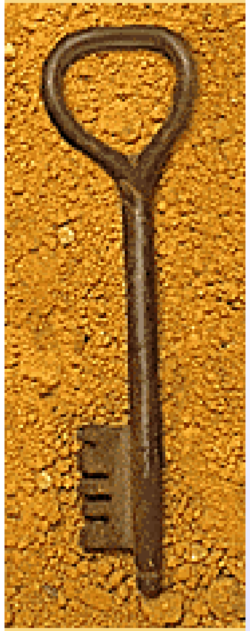
How the NIST Computer Security Process informs OSG Security Plans

Irwin Gaines - FNAL

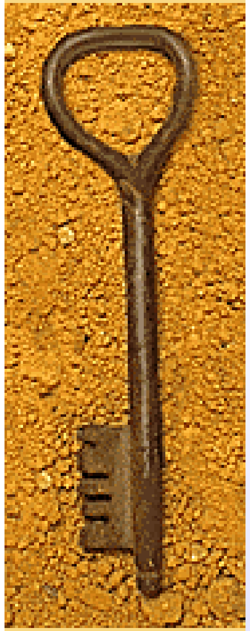
6-Jun-2006



Outline

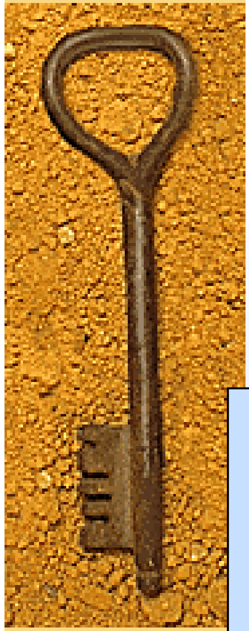
- What is the NIST security framework (high level overview)
- Why should this have anything to do with OSG?
- More details about the NIST process
- Preparing OSG security plans (and relationship between OSG security and facility security)

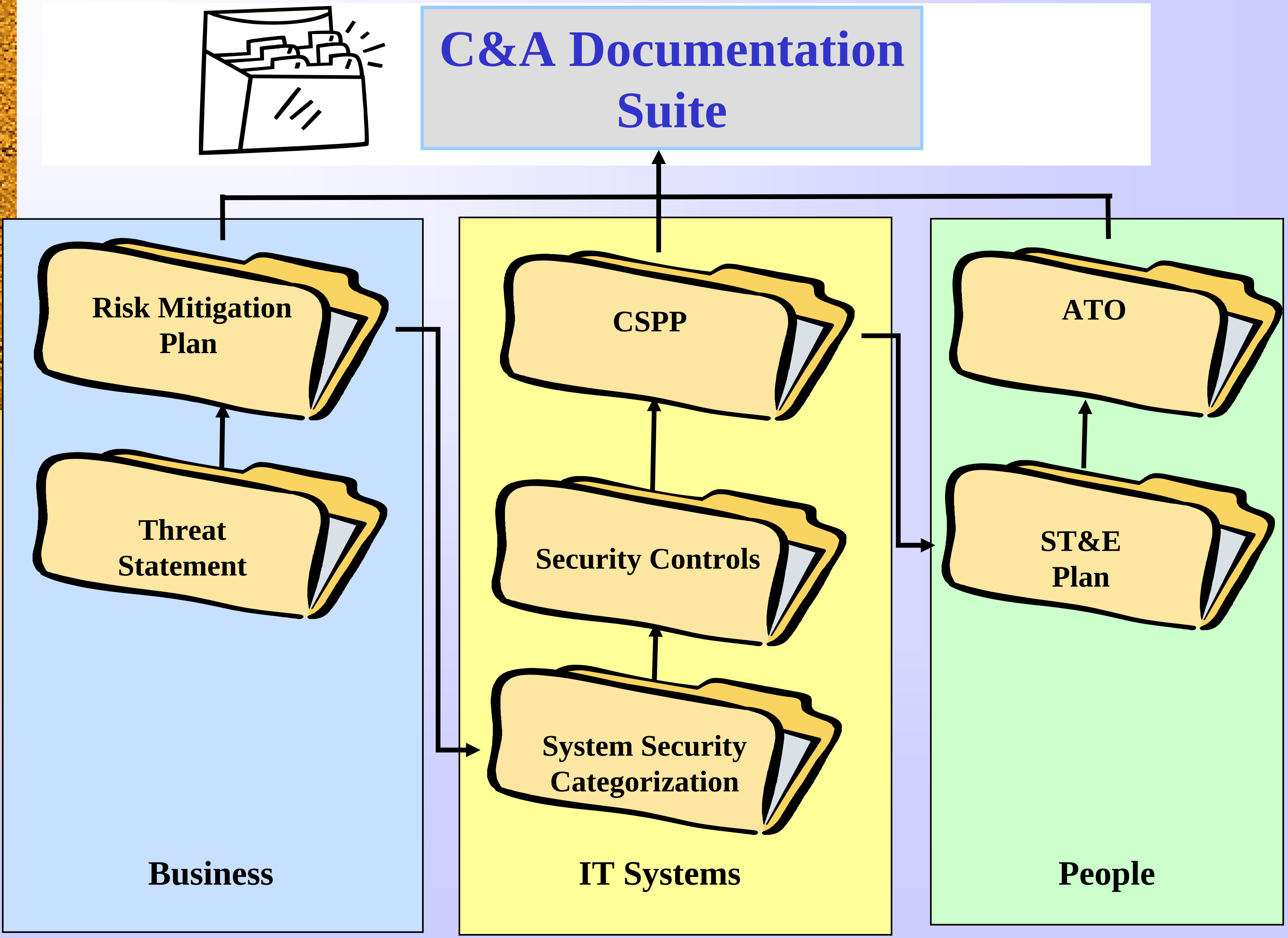
What is NIST?



- National Institute of Standards and Technology has published a large number of guideline documents about various aspects of computer security
- New legislation, OMB guidance, and DOE orders require all DOE labs to use NIST standard framework for computer security
- Office of Science trying to get out in front with program of “site assist visits” (establish OS as center for excellence)
- Fermilab has rewritten their security plans in accordance with NIST

Required NIST documents





C&A Documentation Suite

Risk Mitigation Plan

Threat Statement

Business

CSPP

Security Controls

System Security Categorization

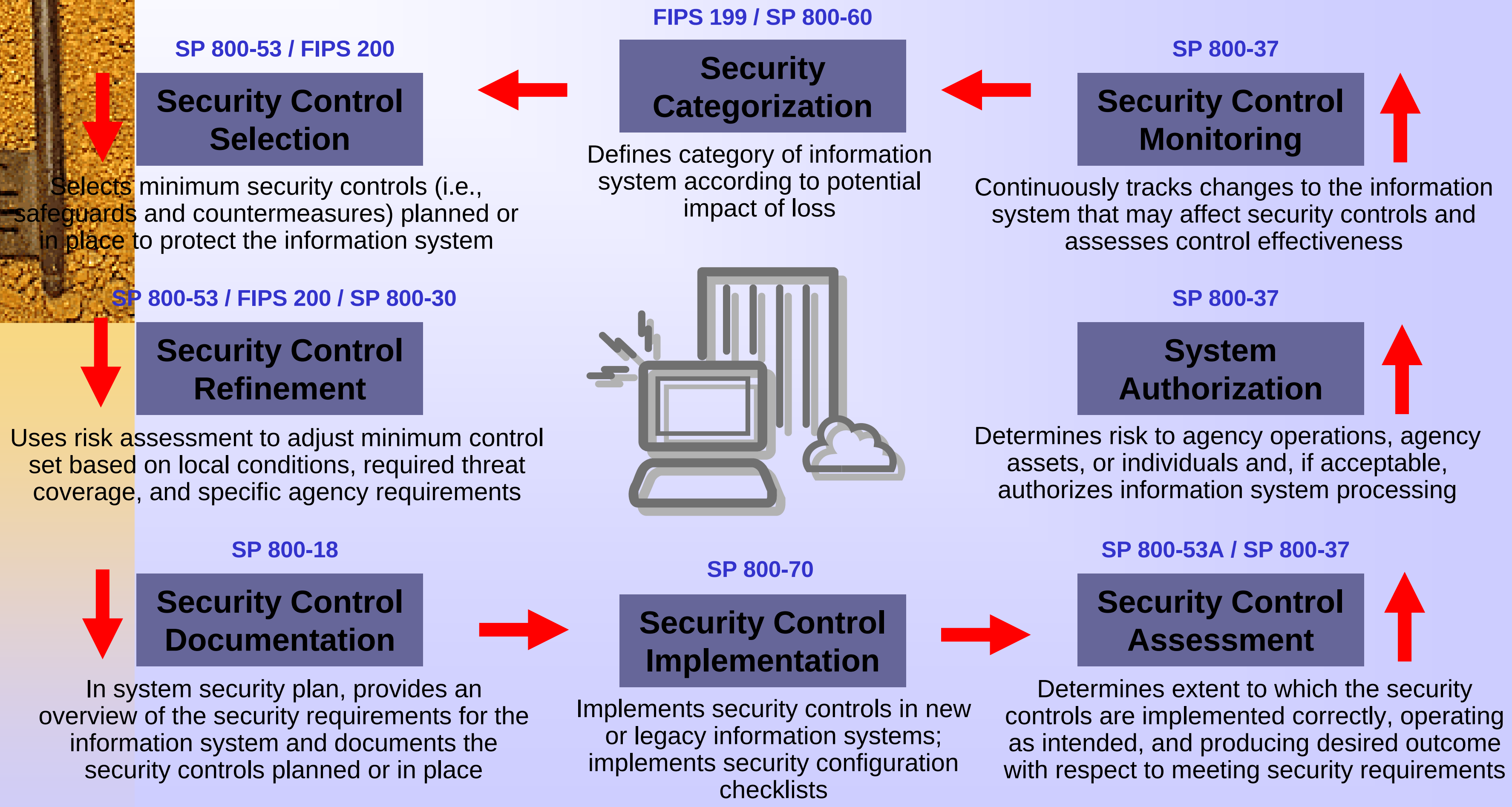
IT Systems

ATO

ST&E Plan

People

NIST Process



FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-18

Security Control Documentation

In system security plan, provides an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

SP 800-37

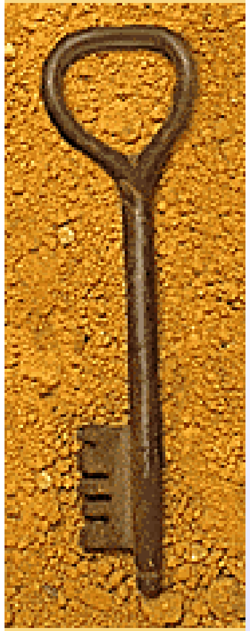
System Authorization

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-37

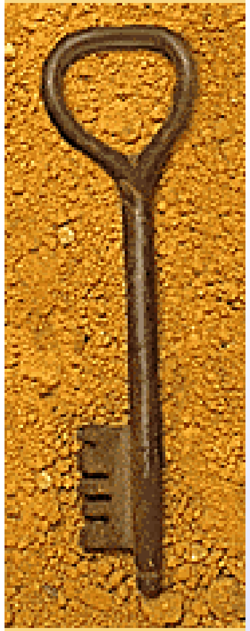
Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness



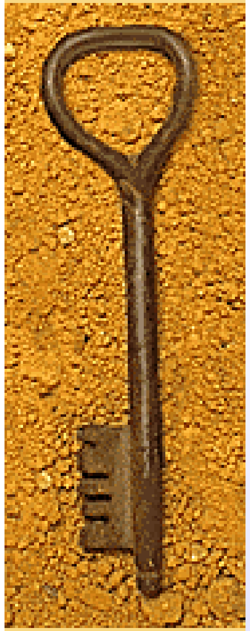
NIST at FNAL

- Looks somewhat daunting at first glance, but not really as bad as it seems
- We were initially very concerned that the NIST documents were very prescriptive (eg, you must change passwords every 6 months and use at least 12 characters..)
- In fact, NIST is more a list of things you must have policies about rather than a specific statement of required policies (eg, you must have a documented policy governing frequency of password changes, minimum password length, etc)
- NIST is actually a framework which allows you to tell your story using common language that is familiar to auditors
- Overall NIST process is quite logical and sensible



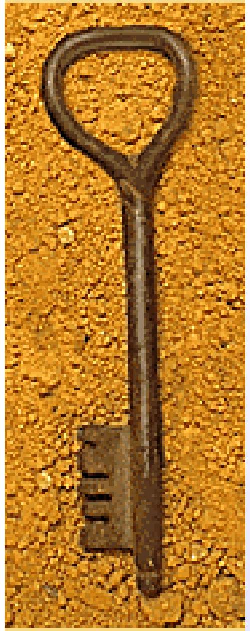
But does this have anything to do with OSG?

- OSG is not a “DOE lab”, so perhaps standards do not apply
- But OSG is certainly a virtual lab, and will be examined and perhaps even audited using same criteria
- And all labs that have resources used by OSG must live by NIST, so perhaps OSG should provide NIST framework examples for use in documenting grid computing security in a variety of locations!



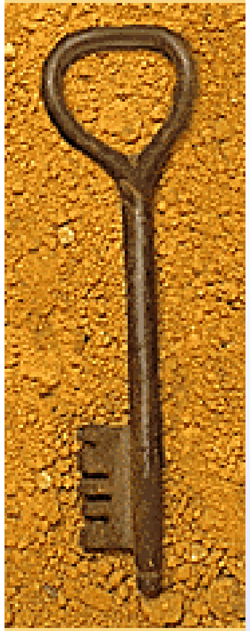
Two Types of Security Plans

- Core OSG: assets under complete control of OSG (eg, middleware software cache). OSG is responsible for security of these systems
- Facilities, VOs and software providers that are "part" of OSG. OSG can create examples and templates of security plans that can be incorporated into site and VO plans. Sites and VOs are responsible for security of these systems.
- For now concentrate on first type (core OSG)



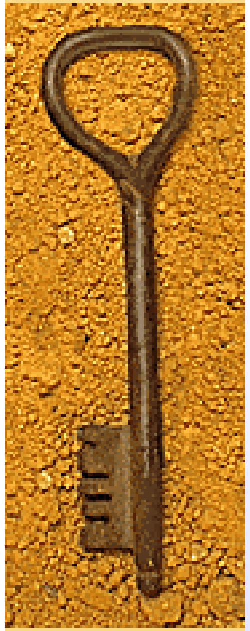
Details of the NIST Process

- **Each system needs:**
  - ❖Functional description
  - ❖Hardware and software description (especially description of boundaries)
  - ❖System Sensitivity Categorization (low/moderate/high sensitivity)
  - ❖Risk assessment
  - ❖Security plan (showing controls to mitigate the greater impact or likelihood risks)
  - ❖Contingency plan
  - ❖Security control testing and evaluation
- **Process for certification and accreditation**



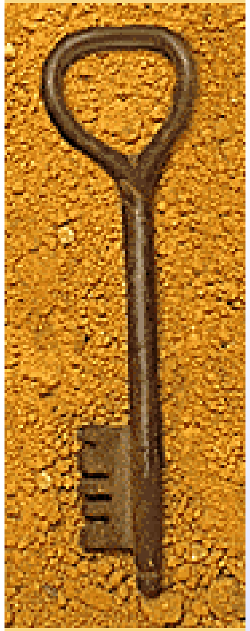
Sensitivity Categorization

- **Must evaluate the sensitivity of the information system and the information contained therein on the basis of:**
  - Confidentiality: A loss of *confidentiality* is the unauthorized disclosure of information.
  - Integrity: A loss of *integrity* is the unauthorized modification or destruction of information.
  - Availability: A loss of *availability* is the disruption of access to or use of information or an information system.
- **Low/moderate/high categorization**
  - The *potential impact* is **LOW** if: The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. [For us, loss us beamtime or downtime of a major server for up to a week]
  - Moderate: The *potential impact* is **MODERATE** if: The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
  - High: The *potential impact* is **HIGH** if: The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.



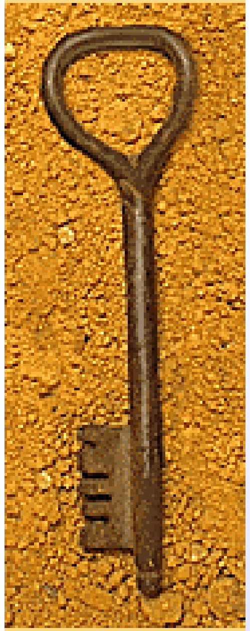
Mandated controls

- Based on the data sensitivity categorization, NIST has a long list of “required” security controls that an auditor will look for; low sensitivity controls are fewer in number and easier to satisfy



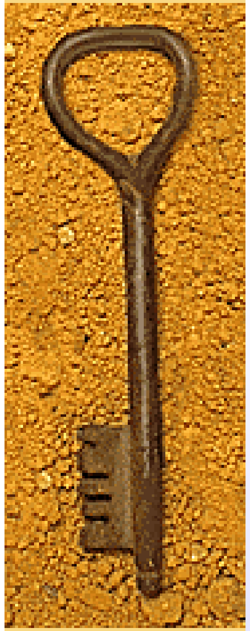
Why start with Risk Assessment?

- Looking at what can go wrong and potential impact allows rational choice about what to protect and what resources to commit to protective measures
- A formal process to ensure that all possible risks are considered and categorized
- First step towards security plan (security controls that mitigate identified risks) and contingency plans (procedures for dealing with residual unmitigated risks)



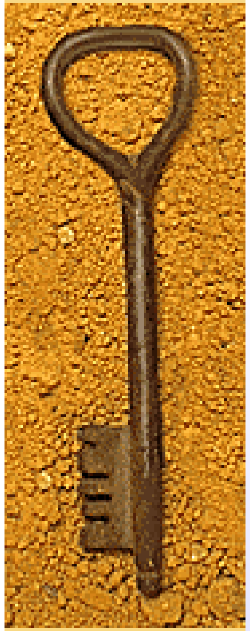
What is a risk assessment

- In general terms, a risk assessment is a statement of what could go wrong, countermeasures to prevent some of these things from happening, and statement that you will live with the risk of the rest (residual risks)
- Threat: who is knocking on the door
- Vulnerability: improperly secured door; you cannot have a risk without both a threat and a vulnerability
- Likelihood: probability of occurrence
- Impact: what is the damage if the risk occurs
- Security controls: mitigations against risks



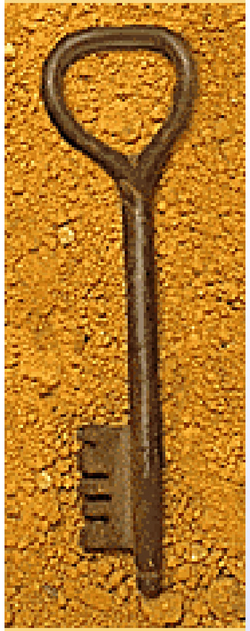
Example: locking the barn door

- **Threats**
  - Horse thieves
  - Squatters and trespassers
  - Vandals
  - Smokers
  - Natural and environmental threats (flood, earthquake, etc)
- **Vulnerabilities**
  - Broken locks; users forgetting to lock doors
  - Open windows
  - Broken walls



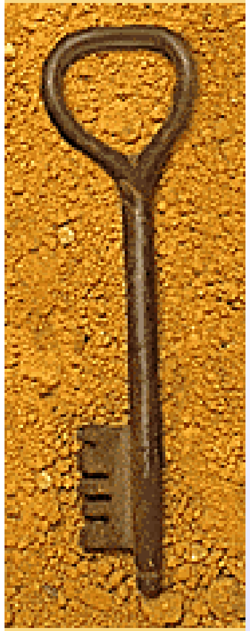
Threats

- **Trespassers**
  - those who walk in and use our resources, generally non malicious: worms, bots, squatters
- **Vandals**
  - web page defacers, data destroyers, destructive viruses, those who smear reputation
- **Thieves**
  - Those who steal substantial use of computing resources
  - Financial gain (much phishing and spamming)
  - Identity theft
- **Malware Authors**
  - Those who write malicious code
- **Spies**
  - Agents of foreign powers or commercial entities who access non public sensitive information
  - Those with political/social agendas
- **Alarmists**
  - Those who waste our time with false alerts (crying wolf) or overzealous calls for data



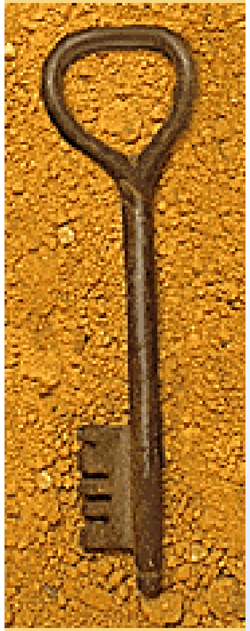
Vulnerablities

- **Remote access**
  - Scientific necessity of living on an open network means we are subject to remote denial of service attacks, remote scanning, potential resource use by unknown parties
- **Operating system vulnerabilities:**
  - bugs in an operating system can allow unauthorized remote users to access a system or local users to elevate their privileges, until patched
- **Application vulnerabilities**
  - Bugs in applications can allow unauthorized actions
  - Many applications are “delivered” with significant security holes until properly configured
- **Improper user actions**
  - Many ways for users to inadvertently execute malicious code (email, web browsing, ..)
  - Privileged users can improperly configure a desktop system
- **Physical access**
  - Unauthorized physical access to unprotected machines can allow malicious use



Methodology for identifying important risks

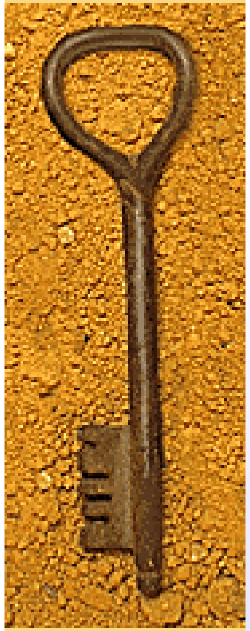
- Likelihood/impact table: each risk is ranked low/medium/high in both likelihood and potential impact if unmitigated; then important risks are those that are >low in both
- Bulleted list of those risks considered to be more than minimal (=low) in likelihood and/or impact
- At Fermilab, low is defined as minimal impact to program; medium is limited but non minimal impact



Risks of above minimal concern (impact or rate):

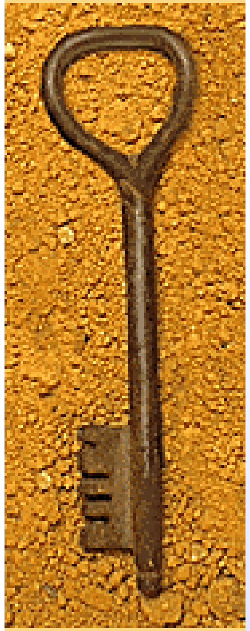
- Disruption or data corruption by disgruntled employee (human threat 1, vulnerability all)
- Automatically spread worms and viruses (human threat 2, vulnerabilities e, f, g, h, i)
- Script kiddies (semi skilled adolescent hackers) (human threat 3, vulnerability a-i)
- Exploit of OS and application holes (human threat 5 and 10, vulnerabilities e, g)
- Web page defacement (human threat 4, vulnerabilites e, g, i)
- Skilled hackers (human threat 5, vulnerability all)
- Unauthorized resource use (human threat 10, vulnerability all)
- Phishing for financial gain (human threat 9, vulnerability i)
- Inappropriate security alerts (human threat 6, vulnerability all)
- International intrusions (human threat 7 and 8, vulnerability all)

- Each of these risks must be mitigated by one or more security controls



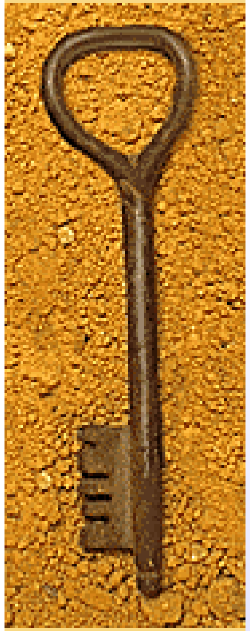
Residual risks

- **Residual risks are divided into categories based on expected frequency of occurrence after full implementation of all security controls. We consider an occurrence rate to be:**
  - low if it is expected to happen <10 times per year,
  - very low if it is expected to happen less than once/year
  - extremely low if it is expected to happen less than once every five years.
- **With these definitions, our residual risks are:**
  - Low rate of occurrence of unauthorized access to desktop machines due to late delivery or application of patches and/or poor user behavior
  - Low rate of unauthorized access to lab desktop machines due to improper or careless actions by remote users with lab computing accounts
  - Low rate of virus/worm infection due to late virus signatures and poor user behavior
  - Very low rate of unauthorized access through physical access
  - Extremely low rate of damage due to disgruntled insider with specialized knowledge
  - Extremely low rate of loss of important data
  - Extremely low rate of penetration of servers and central systems due to totally unexpected occurrences



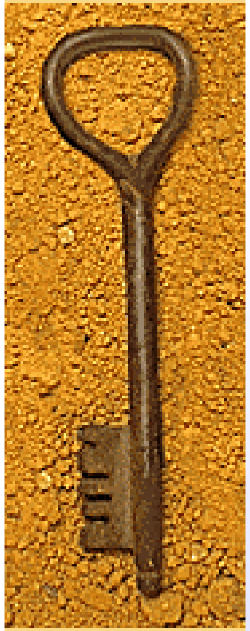
Security Plan

- Fully describe each control mentioned in your risk assessment
- Organize controls into management (policies), operational (things people do) and technical (things machines do) controls, and relate them to NIST control families
- Show how each control will be assessed (Interview, Examination, Test)



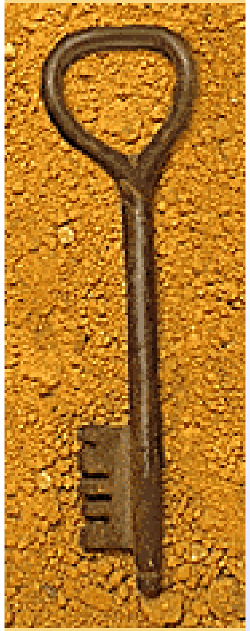
NIST Security Control families

- **Management**
  - Management Risk Assessment RA
  - Management Planning PL
  - Management System and Services Acquisition SA
  - Management Certification, Accreditation, and Security Assessments CA
- **Operational**
  - Operational Personnel Security PS
  - Operational Physical and Environmental Protection PE
  - Operational Contingency Planning CP
  - Operational Configuration Management CM
  - Operational Maintenance MA
  - Operational System and Information Integrity SI
  - Operational Media Protection MP
  - Operational Incident Response IR
  - Operational Awareness and Training AT
- **Technical**
  - Technical Identification and Authentication IA
  - Technical Access Control AC
  - Technical Audit and Accountability AU
  - Technical System and Communications Protection SC



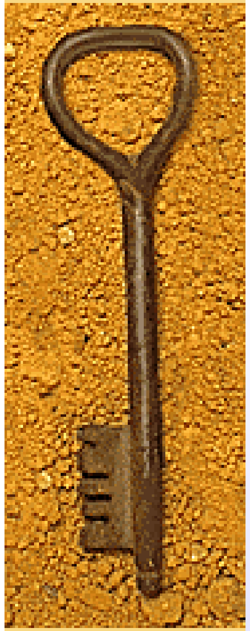
Example: Security Controls in FNAL General Computing Enclave

- Integrated Computer Security Management (M)
- Static Perimeter Protection (T)
- Dynamic perimeter Protection (T)
- Host based protection (T)
- Application specific protections (T)
- Data integrity protection (O)
- Strong authentication (T)
- Standard configurations baselines (O)
- Critical vulnerability (O)
- Vulnerability scanning (T)
- Physical access control and site management (O)
- Enclaves with above baseline protections (O)
- Security Incident response (O)
- Intelligent and informed user community (training) (O)



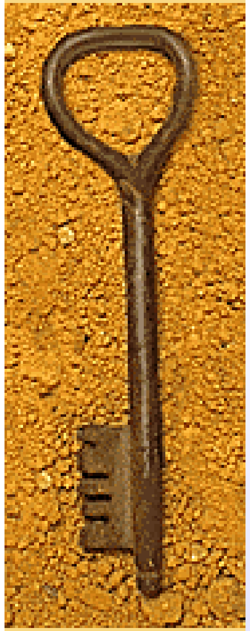
Security Control Details

- **Integrated Computer Security Management**
  - Part of line management
  - General computer security coordinators (GCSCs) and major application security coordinators (MASCs)
  - Terminating Employee Potential Computer Security Risk procedure (TEPCSR)
- **Static Perimeter Protection**
  - Scientific computing behind default allow firewall
  - Most administrative/business computing behind default deny firewall
  - Selected permanent block of ports/protocols
- **Dynamic Perimeter Protection**
  - Workgroup networks can be isolated
  - Realtime traffic flow selects ports/IP addresses to block
  - Blocking dangerous traffic during incidents
- **Host based protection**
  - Personal firewalls
  - Virus protection
  - Removal of unnecessary services
- **application specific protections**
  - Virus scanning
  - Restricted SMTP
  - Restricted HTTP



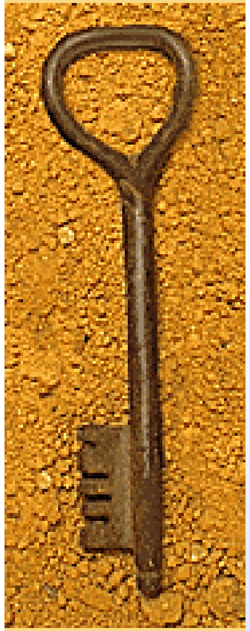
Security Control Details - 2

- **Data integrity protection**
  - ❖ Backups
  - ❖ Multiple copies of data
- **Strong authentication**
  - ❖ Internet visible network services require Kerberos authentication
  - ❖ No passwords on the network
  - ❖ Scan for unauthenticated service offerings
  - ❖ Scan for exposure of Kerberos passwords
- **Standard configuration baselines**
  - ❖ Standard configurations for Windows and Linux desktops and servers
  - ❖ Tools to monitor deviations from baseline
- **Critical vulnerability**
  - ❖ Identification of urgent threats
  - ❖ Scanning for vulnerability
  - ❖ Denial of network access if not patched



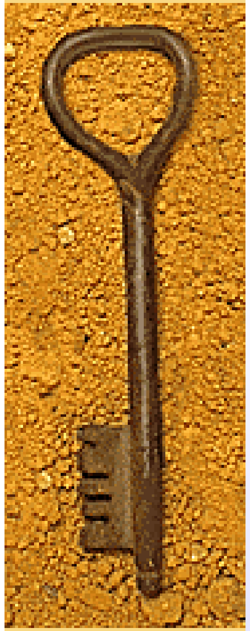
Security Control Details - 3

- **Vulnerability scanning**
  - ❖ Inventory scanning
  - ❖ Vulnerability scanning
  - ❖ Scanning when attaching to network
- **Physical access control and site management**
  - ❖ Property protection areas
  - ❖ UPS, fire and environment protection
- **Enclaves with above baseline protections**
  - ❖ Special security controls for major applications with above average security requirements
- **Security Incident response**
  - ❖ Mandatory incident reporting
  - ❖ FCIRT team assembled from throughout lab
  - ❖ FCIRT "owns" machines during an incident
  - ❖ Lessons learned from incidents feeds back to security policies
- **Intelligent and informed user community (training)**
  - ❖ Required training at different levels for different roles



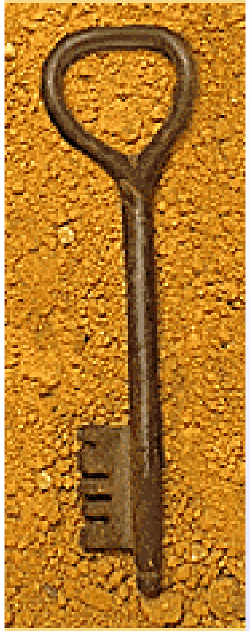
Contingency Plan

- Discuss how contingencies are recognized and declared and how notification is done
- Show roles and responsibilities (who declares contingency, who is in charge during, who says it is over)
- Discuss how services will be provided or done without for the duration of the emergency
- Discuss how contingency is declared over
- Discuss testing of contingency plan (table top exercise or actual fire drill)



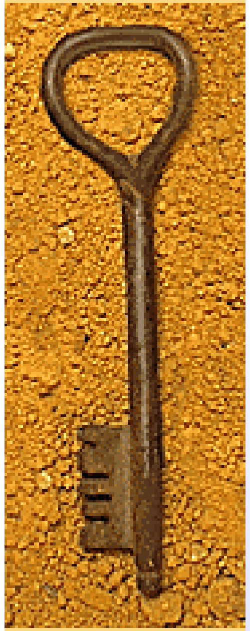
What are contingencies

- You have described what can go wrong (risk assessment)
- You have protected against the most likely and most damaging of these (security plan)
- Contingencies are the things that still could go wrong (with lesser probability) that you choose not to protect against
- Still need some planning on how to deal with these unlikely occurrences
- Note: not the same as a business recovery plan or continuity of operations (COOP) plan



Contingency vs normal operation

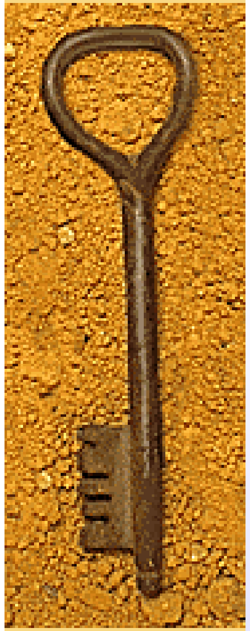
- **Is some particular plan or procedure part of normal operating practices or is it contingency planning?**
  - In most cases it is both (eg redundant network paths), but go ahead and briefly describe it anyway
  - When it is only used in unusual circumstances (hot spare system only used in emergencies) it is purely contingency planning



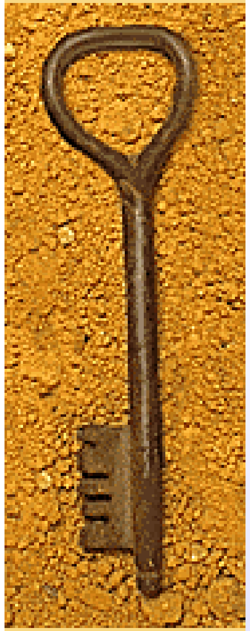
Methods of dealing with contingencies

- Redundancy (even if also used in ordinary operation)
- Spare systems that can be turned on or transferred from other applications
- Plans for operation at reduced capacity or capability
- Plans for temporarily doing without the affected service (service not needed in large emergency, delaying certain operations, …)
- Plans for alternate ways of providing the affected service (outsourcing, …)

NIST Guidelines (800-34)

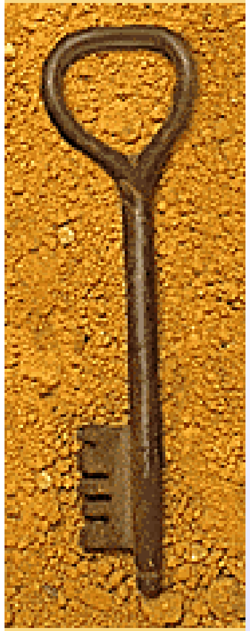


- The document also defines the following seven-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for their IT systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.
- 1. **Develop the contingency planning policy statement.** A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
- 2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical IT systems and components. A template for developing the BIA is also provided to assist the user.
- 3. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
- 4. **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- 5. **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
- 6. **Plan testing, training, and exercises.** Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
- 7. **Plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements.
- The document presents a sample format for developing an IT contingency plan. The format defines three phases that govern the actions to be taken following a system disruption. The **Notification/Activation** Phase describes the process of notifying recovery personnel and performing a damage assessment. The **Recovery** Phase discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions that can be taken to return the system to normal operating



ST&E Plans (assessment of your security controls)

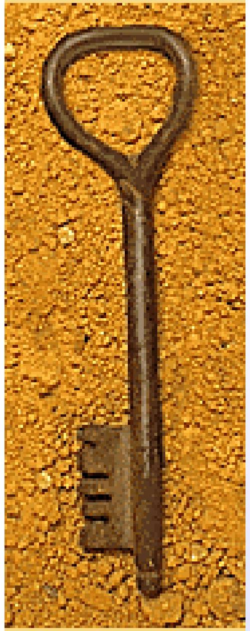
- **All controls must have procedures for testing and evaluation (it is not enough merely to be secure, you must be able to prove that you are secure)**
  - Can be an ongoing process (eg, we continually monitor the logs of all user access to our system)
  - Can be an annual (at a minimum) special test (eg, once per year we attempt to penetrate our firewall from the outside)
  - Can be statistical sampling (interviewing or examining some randomly chosen subset of managers or systems)
  - In either case must provide documentation that the test were performed and their result
  - We will provide some central location for these test results



Three types of assessments

- **The three types of assessment mechanisms used for security controls are Interview (I), Examine (E), and Test (T). As explained in NIST publication 800-53A "Guide for Assessing the Security Controls in Federal Information Systems", these three types of assessment mechanisms can be described as follows:**
  - **Interview**: this involves asking a selected set of individuals, based on their roles, specific questions about configurations, their actions, etc. For Interview assessments, we indicate who will be interviewed (not a full list of names, but the roles involved, and whether it is all of those individuals or some statistical sample), what questions you will ask them, and where the results are recorded.
  - **Examine**: this involves doing an analysis of some existing data sample and recording the results of the analysis. For Examine assessments, we give a pointer to the data set being analyzed, a description of what analysis is done, and the locations of the results of the analysis.
  - **Test**: this involves performing some specific test (or fire drill) of the security control to verify that it is performing as expected. For Test assessments we describe the test, the test frequency, and the location where the test results are recorded.

Current OSG Work



- **Weekly phone conferences to proceed with inventory of core OSG and risk assessments and security plans for these resources**
  - Start with overall OSG (common baseline for subsidiary assessments)
  - Proceed per OSG core asset inventory
- **OSG should determine relationship between its core resources and those of its host labs and VOs**
- **Establish basis for trust relationships among OSG, sites and VOs (plans and agreements)**
- **Collaborate with sites and VOs on preparation of their plans**