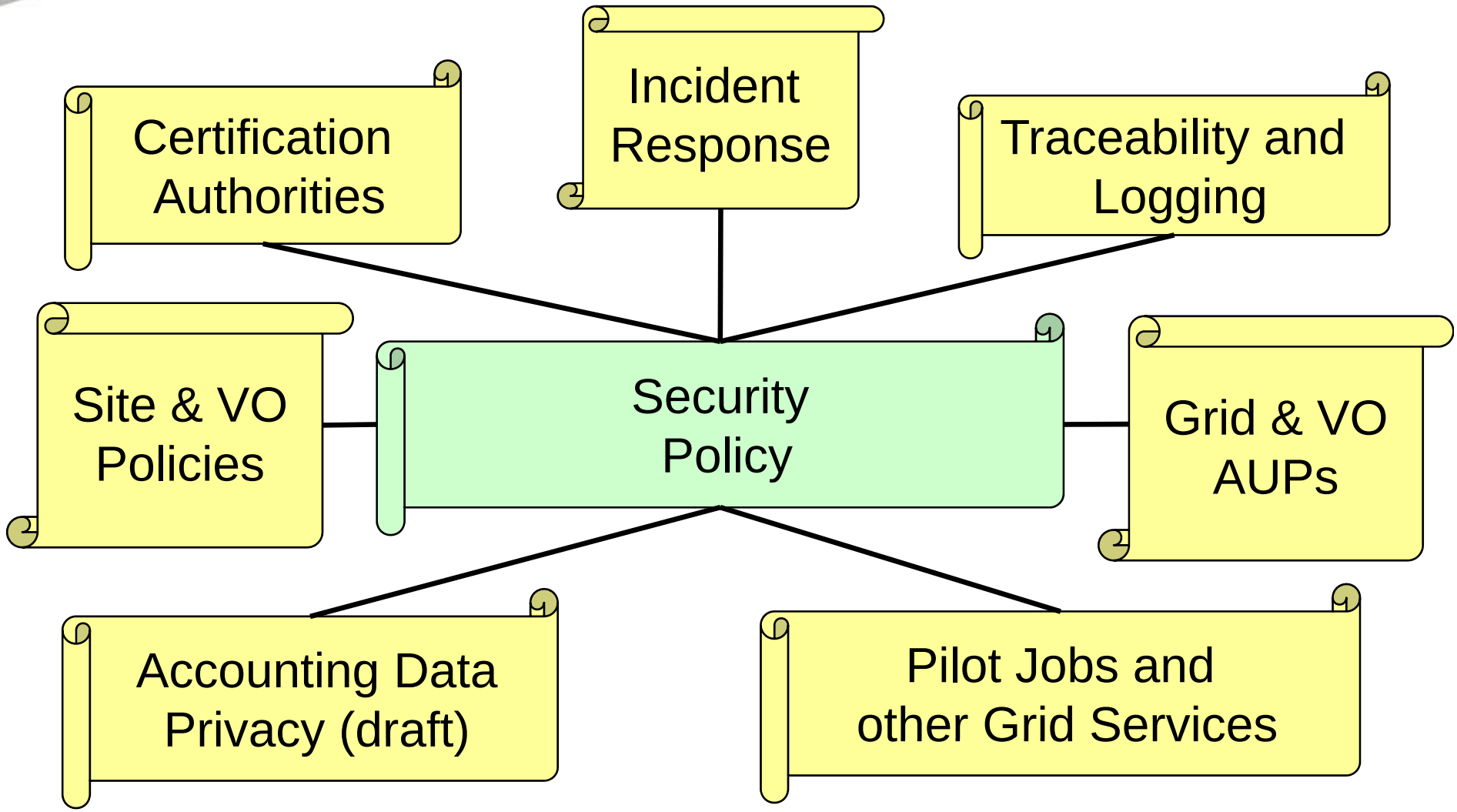
Oxford

22 October 2008

Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

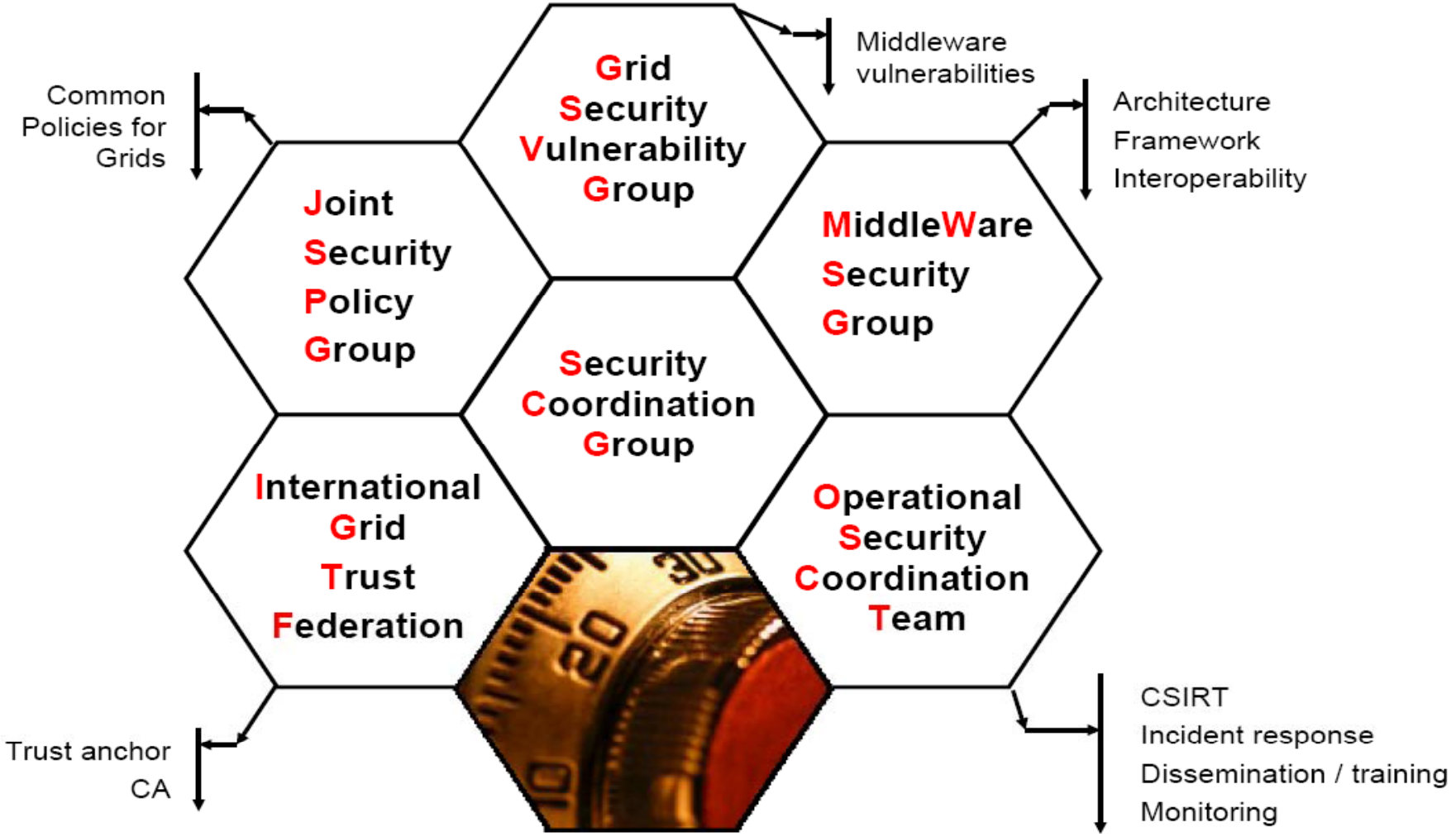
Security Policy



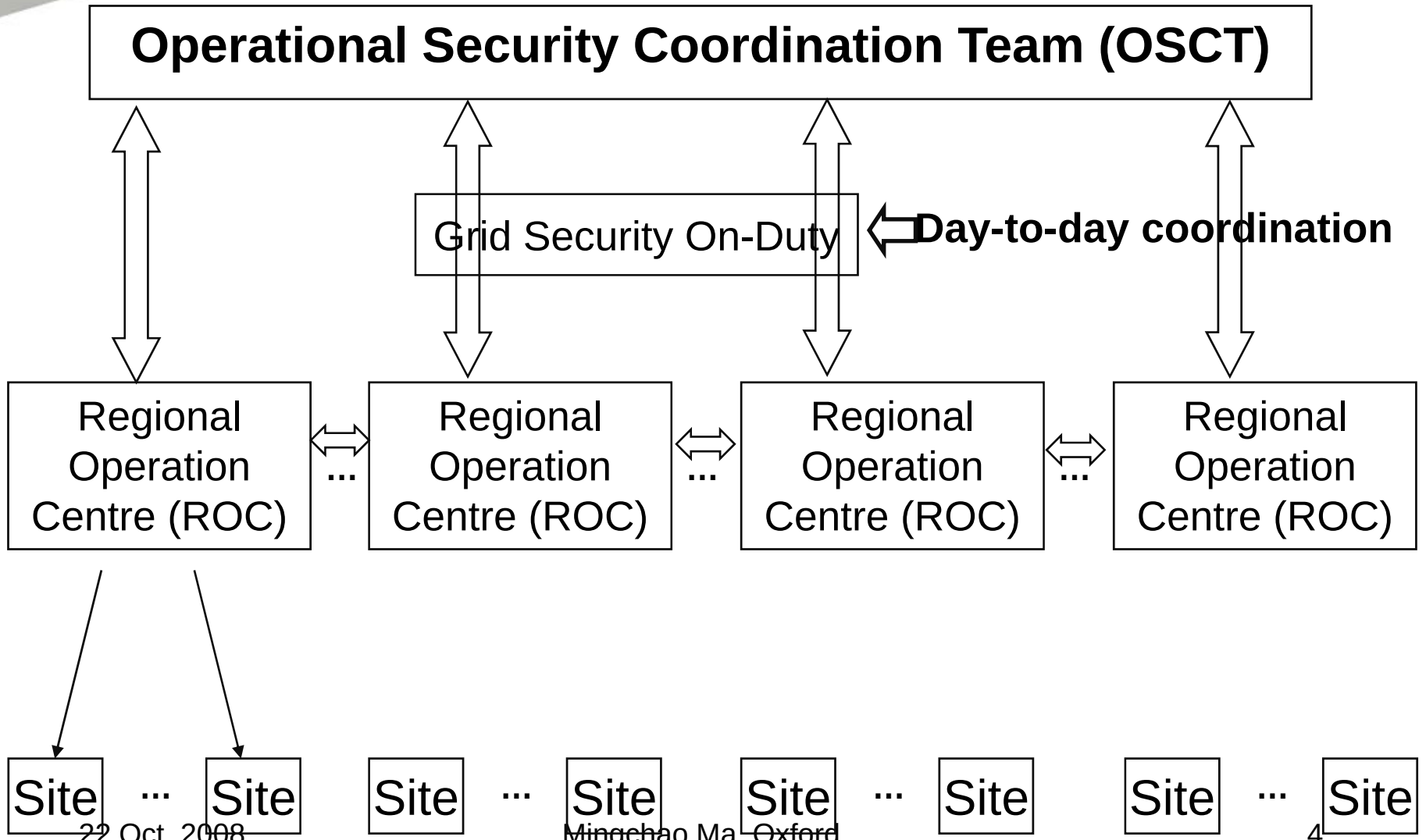
Science & Technology Facilities Council

GridPP
UK Computing for Particle Physics

EGEE Security Groups



OSCT


Operational Security Coordination Team (OSCT)
Grid Security On-Duty
Day-to-day coordination
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
Regional Operation Centre (ROC)
...
...
...
Site
Site
Site
Site
Site
Site
Site
Site

OSCT Activities

- Weekly telephone meeting; Twice F2F meeting per year
- Work together with other security groups to improve Grid security;
- Provide security expertise to sites;
- Handling and mitigating Grid security incidents
  - Procedures; Incident tracking; IR Channel (list, IM) and Security Service Challenges;
- Best practice, training and dissemination
  - Security RSS feed; OSCT website/Wiki; Training events
- Security Tools (monitoring, detection and prevention)
  - Pakiti; SAM security tests
- Analysing and evaluating security risks/vulnerabilities (together with GSVG)

UKI ROC and GridPP

- Security officer, deputy security officer and production manager
- Quarterly report to PMB;
- Day to day operational security issues
- Run security service challenges (SSC)
- Best practices, recommendations, Procedure;
  - Wiki, GridPP security page;
- OSCT-DC rota;
- Handle and response security incident/vulnerability
- … …

Incident Handling – UKI ROC

- Policy & Procedure
  - Detect, Contain, Analysis and Restore
- Communication Channels
  - Copy of security contacts (email & tel. in GOCDB)
  - Tier2 technical coordinators
  - Production manager
  - PMB
  - JANET CSIRTs and University CSIRTS ??

Security Incidents

- So far no “grid incident” ... but will happen (where the grid is the attack vector)
- A few incidents per year within the grids
- From a site perspective, the incidents are often caused by:
  - Failure to apply security patches provided by vendors
  - Poor access control management (ex: root password)
  - Incidents at other sites
  - Unresolved past security incidents (lack of traceability)
  - Incorrect risk assessment (threats were not correctly identified)
  - Shared user community, staff and computing resources between grids and HEP sites make propagation easier

NGS Security

- Policy
  - Regulations for Use of the UK National Grid Service (2005)
  - NGS Security Incident Response policy (2005)
- Security incident handling
  - Building up security contact list
  - NGS-Operation mailing list
- ??

Links

- Policy
  - http://www.jspg.org/
- OSCT
  - http://osct.web.cern.ch/osct/
- GridPP
  - http://www.gridpp.ac.uk/security
- NGS
  - http://www.ngs.ac.uk/security.html

More links

EGEE Security

http://www.eu-egee.org/security/

OSCT Wiki

https://twiki.cern.ch/twiki/bin/view/LCG/OSCT

Security RSS feed

http://rss-grid-security.cern.ch/rss.php

Vulnerability reporting

- grid-vulnerability-report@cern.ch

Incident reporting

- project-egee-security-support@cern.ch
- Incident response procedure
  - https://edms.cern.ch/document/867454/