QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

OSG Operational Security

D. Petravick

For the OSG Security Team: Don Petravick, Bob Cowles, Leigh Grundhoefer, Irwin Gaines, Doug Olson, Alain Roy, Vikram Andem

EGEE06

Sept 25, 2006

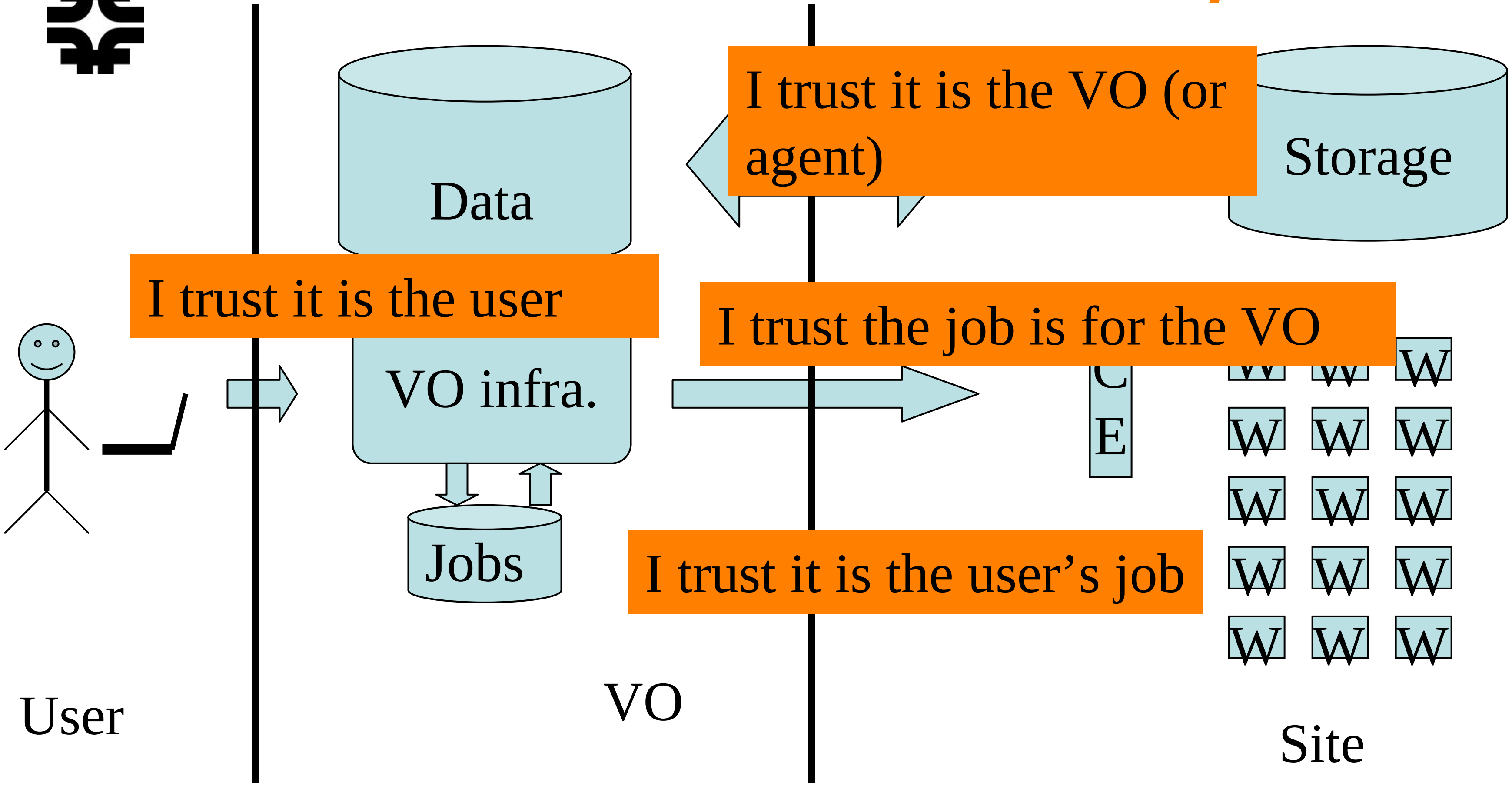
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Background

- OSG Project now funded by DOE and NSF as a national production level distributed facility.
- Moves on from the Grid3-Trillium era as being a relied upon, sustained infrastructure.
- As a contributor to the WLCG OSG must satisfy the security requirements of the LHC.
- OSG Security is building on prior work of Trillium collaborating with EDG, EGEE, WLCG.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Illustrative example



I trust it is the VO (or agent)

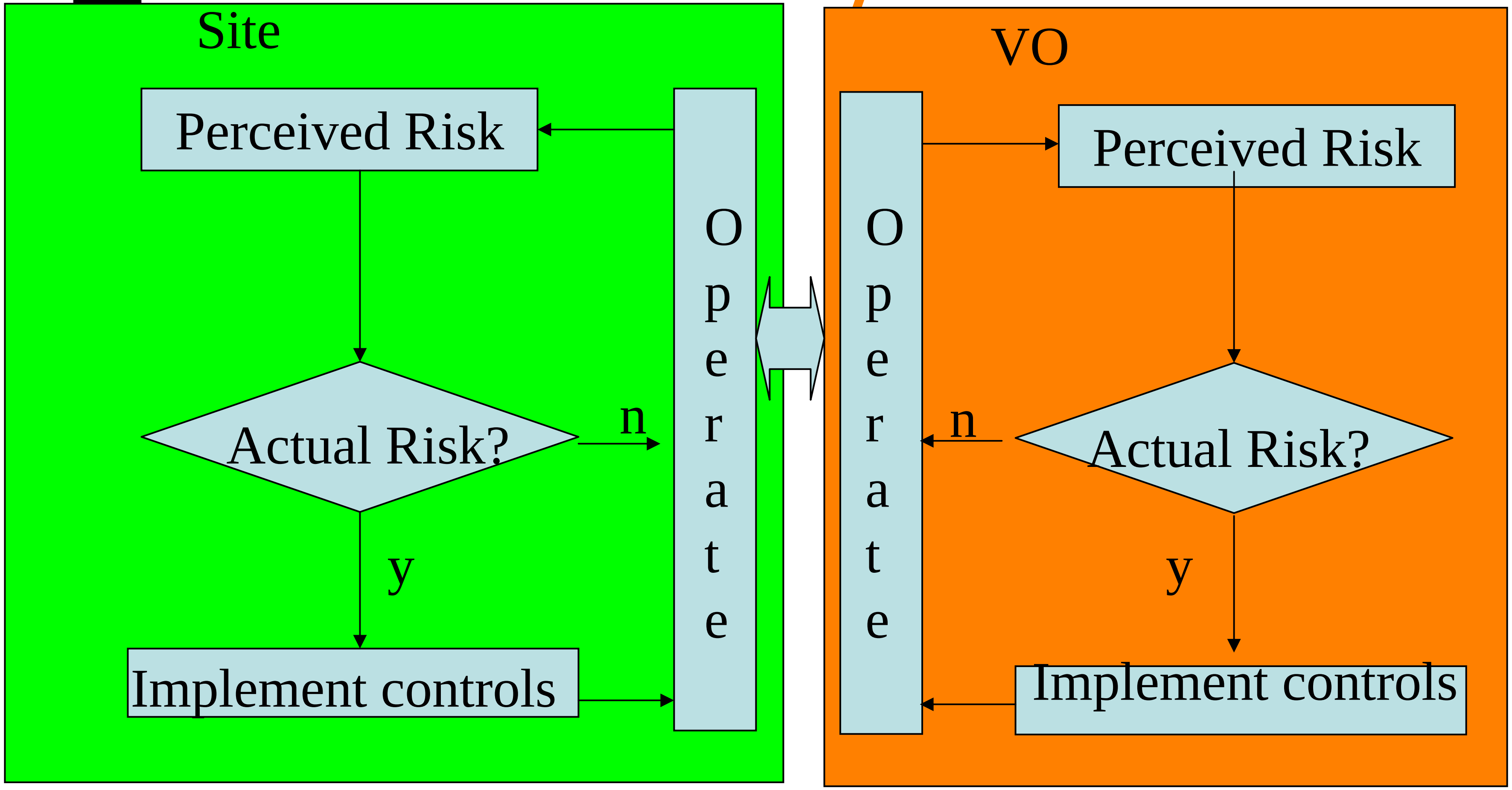
I trust it is the user

I trust the job is for the VO

I trust it is the user’s job

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

OSG Site-VO Interoperation



QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Risk based view of the world

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

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Two Broad Documents in the NIST pattern.

- Risk Assessment
  - – Analyzes
    - threats and vulnerabilities
    - With mitigation in 13 control clusters
    - To see if the residual risk is acceptable.
- Security Plan
  - – Explains each control cluster.
  - – Establishes tests of effectiveness.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

(Imagined) Security Assessment

- Do you have focus?
  - Have you written down what is important and what is not (Risk Assessment)
- Have you written down your Policies?
- Do you have plan? Do you know it is working? (Security Plan)

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

RA(1) Threats to OSG

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

RA(2)Vulnerabilities

- Reliance on Third Parties.
  - This is a “whopper”.
- Improper (core person/user) Actions
- Remote Access.
- Exploits latent in Vulnerable Software.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

RA(3)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.

SP(1)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

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

SP(2)Draft Cluster -- Vul. Mgt.

- General Vulnerability Reporting
- Primary Vulnerability Reporting
- Secondary Vulnerability Awareness
- Vulnerability Mitigation
- Vulnerability Communication
- Vulnerability Awareness

(SP3)DRAFT Primary Vulnerability Reporting

- Plan:
  - … entities operating a service or running a process for the OSG have primary responsibility for identifying vulnerabilities.
  - … requires services and processes to report vulnerabilities inconsistent with acceptable risk to the OSG. to the OSG security officer. Acceptable risk is defined in the OSG Risk Assessment.
- Evaluation
  - This control is evaluated annually by an inspection of the vulnerabilities logs
    - Comparing the primary reports to reports from the secondary chain.
    - Comparing the primary reports to vulnerabilities exploited in incidents.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Summary

- Security interoperation is required for grid interoperation.
  - Without work, interoperation is n**2 agreements.
  - Each organization must satisfy its self-identified security needs.
  - Common policies (such as the user AUP) speed up the n**2 process.
  - In the OSG, VO’s with heavy infrastructure seem to face diligence approximately equal to a site.
  - We are hear to learn about EGEE.
  - One way forward which may provide maximum interoperation and scaling seems to be to agree on Control Clusters, and then drill down.
- OSG has begun writing plans in a structure based on an understanding of NIST.
- OSG is working with the Site and VO Managers to clarify and collaborate on Security matters (as well as with EGEE and TeraGrid).