What you need to know Security Awareness for the OSG

D. Petravick

OSG Security Officer

March, 2007

Outline

- Unit 1: Overview and vision. (~15 slides)
- Unit 2: What is the Core? How is it secured? (~30 slide)
- Unit 3: What about the rest, are we chopped liver?(~15 slidea)

Unit 1
Overview and Vision

Where we are at

- OSG is not a site, it's a consortium
  - Try to specify the OSG's interest in services that are provided to the consortium by agreement.
- Careful thinking about what a grid organization can and cannot do.
- This is version 1 of a top-down complete approach.
  - Not everything is finished.
  - Can collect your input during presentation.
    - Recall that this talk is ~60 slides.

OSG top-down security in a nutshell.

- Goals of security:
  - Reduce risks to "acceptable" risks.
  - Completely secure => trivial system
- OSG Methodology:

  Focus on the most important Risks.

  Implement controls to achieve acceptable risk.

  .

Practiced by all parties, commensurate with responsibility

- Experts cannot sprinkle on security
  -- Place responsibilities on those who are in the situation to best bear them

  Everyone is obliged
- Everyone is obliged
  - To work diligently.
  - To work with the OSG controls.
  - To feed into process.
  - To be proactive.
- Need to have knowledge commensurate with responsibility.

Risk Based Approach

- A way to
  - reason about our security issues
  - to justify decisions about applying our limited resources in the best way.
- A way to defend ourselves against "why did you not buy everything" criticism when something goes wrong.

Risk in a Nutshell

- Risk : f(Vulnerability, Threat)
- Vulnerability -- Unlocked door.
- Threat -- Likelihood of someone exploiting the door.
- Increasing function, but a big hole with no exploiter is a small risk in the present.
  - Low present risk does not imply low future risk.

OSG threat actors

- Careless or uninformed authorized person
- Squatter
  - unauthorized persons who use our resources, but not at an economically significant level
- Vandals
  - web page defacers, data destroyers, vandalize reputation
- Thief
  - take services, money, things of value
- Author who writes malware
- Spy
- Alarmist

Risk Analysis

- Systematic way of thinking about risk.
- To see which are worth worrying about.
- Primary OSG goal: Low Risk
- "A security event has LOW impact if
  - it occurs less than 10 times per year
  - AND
  - does not disrupt the perception of the OSG as a computational facility that can be relied
  - AND
  - no single occurrence of the event disables the substantially all OSG's operational Compute Element service for more than two days."
- Would, of course like to have very low risk

Hypothetical Example

- Something in the OSG stack allows worker nodes to be rooted, No exploits noted yet.
- Fix is many days away.
- Assume three possible actions:
  - Shut the grid down.
  - Use white lists to restrict usage to a more trusted class of users.
  - Do nothing.

Security Plan

- Lists the controls that are in place to obtain acceptable risk.
- Each control
  - has a rationale.
  - Has prose saying what the control is
  - test which is made to determine it is in place and effective.
- Status -- We have an approved plan, and are implementing controls.

Unit 1 Summary

- In the present
  - Justify course of action in terms of risk.
  - Be comfortable defending the decision in case of breech.
- Affect Future -- what does this mean in the long term

  Change our deliverables?

  Change our processes?

Unit 2
Core OSG

Core OSG:what is it?

- NOT the activities of Sites or VO's.
- IS the activities the OSG is organized to do.
  - Funded activities
  - Contributed activities

Process Overview

- The OSG Core has a risk analysis, security plan, and process,
  - Modeled on traditional organizations.
  - But Adapted to our consortium.
- The Security Plan is a collection of specific actions we undertake to protect ourselves.
  - In NIST security jargon these are called controls.

Structured thinking about controls

- Management Controls -- Our plans about Security.
- Operational Controls -- How we count on people behaving.
- Technical Controls -- How our systems and software behaves.

Integrated Security Management

- The line managers of the OSG are primarily responsible for the computer security aspects of their work.
- This work is governed by OSG computer Security process.
- This philosophy ensures that computer security, like safety, is not an arbitrary set of prescriptive rules imposed from the outside, but rather a part and parcel of all core OSG activities.
- Each area of the core OSG has an individual to act as their OSG Security Coordinator. This individual aids the computer security team.

Security Office Roles

- The OSG Security Officer
  - Is responsible for coordinating, monitoring, responding to, and supporting the security of the OSG infrastructure.
  - Leads the Security Team.
  - Promotes the mechanisms of integrated security management and ensures that the OSG Staff know their responsibilities and implement them.
  - Organizes the assessment of the security controls, drawing upon others as necessary to evaluate the operation of the security office itself.
- The Deputy Security Officer and the OSG Security Policy Officer are members of the Security Team

Roles and Responsibilities

- The OSG Executive Director
  - is responsible for the security of the OSG core assets
  - is the security contact of the OSG VO.
- The OSG Facility Coordinator
  - is responsible for the security of the OSGF assets.
- The Software Coordinator
  - is a member of the security team.
  - is responsible for the security of the VDT asset.
  - Is a contact for all aspects of security related to the providers of software in the VDT and OSG software caches.

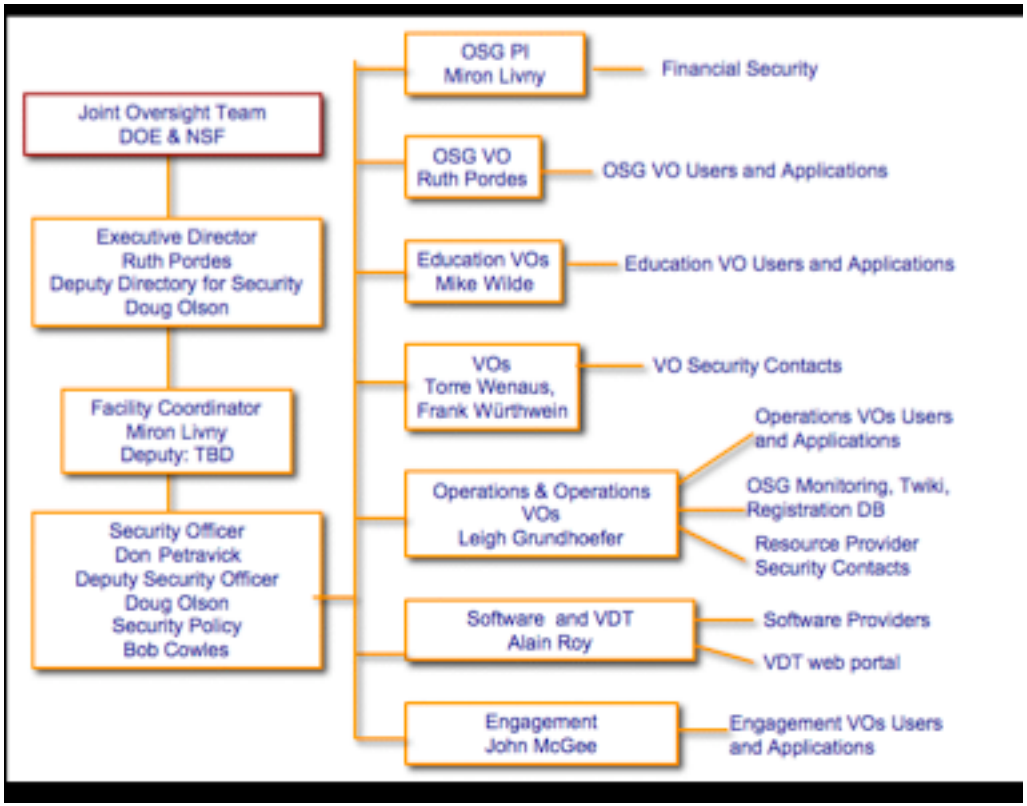
Roles and Responsibilities

- The Operations Coordinator
  - is a member of the OSG Security Team.
  - is responsible for the security of the core OSG operational services monitoring, databases etc.
  - Is responsible for communications with and training of the Resource Security Contacts.
  - is the security contact for the Operations VOs.
- The Applications Coordinators
  - Are members of the OSG Security Team.
  - Are responsible for communicating with and training the Virtual Organization Security Contacts.

Roles and Responsibilities

- The Education Coordinator
  - is the security contact for the Education VOs.
- The Engagement Security Contact
  - is the security contact of the Engagement VOs.

Roles in the OSG



Awareness for Managers

Accountability

- Users of OSG resources are given authority to use the OSG through a trust relationship VO of which they are a member.
- In the OSG, the VO holds responsibility for the associated management controls for that user.
- Hence, Virtual Organizations stand accountable for the actions of their users.

Accountability

- Virtual Organizations face the possibility of losing their privilege to access resources through the OSG if they fail to exercise the requisite controls.
- The OSG Executive Director can bar a VO from accessing resources by means of the OSG.

Accountability

- Providers of OSG resources must abide by the OSG service AUP.
- If the AUP is violated, the OSG Executive Director can bar the responsible party from offering services via the OSG.

Computer Security Lifecycle Meeting.

- The OSG Security Officer holds periodic meetings. The purpose of the meeting is to discuss operational security matters, to assess the security status of the OSG, and to assess and execute change control of the OSG's security policies, plans, procedures
- Agendas for the meeting are prepared, and meeting notes are kept and distributed on the security-discuss-l mailing list.

Operational Controls

Risk Analysis

- Key concepts
  - Risk = Threat + Vulnerability
  - Minimal Acceptable Risk.
- Refer to Unit 1.
- Integrated Security Management requires you to be able to assess risk.
- Security office can help you.

Trust Relationships

- What is "trust" in a computer security context?
- "A" relies on "B" to do something and does not check it every time.
- A trust relationship is the presumption that trust exists.
- This is a key concept in Open Science.

Trust Relationships

- Two kinds
  - Default the operational body of security and operational plans, policies, and methods will be abided by based on prior collaborative work (typically over an extended period).
  - Detailed there are additional written agreements defining the trust relationships between the parties.

Example - Detailed Relationship.

- Example: opensciencegrid.org and content incidents.
- A type Content incident -- defacement
  - Threat -- Vandals.
  - Risk -- embarrassment.
  - “researchers” who actively look for this stuff.
  - of course OSG is embarrassed who else?
    - Follow the DNS name -- DOE lab.
    - Follow dotted quad -- institution hosting site.
- Document mandatory incident reporting and content incident.

Role based Training

- This is V1.
  - Available on OSG site.

Incident Handling

- Mandatory reporting to security at opensciencegrid.org
  - List has a human in the GOC behind it 24x7.
- OSG response is complimentary the response given by a site.
  - Do not hesitate to involve site responders.
  - OSG Response
    - Follow up on trust relationships
    - Looks for impact elsewhere in the OSG grid.
    - If OSG stack/grid methods involved, follow through
    - Deal with similar vulnerabilities in OSG.
    - Assess our own process

Data Integrity - Background

- Availability, Integrity and Confidentiality
- The Plan speaks to the CORE does not speak to VO's or to the qualities or properties of data areas available to them on the sites.
- Availability and integrity are obtained by sound administration of the underlying systems hosting a core service.

Data Integrity -- Confidentiality

- How to build a system for the OSG to hold data closely? OSG has confidentiality classes:
  - Sensitive Personal information.
  - OSG Restricted data (stronger controls)
  - OSG Limited data (controls)
  - Public Data (no controls)
- Distribution
  - by document
  - by service

Sensitive Personal Information

- Kinds of data we should tell an institution to hold, not a OSG core system.
- Why?
  - Expense of dealing w/it
  - Far away from focus of enabling open science
- What is it exactly.
  - Security officer maintains a list.
  - Regular and even-driven maintenance of list.
- Current Seed list:
  - SSN# Credit card #s.

OSG Restricted Data

- Author
  - Labels documents "OSG Restricted".
  - Names and approves distribution list.
  - Evaluates the trustworthiness of non OSG core recipients. Instructs them on handling
- Handling rules:
  - Do not distribute
  - Uses information for OSG business purposes only.
  - Holds with reasonable care.
  - Deletes when no longer needed.

OSG Limited Data

- Meant for things we do not want appearing on web pages
- Author
  - Labels documents "OSG Limited"
  - Evaluates the trustworthiness of non OSG core recipients. Instructs them on handling
- Handling rules:
  - Evaluates the trustworthiness of non OSG core recipients. Instructs them on handling.
  - Holder may re-distribute for OSG Business purposes.
    - But evaluates the trust in non OSG Recipients.
    - Instructs non OSG recipients in handling
  - Uses information for OSG business purposes only.
  - Holds with reasonable care.
  - Deletes when no longer needed.

OSG Public Data

- Author puts no label on data. --public.

Example of data in each class

- Credit card information is Banned.
- An OSG proposal might be Restricted.
- The security discussion list is Limited.
- This talk is an example of public data.

Wrinkle - Distribution by Service

- Well and fine for email, what happens when we have computer generated data?
  - Example would be the OSG accounting data set.
- Service owners classify their data in the same confidentiality schema.
  - Analogous discussion is has when enabling access to service.
  - Access to non OSG is bounded in time, duration related to risk.
  - Some writing (e.g. email) is retained by service owner.
  - Some services can only support group level access controls.

Confidentiality Backstop:

- The OSG Security Officer can classify any data in Core OSG, and issue a plan for dealing with extant copies of the data.

Configuration Management

- Two Classes of configurations
  - Services in the core
  - Recommended or reference configurations for the services which are downloaded and installed from the OSG software stack.
- Controls not yet implemented, include Monitoring, Version Control, Review of propsed Changes.

Vulnerability Management

- A vulnerability is a flaw in a system which leaves it open for exploitation.
- A goal of the OSG Security processes is to remove vulnerabilities presenting unacceptable residual risk to the OSG.
  - Core services work autonomously to identify and remove vulnerabilities in their systems.
    - Basic diligence for service providers is to be in communication with software providers.
  - Have to live with a significant vulnerability?
    - Don't do it alone.
    - Report to security at opensciencegrid.org

Physical Controls

- Production core services.
  - Machines shall be in physically secure
    - Locked area
    - Protection against walk-ups
    - Run the minimal level of services
    - Have a plan for sustaining service in case of operational disruptions or emergencies.
    - Retain system and service logs for at least 30 days.

Monitoring

- Monitoring is looking at existing data for security purposes.
  - One tool for assessing the security state of the OSG.
  - Seek to compliment efforts at sites.
    - Some things are better viewed at the grid level
  - Seek to re-use data sets which are acquired for management purposes when feasible.
- Status -- investigating the utility of Accounting data.

Access Control for Core OSG

- The technical direction for Core OSG is services.
- The guidance is to use X509 certificates.
- VOMS Certs? -- perhaps - a development.

Technical Controls

Unit 3
Non-Core Trust Relationships

Scanning

- Is the active probing of deployed services, to determine their security qualities.
- The OSG expects local administrators to scan services as part of local security assessment.
- Status: implementation of scanning is pending.

Non-core

- The OSG compiles a software stack furnished by software suppliers. The software stack allows VOs to interoperate with sites by means of services.
- VO's consist of a number of users. VO's interacts with their users, The OSG provides various level of support for this.
- Plus others (I will gloss over)
  - Identity providers and such.

Software Suppliers

- We are discussing the creation of a software AUP which creates security expectations on our suppliers.
- Items
  - Vulnerabilities process.
  - Configuration management
  - Security related qualities -- e.g. stand up to scanning, buffer overflows in code, and the like.
- Key players: Extention Coordinators, Software Coordinator, Security Officer

"Grid incident"

- The main direction of OSG security is the integrity of OSG Services. -- "grid incident"
  - Current operational properties
  - Future properties
- The OSG play only a communications role for site incidents.
  - For example exploits via ssh.
  - Why? We are not a substitute for site security.

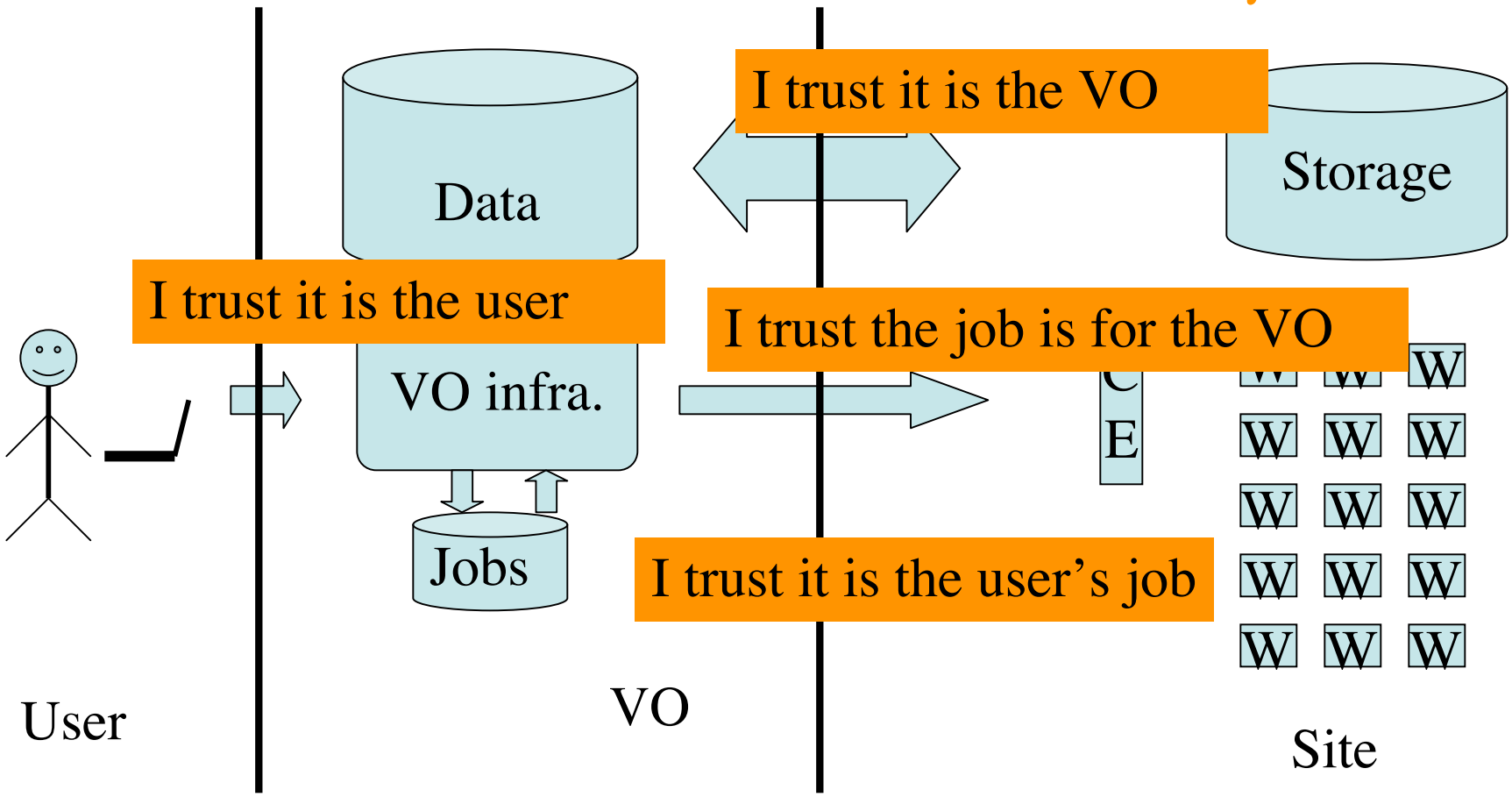
VO and user relationships

- The OSG expects VO's to deal with the users.
  - Users Aware of and abiding by the OSG AUP.
  - OSG Registration Agents.
- OSG believes it needs to support VO's by provisioning process and tools.

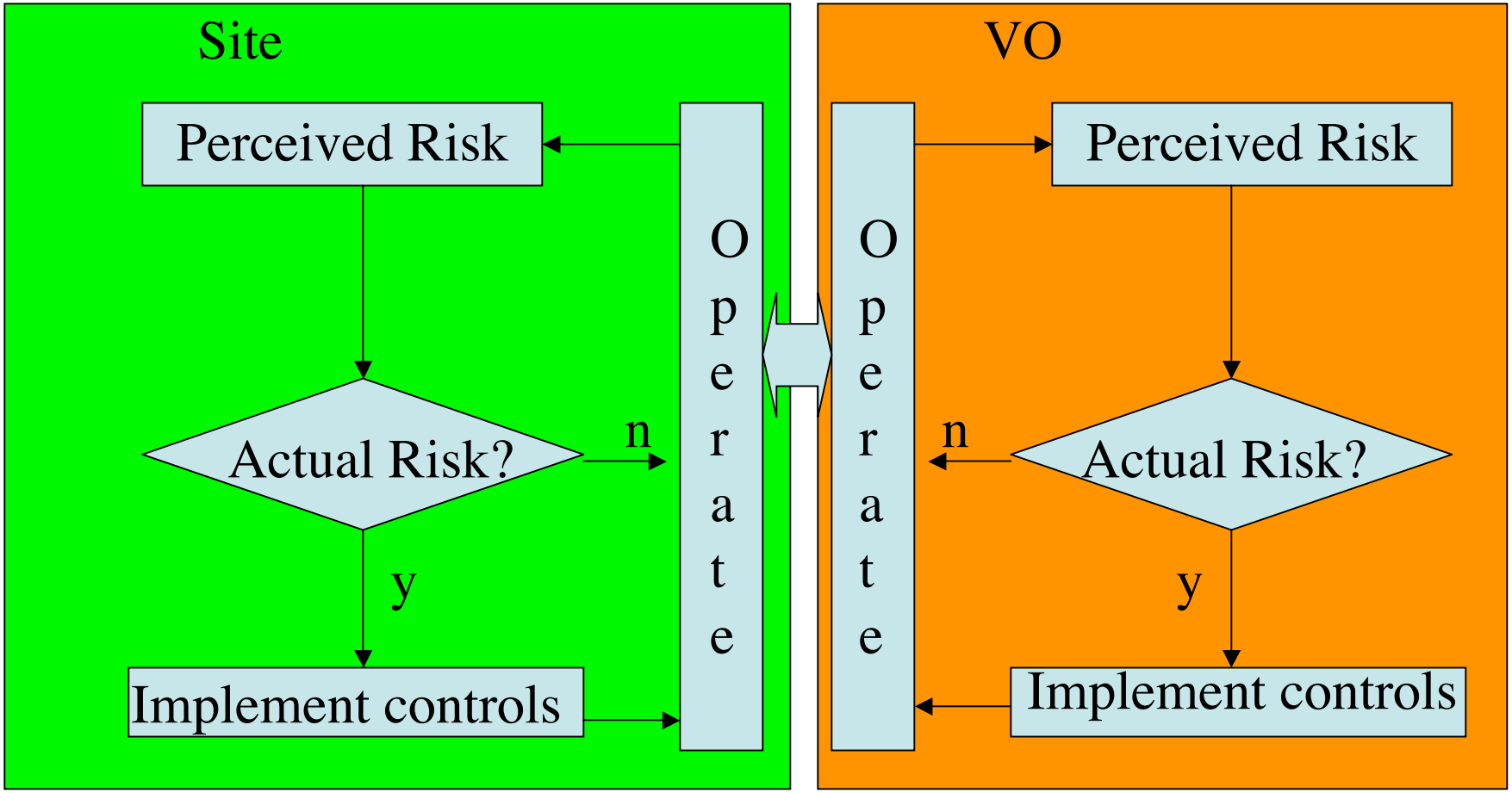
Trust among VO's and Sites

- The OSG does not bear security responsibilities that are best borne by sites and VO's.
- Parties provisioning services have to be diligent, whether they are sites or VO's.
- OSG allows and encourages VO's with thick software stacks of their own.
  - Not all software is VDT-furnished.
  - Not all services are site-run.

Illustrative example



Site-VO Interoperation



Service AUP

- Current -- in a nutshell -- "Handle credentials carefully".
- Future -- You acquire all the diligences of a a service provider.
- For any OSG role -- including sites, Vo's and Users.

OSG's direction

- Recall: Osg cannot bear responsibility for a VO or site
- OSG will create a number of AUP's that are reasonable and embody good practices.
  - Done with the JSPG framework, when possible.
- The AUP's facilitate pair-wise security discussion by defining standard terms.
  - Such discussions would be strucutured.
- IF no pair-wise discussion? At least something has been agreed to.

Interactions w/ CORE osg

- Software coordinator and extentsions coordinator create awareness of the software AUP.
- coordinators create awareness of the AUP's for VO's and sites.

Review

- The OSG compiles a software stack furnished by software suppliers. The software stack allows VOs to interoperate with sites by means of services.
- VO's consist of a number of users. VO's interacts with their users, The OSG provides various level of support for this.