OSG -- Risk Analysis Report.

D. Petravick

GDB Brookhaven Meeting

September 5, 2006

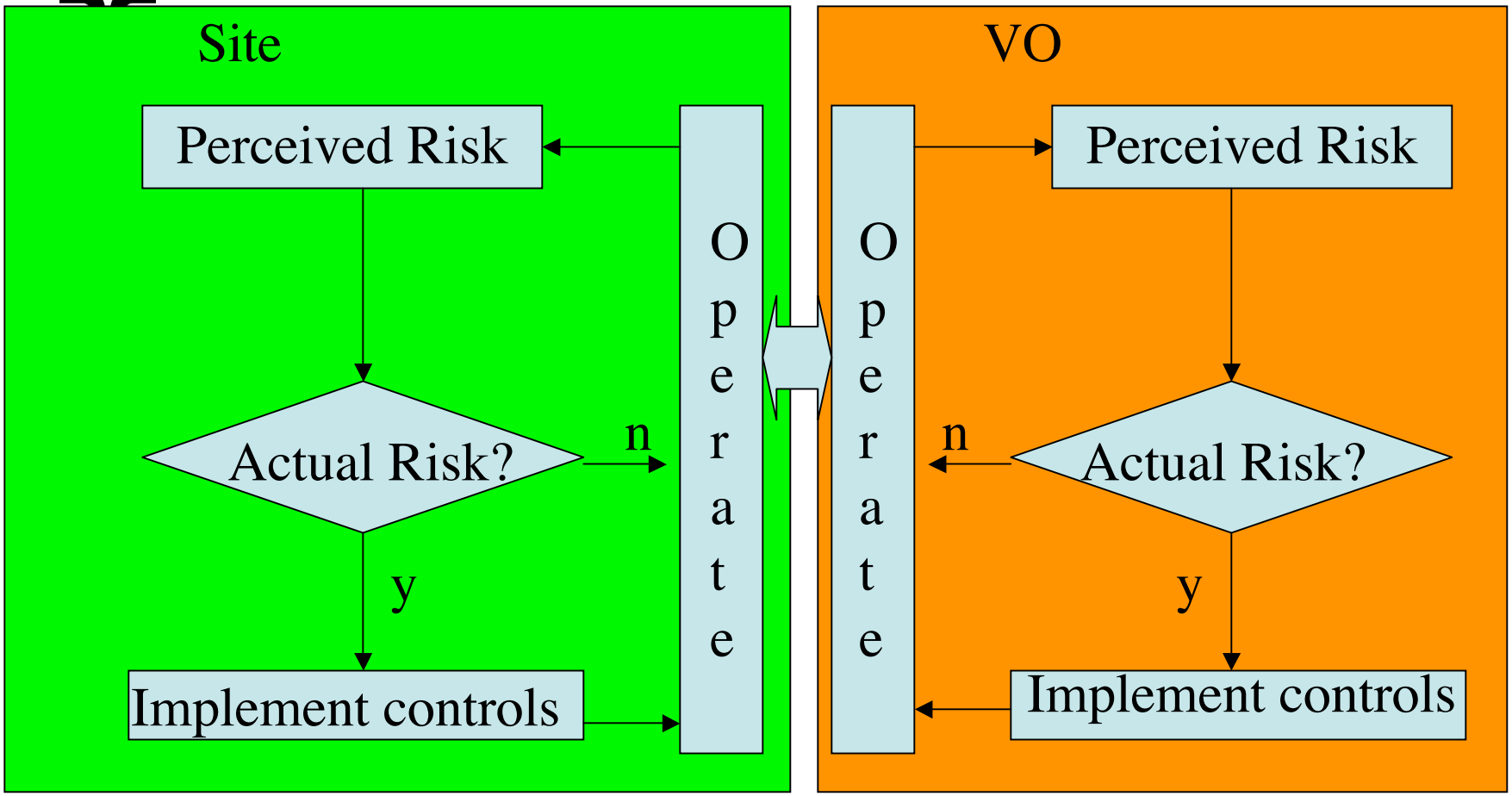
Overview

- Security is a process.
  - Using NIST as guidance.
- Decisions Process is Risk Based.
  - A risk is a **vulnerability** and a **threat**.
  - Organizations implement controls over their activities to obtain **acceptable risk**.
- OSG relies on many organizations feeling secure enough to interoperate.

Risk based view of the world

- Organizations implement **controls** over their activities so as to obtain acceptable residual risk. Each has a security process lifecycle.
  - Satisfaction jointly and severally.
- Each organization is captain of its own ship.
  - However, constrained to interoperate.
  - Organizations: Sites, VOs and Grids.
- Standards (e.g. OSG AUP) aid interoperation.

Site-VO Interoperation



Scaling :-(

- Every organization has to reduce its risk to acceptable residual risk, and the security has to interoperate.
  - Identified trust.
    - Something specific is relied on
    - Is not checked each time.
  - Apropos Managerial, Operational and Technical Controls, for trust items.
- Scaling is a problem, work needs to be done
  - Common standards -- I.e OSG AUP.
  - Fewer entities -- Aggregate the small.

Liaison work

- TAGPMA, DOEgridPMA, EUgridPMA
  - A PMA is Policy Management Authority
- MWSWG -- Meeting at SLAC with emphasis on interoperability.
- GGF -- Global Grid Forum
- JSPG -- Joint Security Policy Mgemt Group
- DOE Security CET
- DOE Grid Briefing
- VO AUP
- Grid Policy working group

OSG Security Documentation roadmap

- Main security documents
  - Risk Assessment (First releasable version)
    - For the Core
  - Security Plan (Based on the above)
  - Contingency Plan (Less priority)

NSF thinking

- **Draft Article for Agreements for Large Facilities and FFRDCs**
- July 24, 2006
- "…Security for **all information technology (IT) systems employed** in the performance of this award, **including … information**…awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee's organization as part of the organization's IT security program…. including, but not limited to: **roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training, and notification procedures** … **appropriate** security measures **required of all subawardees, subcontractors, researchers and others** who will have access to the systems employed in support of this award…..

Outline of RA.

1. Identification
2. Methodology
3. Threats
4. Vulnerabilities
5. Impact Analysis
6. Control Analysis
7. Risk Mitigation and Residual Risk Level
8. Control Recommendation
9. Risk Mitigation

Identification -what is the OSG

- CORE OSG as a collection of processes
  - Software Stacks and Release
  - Communications and Web Presence
  - User's
  - OSG hosted VO
  - OSG Validation, Monitoring and Accounting
  - Inter-Grid Operation
  - Security
  - Trust Relationship

Threats to OSG

- Careless or uninformed authorized person
- Squatter
- Vandals
- Thief
- Malware Author
- Spy
- Alarmist

Vulnerabilities

- Reliance on Third Parties.
- Improper (core/user) Actions
- Remote Access.
- Exploits latent in Vulnerable Software.

Impact

- Impact to be consistent with LCG T2 requirements (among others)
- The goal is to get to LOW
  - Occurrence -- Less than 5x/year
  - Perception … OSG can be Relied on.
  - No single occurrence disrupts … all.
- Then there are medium and high, but the point of the analysis is to get to low.
- How do you get to low? Controls.

Controls

- Written as if all are in place.
- Management
  - ***Integrated Sec Mgt***; Sec processes; **Trust Relationships & Agreements**
- Operational
  - Awareness; ***Response***; **Data Integrity**; Config Management; **Vul. ID**; Physical
- Technical
  - Monitoring; Scanning; Control of people

Risk matrix

- Contribution from each process area.
  - ~80
  - Subject to continuous improvement.
- Format
  - Description of Risk
  - Expected Occurrence
  - Severity
  - Grade
  - Status

Example Risks

Note: Many Risks can only be addressed By operational or management controls

- Disclosu
- Users unaware of OSG AUP, may violate policies out of ignorance, may fail to report security incidents
- 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)

Status

- Discussed at
  - OSG Consortium meeting
  - OSG Council
- Basis for security plan
  - Implement controls for each family.
  - Test and evaluate controls to make sure they are in place and effective.
- Living document goes into the security lifecycle for maintenance.

Summary

- Progress made in setting up a security process.
  - Risk analysis emerged from small group.
  - Principal of ISM employed.
- Emphasis is on acceptable risk.
  - Jointly and Severally.
- OSG will develop
  - Few technical controls
  - Many operational and managerial controls.