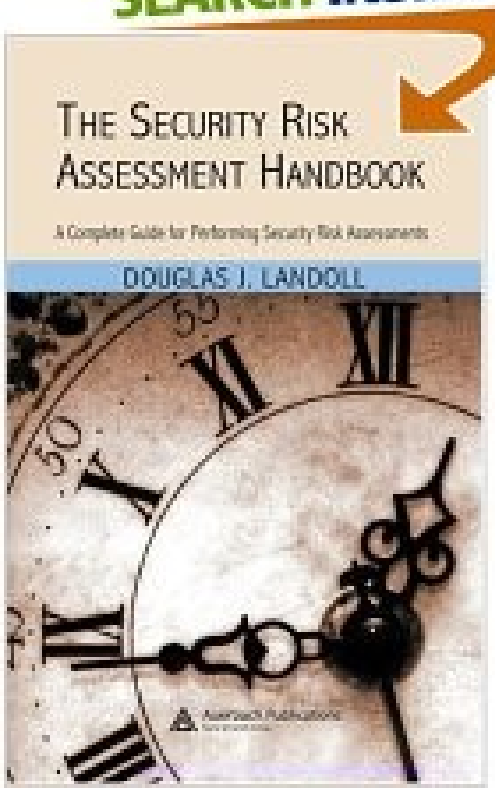
From the Lab to the Boardroom:

How to perform a Security Risk Assessment Like a Professional



Doug Landoll, CISSP, CISA
General Manager, Security Services
En Pointe Technologies
dlandoll@enpointe.com
(512) 310-2228
(877) 321-RISK

NEbraska CERT Conference 2006
Computer Security and Information Assurance

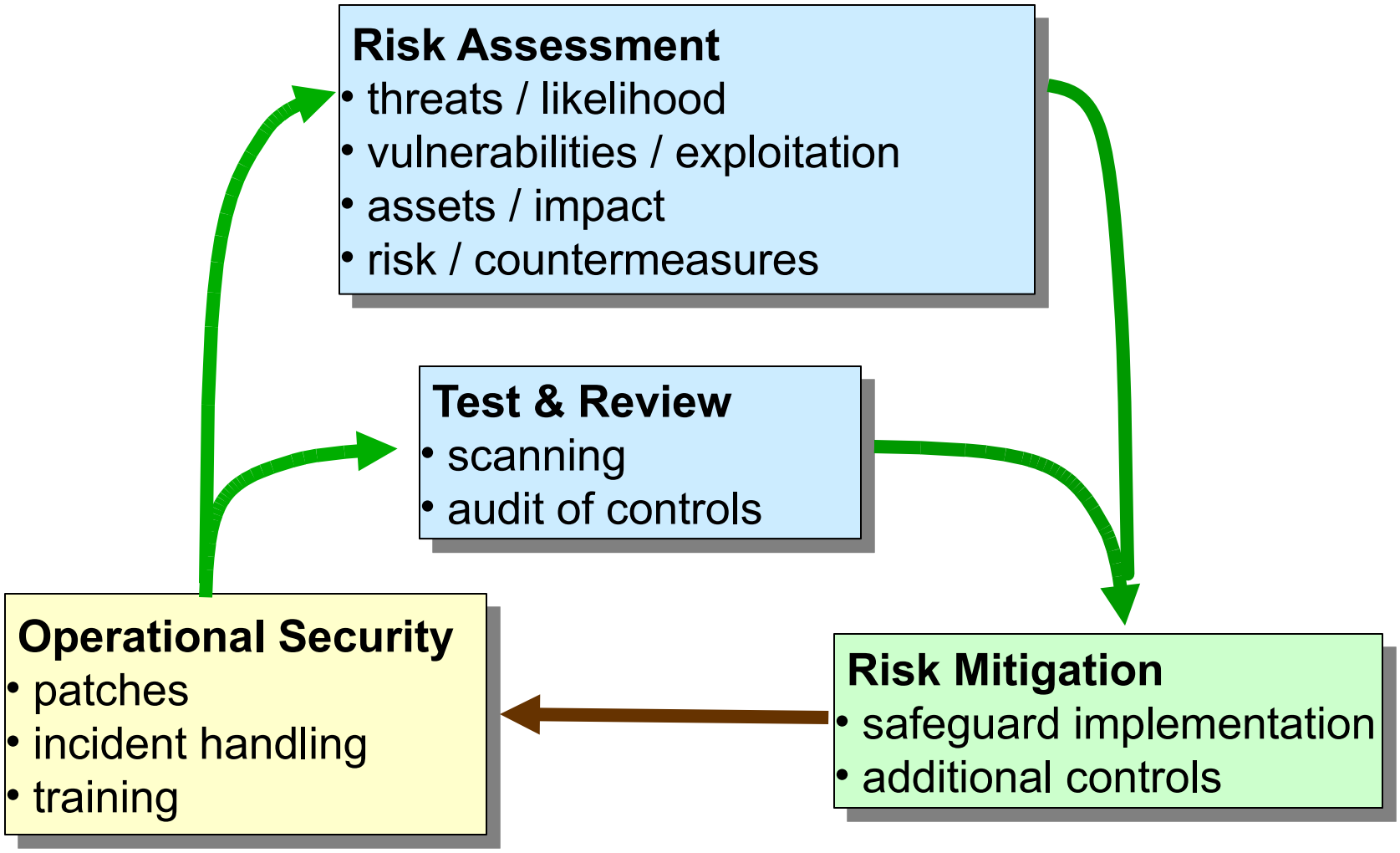
Agenda

- SRA Introduction
- Security Risk Assessment Project
  - Phase 1: Project Definition
  - Phase 2: Project Preparation
  - Phase 3: Data Gathering
  - Phase 4: Risk Analysis
  - Phase 5: Risk Mitigation
  - Phase 6: Recommendations
- SRA Project Management

Security Risk Assessment Introduction

- SRA Role
- SRA Definition
- SRA Need
- What SRA is NOT

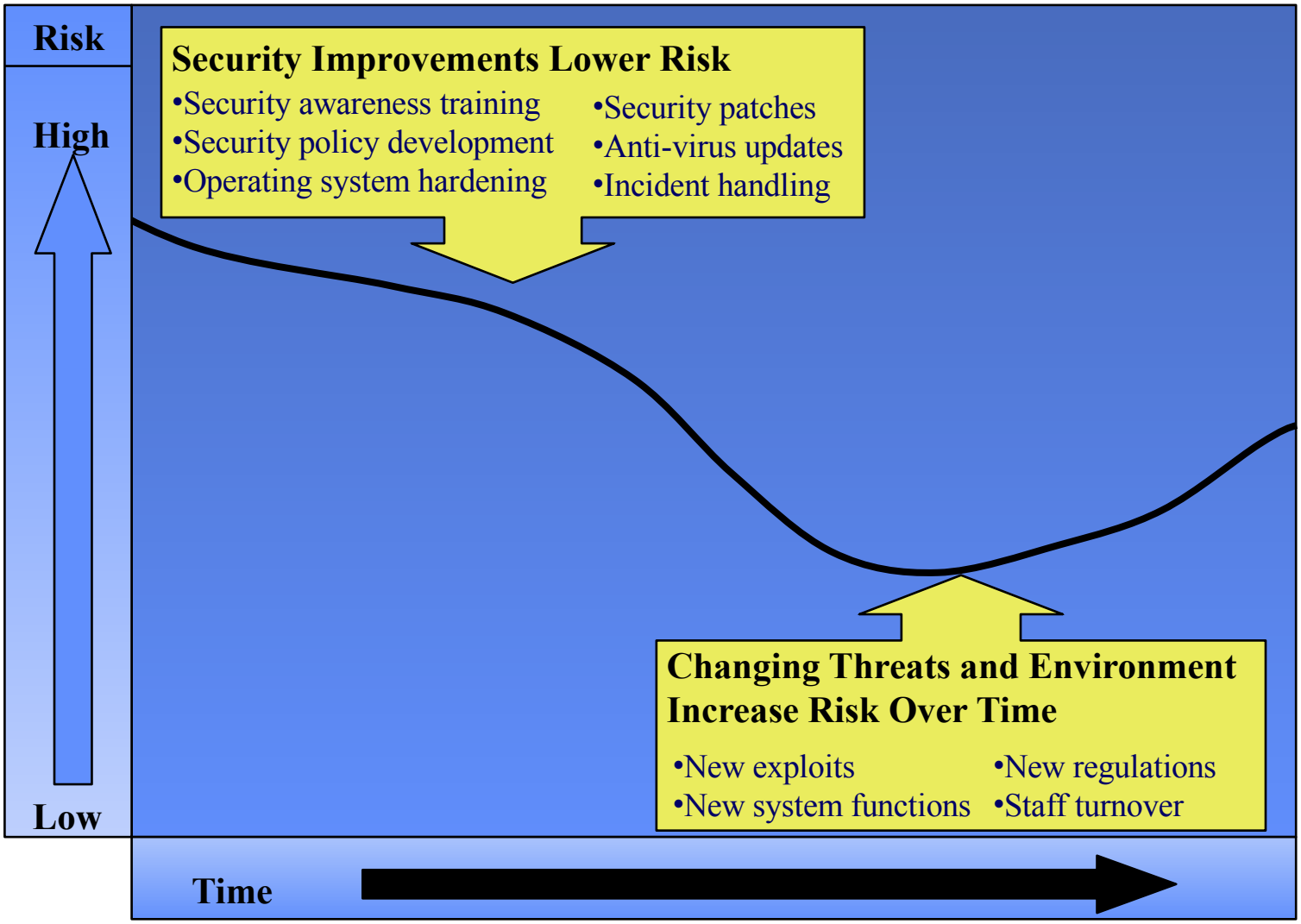
Security Risk Assessment Role



Security Risk Assessment Definition

An objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets.

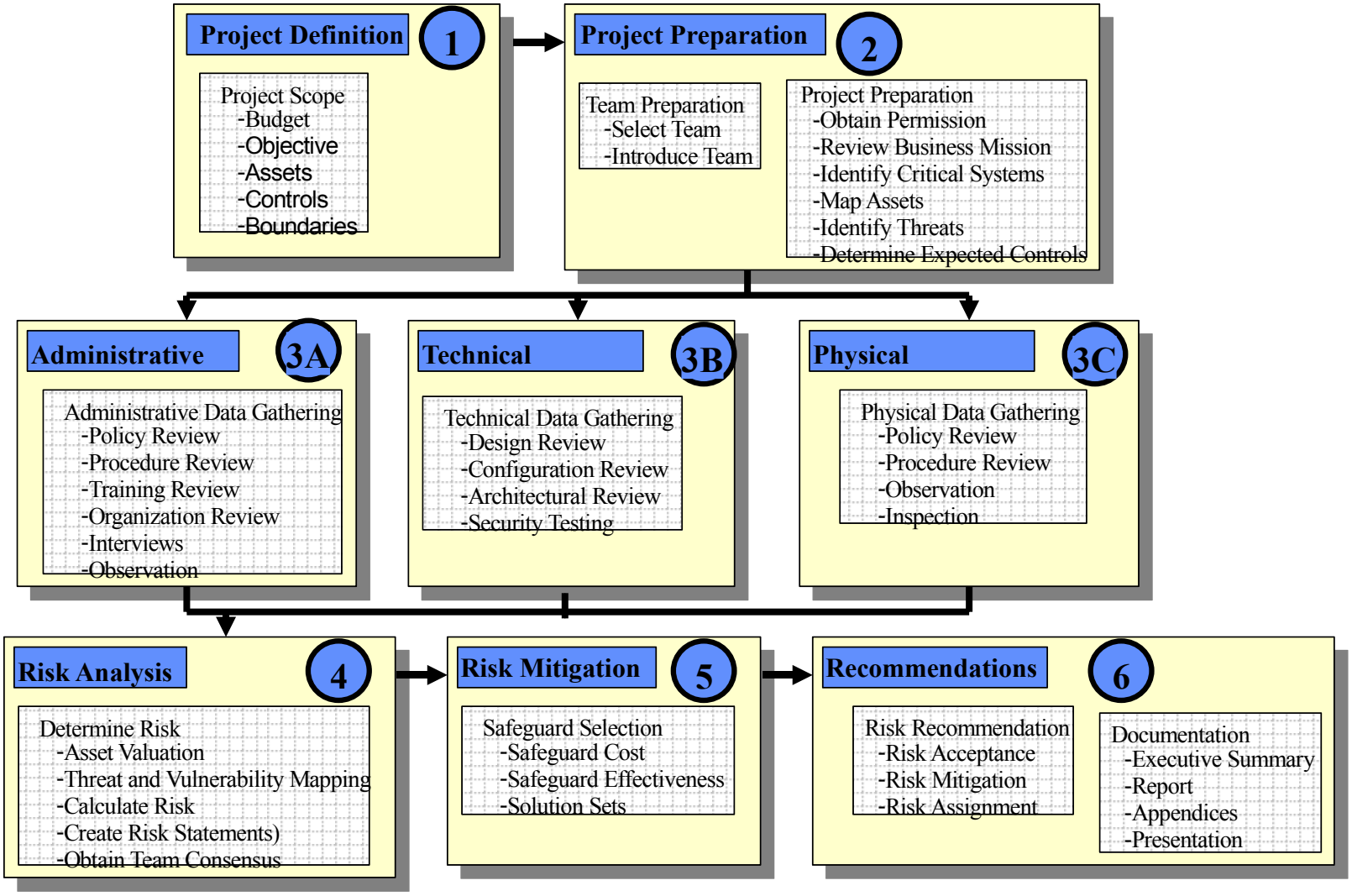
Security Risk Assessment Need



What SRA is NOT

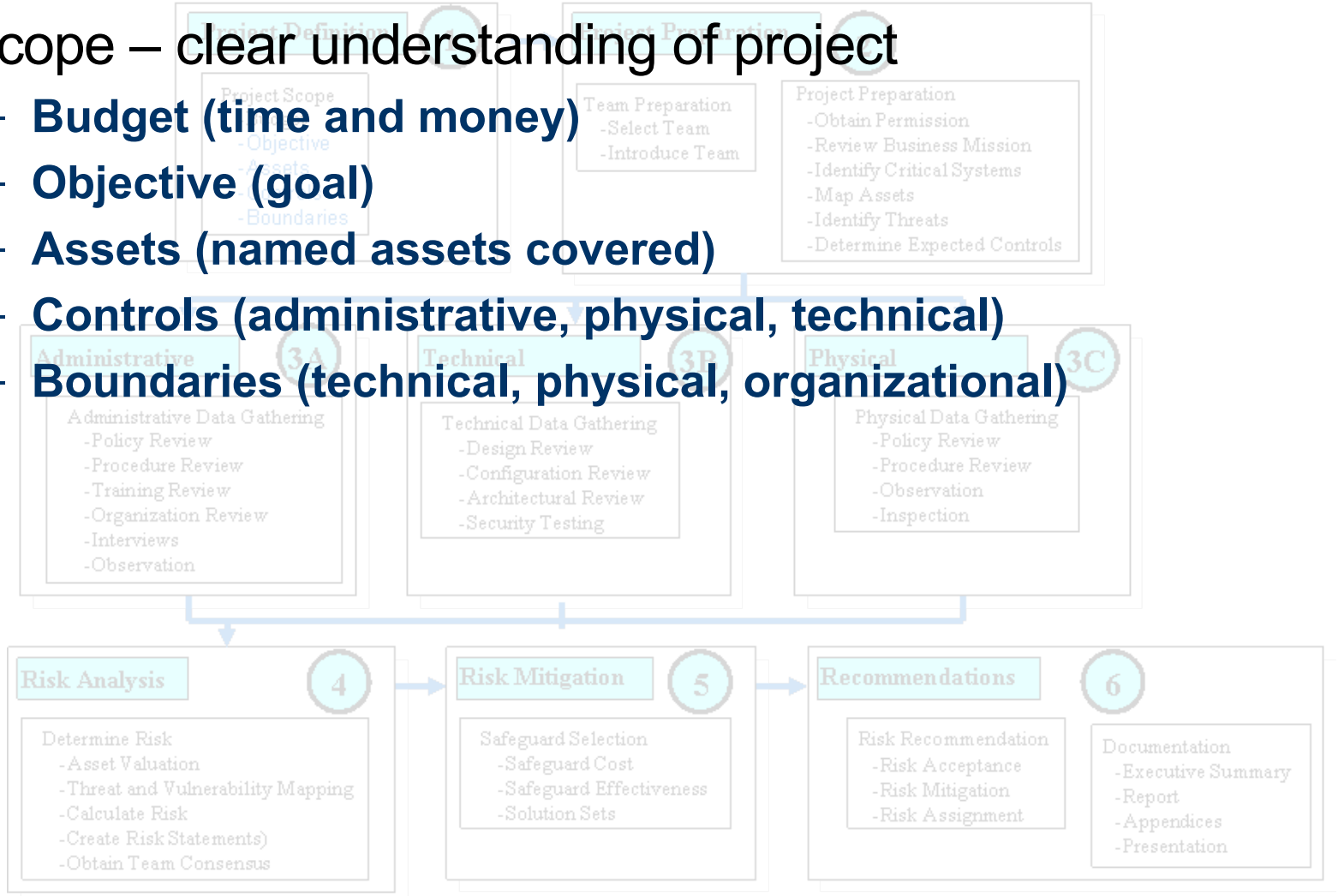
Term	*Definition*	*Purpose*
Gap Assessment	A review of security controls against a standard.	To provide a list of controls required to become compliant.
Compliance Audit	Verification that all required security controls are in place.	To attest to an organization's compliance with a standard.
Security Audit	A verification that specified security controls are in place.	To attest to an organization's adherence to industry standards.
Penetration Testing	A methodical and planned attack on a system's security controls.	To test the adequacy of security controls in place.
Vulnerability Scanning	An element of penetration testing that searches for obvious vulnerabilities.	To test for the existence of obvious vulnerabilities in the system's security controls.

Security Risk Assessment Phases



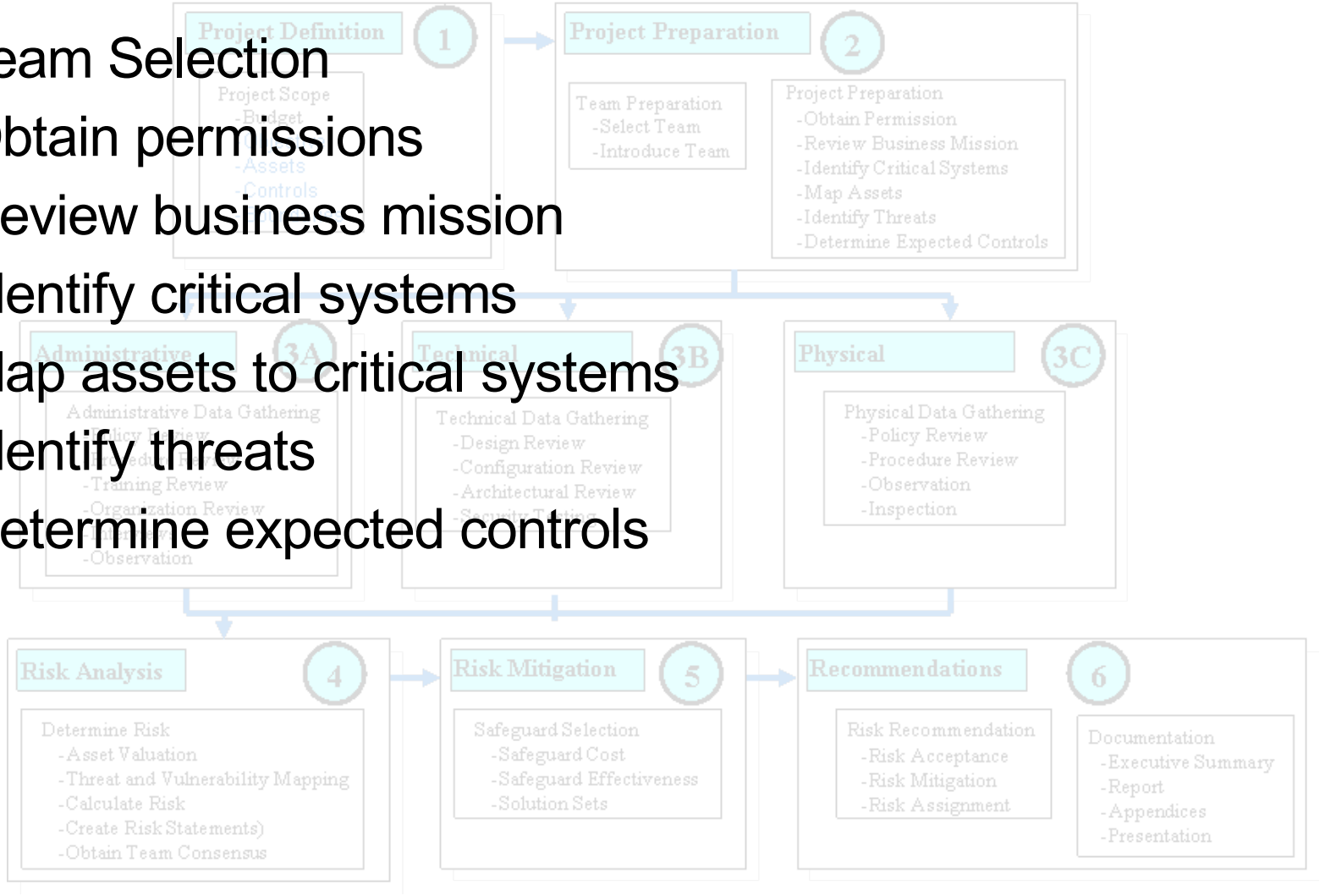
1: Project Definition

- Scope – clear understanding of project
  - **Budget (time and money)**
  - **Objective (goal)**
  - **Assets (named assets covered)**
  - **Controls (administrative, physical, technical)**
  - **Boundaries (technical, physical, organizational)**



2. Project Preparation

- Team Selection
- Obtain permissions
- Review business mission
- Identify critical systems
- Map assets to critical systems
- Identify threats
- Determine expected controls



3. Data Gathering

- Administrative
  - **Policies, procedures, training, organizational structure, behaviors, personnel**
- Physical
  - **Facility design, environmental controls, barriers, alarms, behaviors, response, documentation**
- Technical
  - **Security architecture, device configuration, security testing**

Current SRA Data Gathering Guidance

How exactly do we assess mechanisms?

- *"[Ensure that] the organization's hiring and termination practices for staff take information security issues into account."*
- *"[Assess whether] the organization uniformly enforces its security policies."*
- *"Run Vulnerability Evaluation Tools on Selected Infrastructure Components"*
  - *"[ensure you have the] correct tool...[and the] latest version..."*

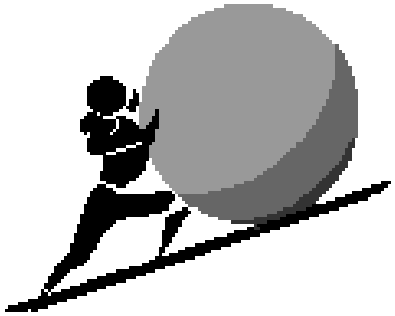
SRA Data Gathering Performance

SRA Execution

- "hero" lead more than process lead (and not enough heroes)
- Checklist-based (misapplied and misinterpreted)

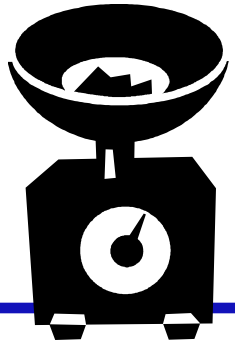
SRA Scope and Rigor

- Unclear scope of assessment (boundaries, techniques, mechanisms)
- Unclear rigor of assessment (skills, time expended, analysis)



SRA Results

- Not standardized
- Not comparable
- Not repeatable



Data Gathering Performance

Labor intensive

- Lots of data, activities, hours

- Project Control Issues
  - Organizing and presenting data
  - Tracking progress
  - Ensuring appropriate coverage

- Little structure or guidance

A structured approach to data gathering

What's Needed

- **General approach to improve current data gathering**
  - Less reliance on heros
  - More repeatable and comparable results
  - Standardized approach
  - Clear rigor and coverage

The RIIOT Approach

- **The RIIOT Approach**
  - Provides a general approach to improve SRA data gathering
  - Works with current commercial or proprietary approaches
  - Supplements current SRA approaches, commercial or proprietary

The RIIOT Approach to Data Gathering

- Organizes the task of gathering volumes of data on a wide variety of controls.
- Identifies the 5 methods to data gathering
- Maps appropriate method for each security mechanism
- Lists data gathering techniques for each method/mechanism pair
- Introduced in “Security Risk Assessment Handbook”

Detail Solution

- There are 5 Methods of Gathering Data

R Review documentation

I Interview Key Personnel

I Inspect Controls

O Observe Behaviour

T Test Controls

RIIOT: Review Documentation

R

- **Key Mechanisms (Controls)**
  - Rules, configurations, networks, architectures, physical layouts, and other mechanisms.

- **Important Elements**:
  - Review for:
    - Clarity
    - Content,
      - Correctness, Completeness, Consistency
  - Expected Elements Review

Example Review Procedures

Objective	*Sub-topic*	*Review Tips*
Gather information from past security review efforts to improve data gathering in the current security risk assessment	Mission Statement	Check mission statements recorded in other reports against the ones provided to you. If they are different ask key personnel why this has changed?
	System Components & Boundaries	Review named system components and indicated system boundaries and compare them to the current statement of work. If they are different ask key personnel for an explanation. Look for any components, subsystems, areas, or interfaces that have not been included in the last or present assessment. For example, some organizations never include physical security as a part of the assessment. Determine if the lack of review for organizational elements is a vulnerability.
	Roles & Responsibilities	Look for definitions of roles and responsibilities from previous reviews. Specifically, look for responsibilities such as running an internal vulnerability scan, account review, or other security activities.

RIIOT: Interview Key Personnel

- **Key Mechanisms** (Controls)
  - Duties and responsibilities
  - Process and procedure (practice and knowledge)
  - History of incidents

RIIOT: Interview Key Personnel

- **Important Elements**:
  - Determine Subjects, Interviewer
  - Review Relevant Document (Prepare)
  - Determine Objective for Interview
    - Confirmation of information
    - Measurement of security awareness
    - Identification of interviewee vulnerabilities
    - Determine ability to perform duties
  - Determine Type of Interview
    - guided, fixed response, conversational, open-ended
  - Prepare questions / questionnaire

Example Interview Procedure

Security Program Interview Questions		
Objective	**Sub-Topic**	**Question**
Determine existence and adequacy of security controls within information security program	Security Awareness	Do you have a list of all users who need training and have received it? Where are the records kept? Do these records include a signature of the student and the instructor?
	Policy Development	When were the policies last updated? How long did it take to get them approved? How were users informed of their change? New signatures?
	Risk Assessment	How often are risk assessments performed? By whom? What is their relationship to the organization or any of its security controls? Did they recommend products? Did you buy them?
	Security Review	Do you think other departments are following the policies you set for them (operations, monitoring, development)? Would it surprise you if I told you they were not? Do you have any annual or periodic report on the security posture of your organization?

RIIOT: Inspect Controls

- **Inspection**:
  - Assess security mechanisms
  - Performed where testing is infeasible, ill-advised or out of scope

- **Key Mechanisms (controls)**:
  - Fire suppression system
  - Glass break alarm

RIIOT: Inspect Controls

- **Important Elements**
  - List controls
    - Visitor control, configuration files, smoke detectors, incident response handling.
  - Verify information gathered
  - Determine vulnerabilities
    - Inspect against industry standards, checklists, common vulnerabilities, or against experience and judgement.
    - See example (next slide)
  - Document and review findings

Example Inspection Procedure

Security Lighting Inspection Checklist		
Objective	**Key Topics**	**Example Questions**
Determine existence and adequacy of security controls within lighting system	Sabotage	Tour areas critical to lighting systems to determine susceptibility to sabotage Switchyards Transformers Circuit breakers Power lines Engine generators UPSs
	Single Point of Failure	Inspect lighting system to determine if security lighting systems have any single points of failure Single lighting circuit Power supply on a single circuit breaker Single power grid
	Access Control	Inspect access controls on areas containing lighting system components.

RIIOT: Observe Behavior

O

- ***Observation***:
  - View organization response and behavior of various situations
- **Key Mechanisms**
  - Enforcement of policy (visitor control, media control, security awareness)
- **Techniques**
  - Observe key behaviors
  - Cause situations that enact policy
    - Example, put your visitor badge in your pocket

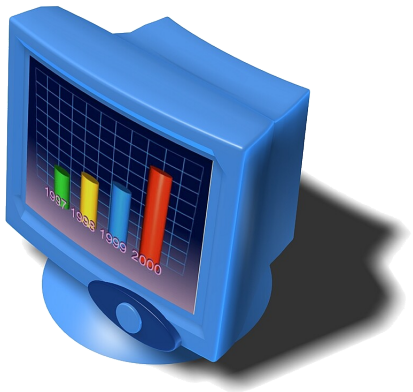
Example Observation Procedure

Technical Control	Claim	Observation Test or Procedure Check
Audit Logs	All security relevant events are audited and reviewed.	Review audit logs for security relevant events that transpired during the onsite. Wait a few days after an auditable event and check to see when the event was first reviewed.
Anti-Virus Systems	System prevents virus infection Updates are performed regularly Users cannot block scans or updates	Be aware of viruses that may be circulating during the time of the assessment. Determine from observation if the virus is having an effect on the information system. When given the chance to interview users or inspect a workstation, check to see if the latest updates have been applied. Also check to see if scans or updates can be blocked.
Screen Savers	All workstations have active screen savers with passwords	General observations of user behavior and workstations viewed while onsite.

RIIOT: Test Controls

- **Key Mechanisms**:
  - Firewalls, servers, open door alarms, motion sensors.

- **Important elements**
  - Documentation (repeatability, trouble shooting)
  - Coverage (sampling or complete)



RIIOT: Test Controls

T

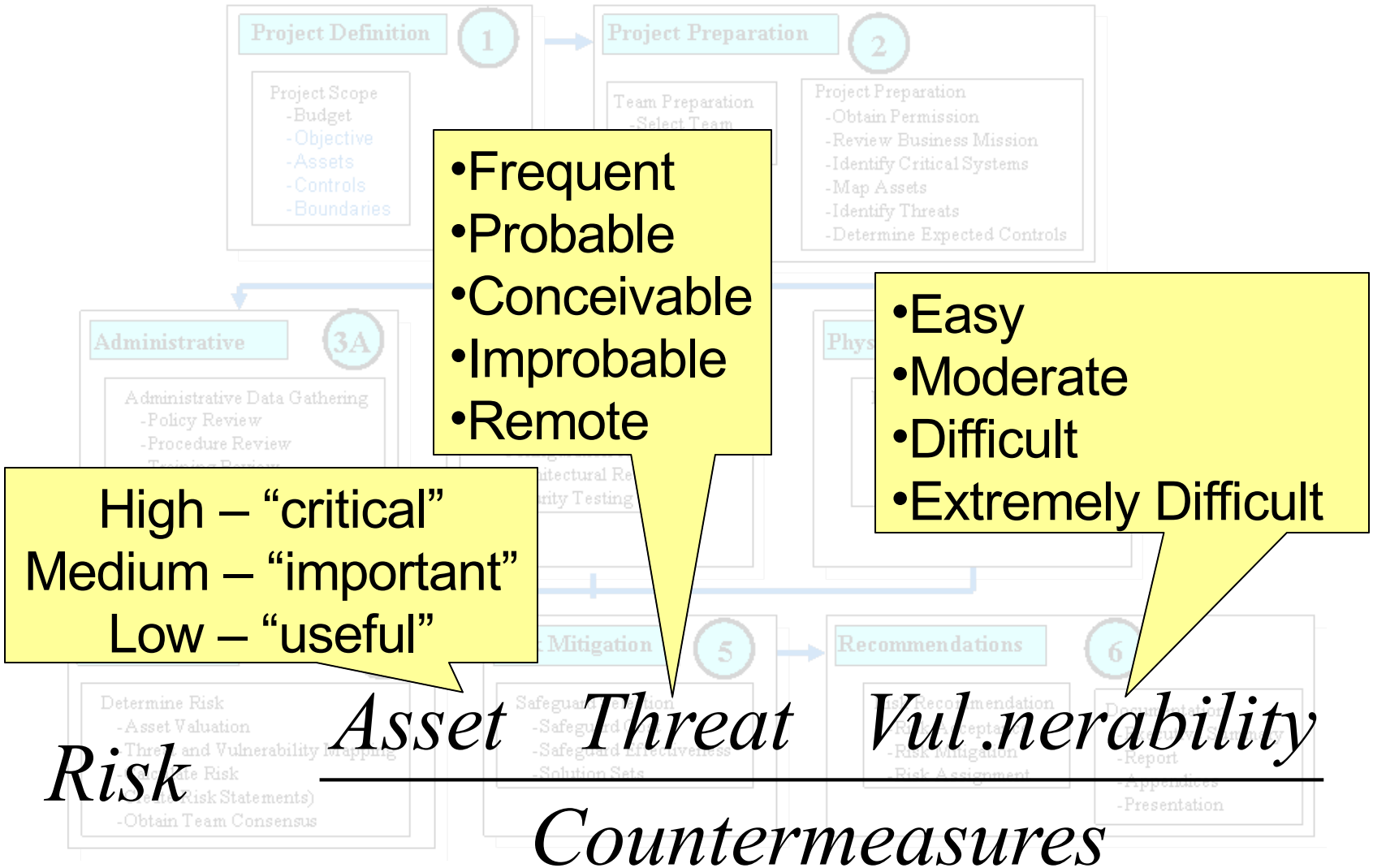
- **Types of testing**
  - Information accuracy
    - Verify information obtained through interviews and documents
  - Vulnerability testing
    - Test for the presence of known vulnerabilities
  - Penetration Testing
    - Exercise discovered vulnerabilities to demonstrate failure to enforce policy

- **Techniques**
  - Vulnerability scanners
  - Shuffle test

Example Test Procedure

Physical Control	Claim	Testing Procedure
Door and Locks	Doors and locks are in good working order. Doors and locks are adequately protected.	**Timed Closure Test:** Open the door to a 90 degree angle and time how long it takes to close. A rule of thumb is six (6) to eight (8) seconds is reasonable. Doors that close slower are susceptible to tailgating. **Closing Latch Test**: Open door just one inch. Let go and witness if the door closes shut or stays open due to the friction or pressure of the latch. **Protected Latch Test**. Inspect door to determine if the door latch is exposed to the outside. This basically means there is a lack of shielding between the door frame and the door near the door handle. If latch is exposed, attempt to defeat the mechanism through the use of a credit card, butter knife, or other tool. **Motion Sensor Activated Doors**. Attempt to circumvent door lock through unprotected gaps in the door. Methods include sliding a coat hanger with a piece of foil on the end through the door gap. The motion and heat of the foil could trip the motion sensor to open the door as is someone from the inside was approaching.

4. Risk Analysis

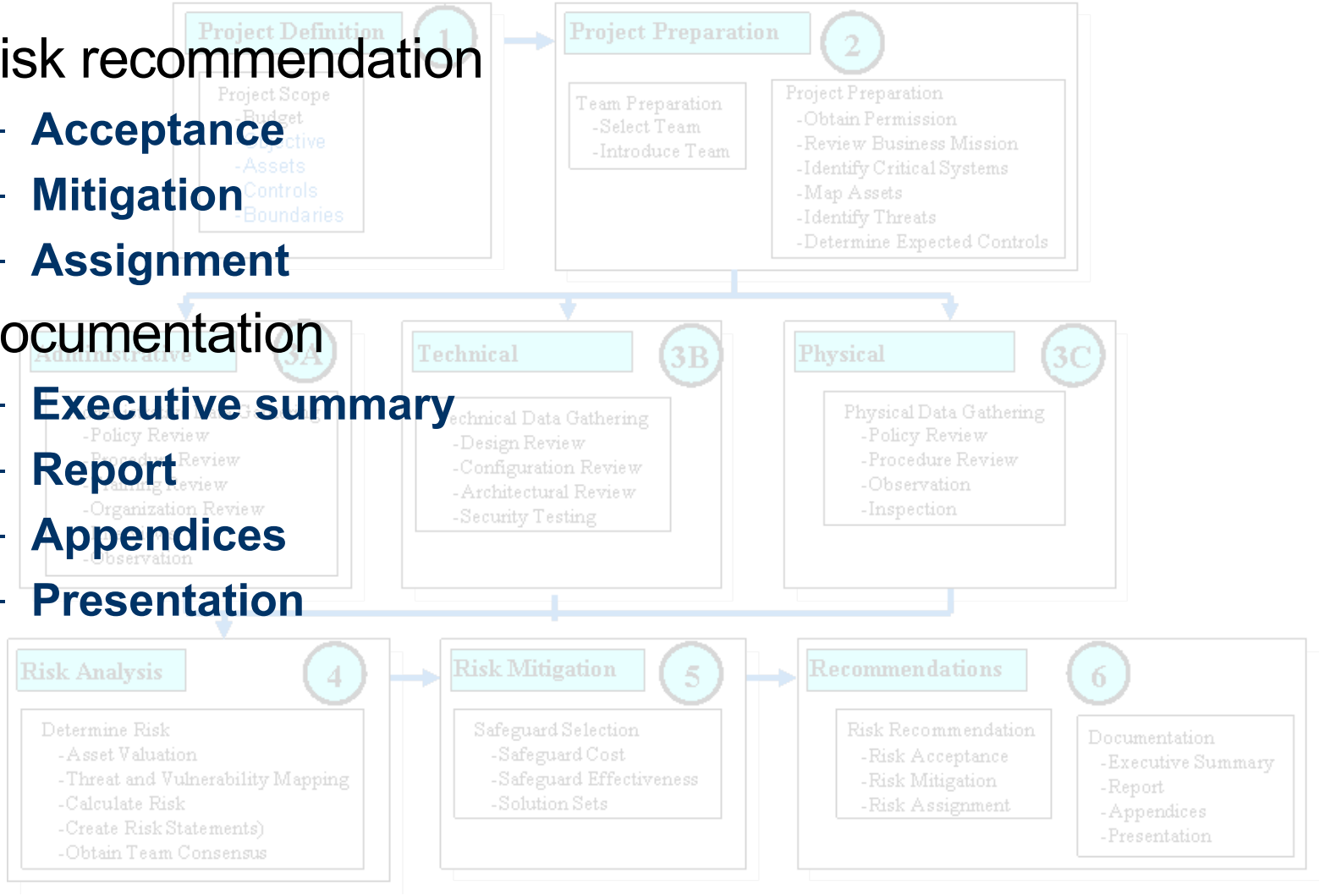


5. Risk Mitigation

- Safeguard selection
  - **Cost (time, money, training, integration)**
  - **Effectiveness**
  - **Solution sets**
    - **Policy, training, product, procedures, sanctions**

6. Recommendations

- Risk recommendation
  - **Acceptance**
  - **Mitigation**
  - **Assignment**
- Documentation
  - **Executive summary**
  - **Report**
  - **Appendices**
  - **Presentation**



Backup Slides

For use during Q&A (if needed)

Detail Solution

- There are 5 Methods of Gathering Data

R Review documentation

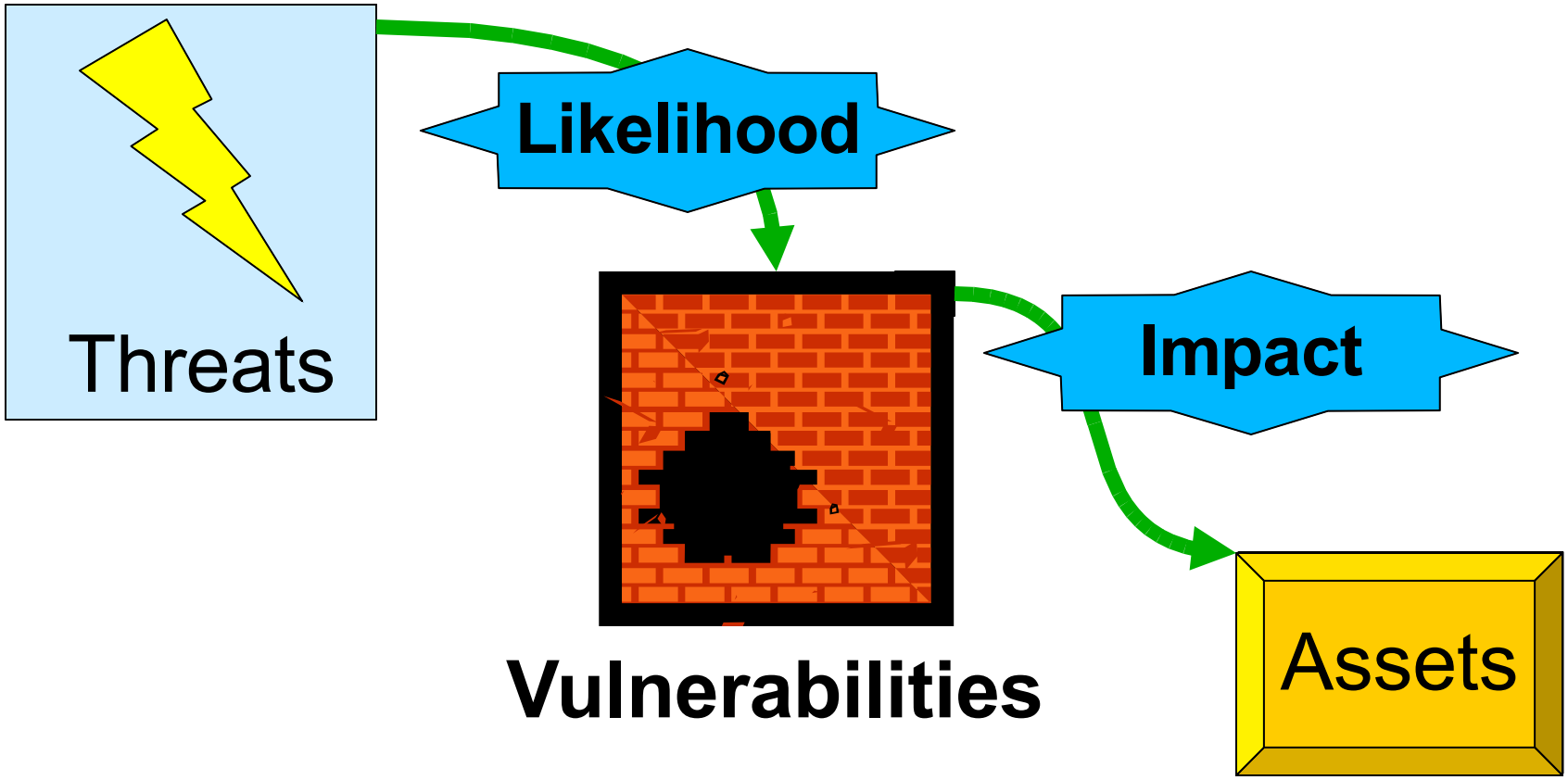
I Interview Key Personnel

I Inspect Controls

O Observe Behaviour

T Test Controls

SRA Basics



RIIOT Application

Controls	*Review Documents*	*Interview Key Personnel*	*Inspect Controls*	*Observe Behavior*	*Test Controls*
Monitoring Technology	X				X
Audit Logs	X	X		X	X
Logical Access Controls	X				X
Checksums	X				*
Encryption	X		X		*
Anti-virus System	X			X	X
Single Sign On Systems	X				*
Two-Factor Authentication	X				*
Identity Management Systems	X	X	X		
Automated Password Policies	X				X
Password Crackers	X				
Password Generators	X				
Data Backup Technologies	X	X			

Backup Slides

- Security Organization Maturity

Level 3: The Security Organization
C-level reporting
oversight, governance, operations
complete security focus

Level 2: The Security Team
security guy with a staff
assigned responsibility
IT focused only
no oversight

Level 1: The Security “Guy”
admin with security interest
default responsibility
activities include only those thing “interesting”

SRA Method Roundup

SRA Basis	"What"	unbiased	Repeatable	Expert	"How"
Facilitated			X		X
Process		X		X	X
Questionnaire		X		X	X
Tool		X		X	X
Interview		X	X	X	X