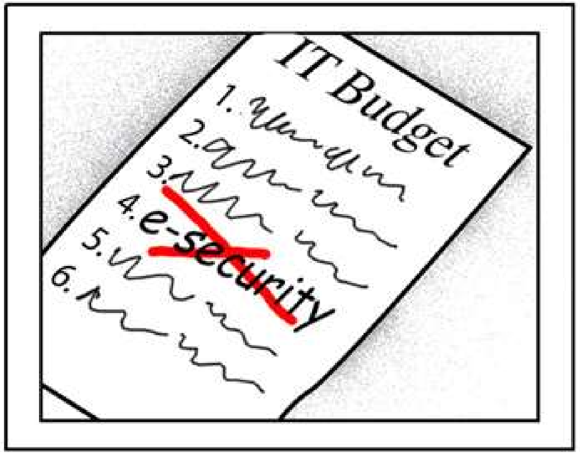
impruve
MANAGE RISK, MAXIMIZE REWARD

Impruve Security

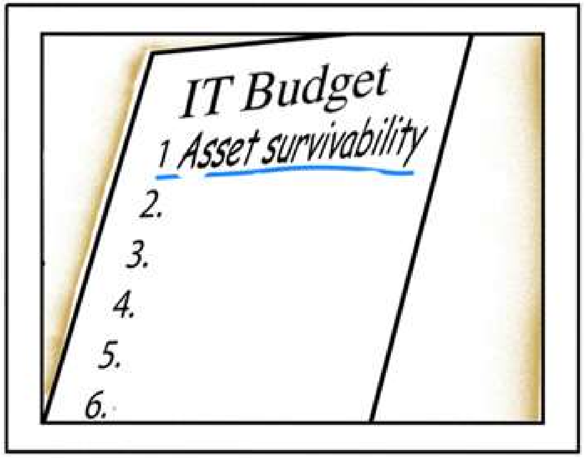
OCTAVE

Security Shifts in Thinking

- **It’s not just an Information Technology Problem**
  - Single point of known responsibility to correct failures to…
  - Shared, sometimes unknown, responsibility



- **You can’t live without it**
  - Security viewed as an overhead activity to…
  - Security viewed as essential part of business continuity



- **Think risk**
  - Security as a narrow technical specialty accessible only to experts; protection of specific components to …
  - Survivability as a risk management perspective requiring involvement of the

Risk Assessments

- *OCTAVE*
  - Operationally Critical Threat, Asset and Vulnerability Evaluation
  - Developed at the Software Engineering Institute (SEI) of Carnegie Mellon University
  - SEI also
    - Manages CERT
    - Studies network survivability

Survivability

- Enterprise-wide perspective to sustain the business in the face of ongoing attacks, failures, unexpected events, or accidents
- Providing business continuity (e.g., services, albeit degraded), in the presence of attacks, failures, events, or accidents
- Focusing the highest level of protection on critical assets
- Complementing the current risk management approaches that are part of the organization’s business practices

Why OCTAVE? -1

- Before OCTAVE, the SEI performed Information Security Evaluations (ISEs).
  - ISE is expert-led vulnerability evaluation consisting of
    - Interviews with information technology personnel and selected users
    - Review of selected components from computing infrastructure for technological weaknesses
    - Analysis of the information gathered by a team of experts

Why OCTAVE? -2

- Observations from the ISE deliveries
  - Organizations did not always take meaningful action after the evaluation
  - Technological focus
  - The expert model would not scale
  - Prioritizing results was frequently difficult
  - Wide variation in products and services
  - Often conducted without a site’s direct participation
  - Precipitated by an event
  - Frequently inconsistent or undefined valuation criteria
  - Few or no follow-on activities

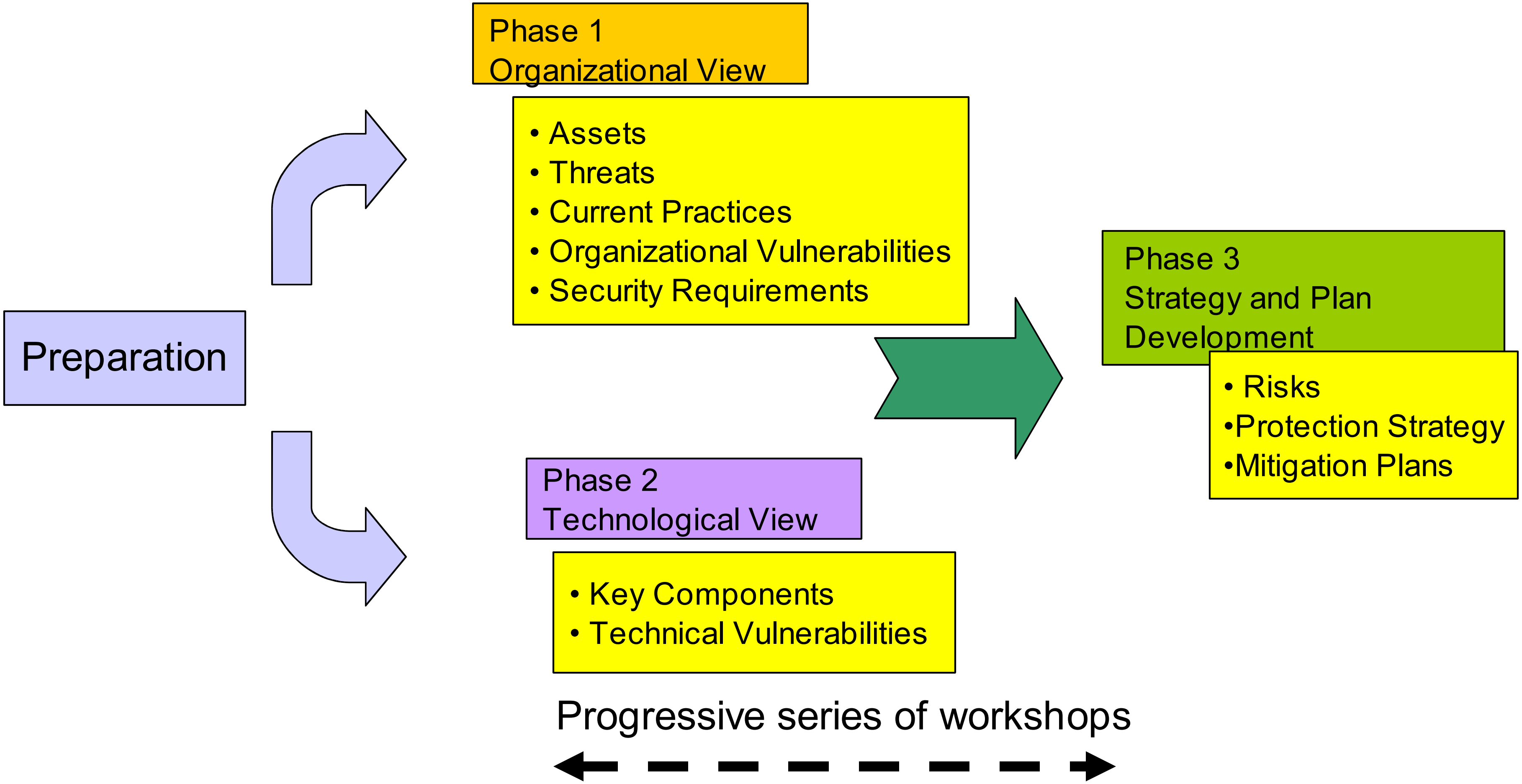
impruve
MANAGE RISK, MAXIMIZE REWARD

Conducting OCTAVE

- An interdisciplinary team – composed of:
  - Business or mission-related staff
  - Information Technology staff

impruve
MANAGE RISK, MAXIMIZE REWARD

OCTAVE Process



Preparation

Phase 1
Organizational View

- Assets
- Threats
- Current Practices
- Organizational Vulnerabilities
- Security Requirements

Phase 2
Technological View

- Key Components
- Technical Vulnerabilities

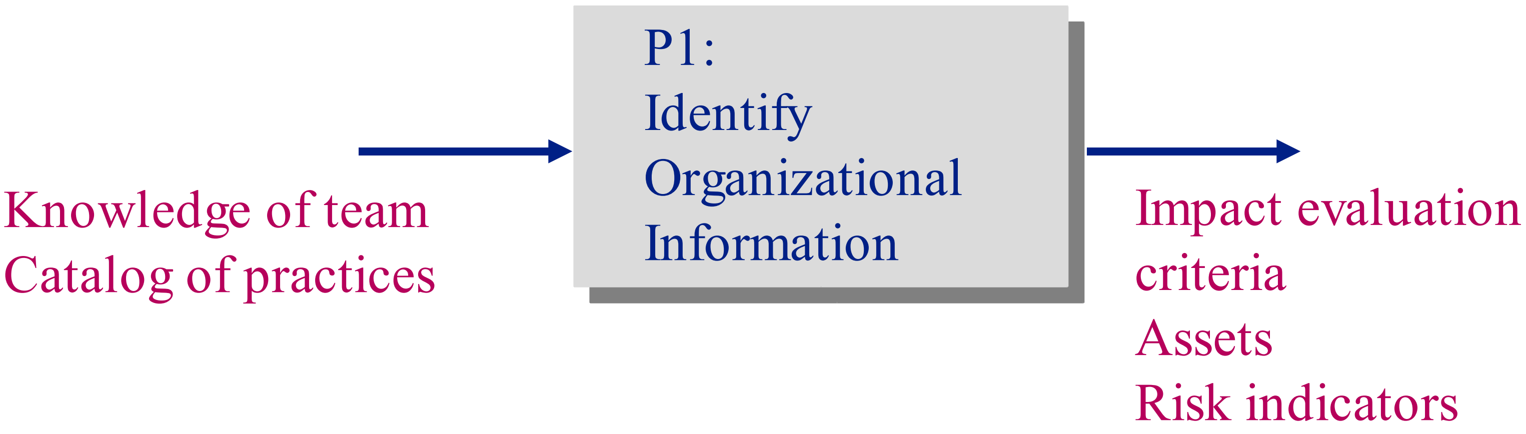
Phase 3
Strategy and Plan Development

- Risks
- Protection Strategy
- Mitigation Plans

Progressive series of workshops

Operationally Critical Threat, Asset and Vulnerability Evaluation

Process 1



Knowledge of team
Catalog of practices

P1:
Identify
Organizational
Information

Impact evaluation
criteria
Assets
Risk indicators

Activities

A1.1 Establish impact evaluation criteria

A1.2 Identify organizational assets

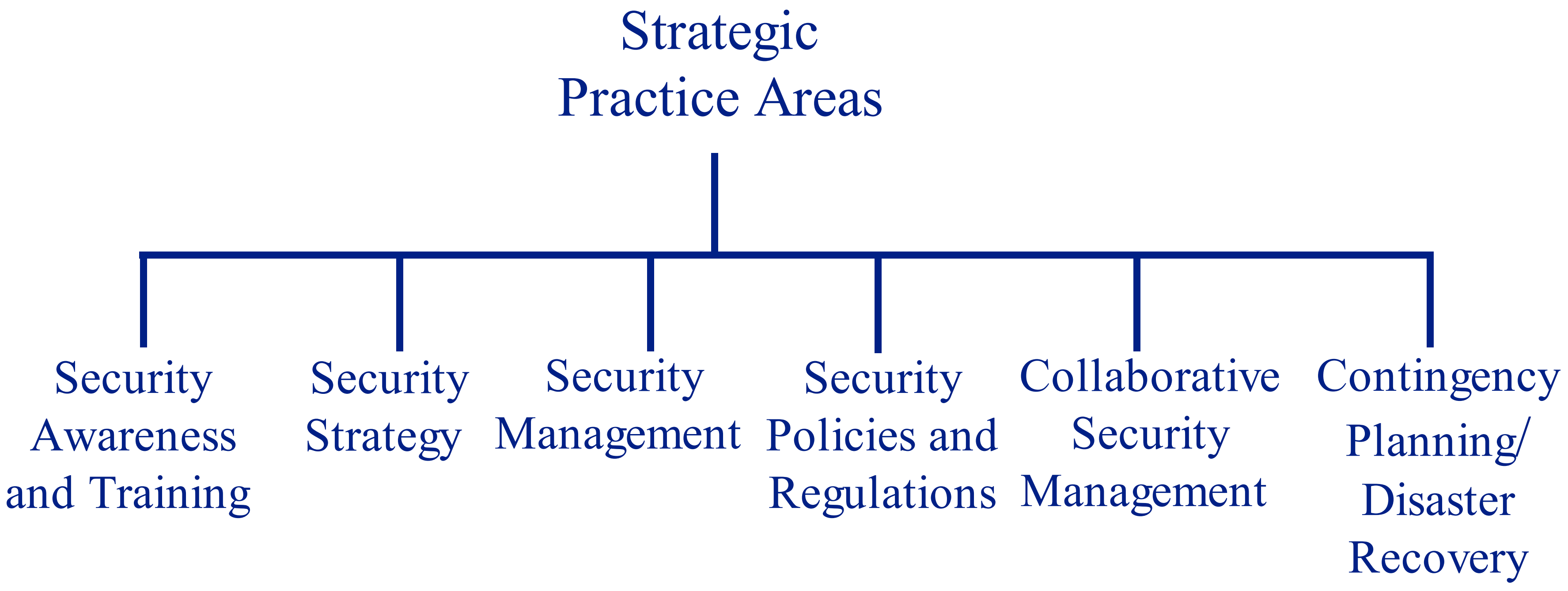
A1.3 Evaluate organizational security practices

impruve
MANAGE RISK, MAXIMIZE REWARD

Sample Risk Worksheet

Reputation/Customer Confidence			
Impact Type	**Low Impact**	**Medium Impact**	**High Impact**
Reputation	Reputation is minimally effected; little or no effort or expense required to recover.	Reputation is damaged and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than ________% reduction in customers due to loss of confidence.	________to ________% reduction in customers due to loss of confidence.	More than ________% reduction in customers due to loss of confidence.
Other:			
Other:			

Strategic Practice Areas

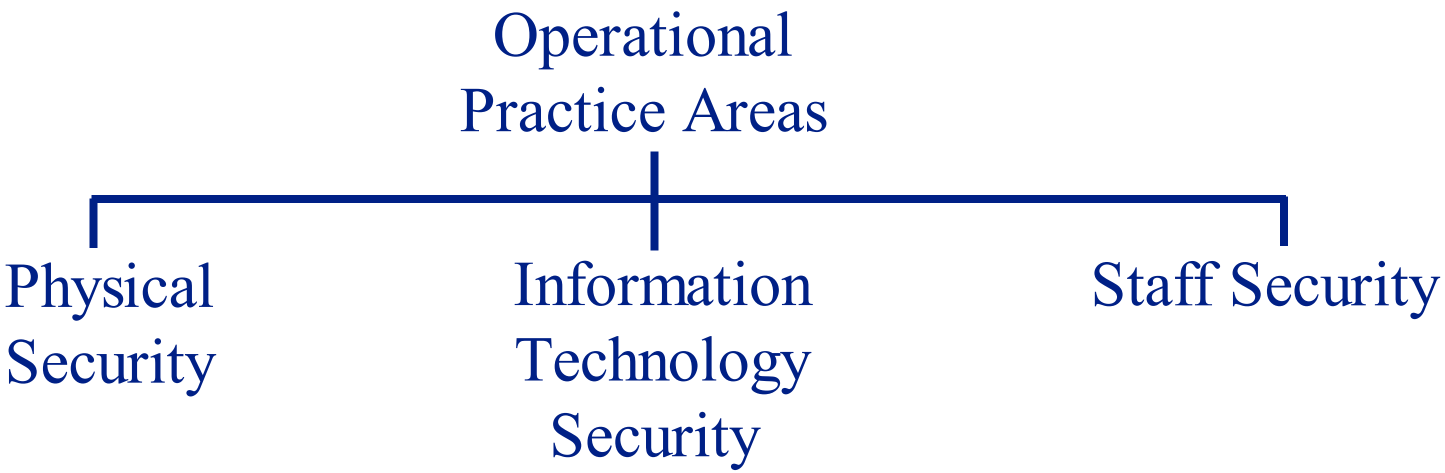


Strategic Practice Areas

- Security Awareness and Training
- Security Strategy
- Security Management
- Security Policies and Regulations
- Collaborative Security Management
- Contingency Planning/ Disaster Recovery

impruve
MANAGE RISK, MAXIMIZE REWARD

Operational Practice Areas



Operational Practice Areas

Physical Security

Information Technology Security

Staff Security

Physical Security Plans and Procedures

Physical Access Control

Monitoring and Auditing Physical Security

System and Network Management

System Administration Tools

Monitoring and Auditing IT Security

Authentication and Authorization

Vulnerability Management

Encryption

Security Architecture and Design

Incident Management

General Staff Practices

Sample Survey

Security Strategy
The organization’s strategies routinely incorporate security consideration.

Security strategies and policies take into consideration the organization’s strategies and goals.

Security strategies, goals, and objectives are documented and are routinely reviewed, updated, and communicated to the organization.

Security Management
Management allocates sufficient funds and resources to information security activities.

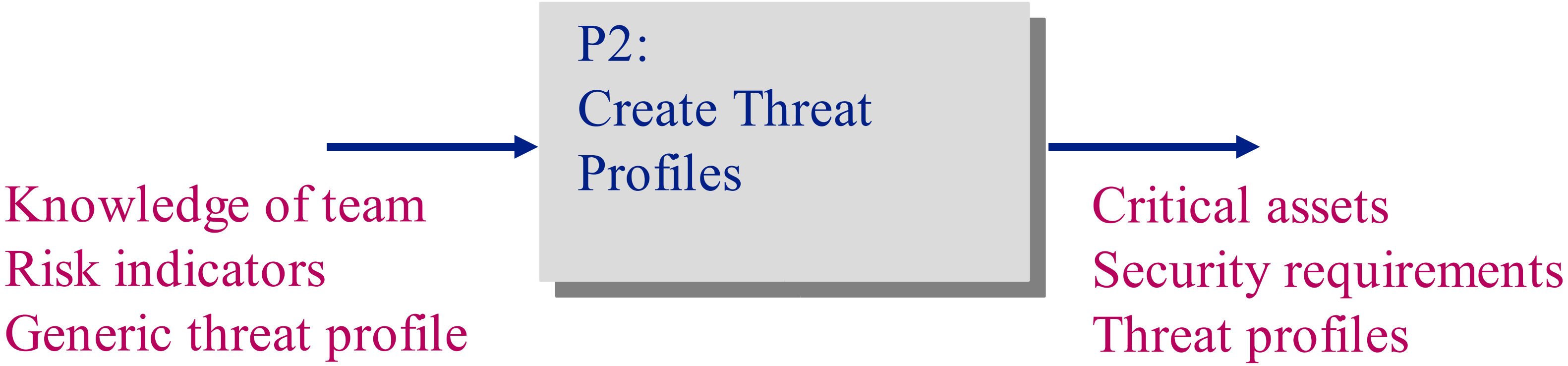
Security roles and responsibilities are defined for all staff in the organization.

The organization’s hiring and termination practices for staff take information security issues into account.

Sample Survey Results

Security Practice Areas														
		Strategic						Operational						
1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
								Staff Responses						
🟩	🟨	🟨	🟨	🟩	🟥	🟨	🟨	🟨	🟨	🟩	▨	▨	▨	🟨
								Div Managers Responses						
🟩	🟩	🟩	🟨	🟨	🟩	🟨	🟩	🟨	🟨	🟨	▨	▨	▨	🟨
								Senior Management						
🟩	🟥	🟩	🟩	🟩	🟥	🟩	🟨	🟨	🟨	🟩	▨	▨	▨	🟩

Process 2



P2:
Create Threat
Profiles

Knowledge of team
Risk indicators
Generic threat profile

Critical assets
Security requirements
Threat profiles

Activities

A2.1 Select critical assets

A2.2 Identify security requirements for critical assets

A2.3 Identify threats to critical assets

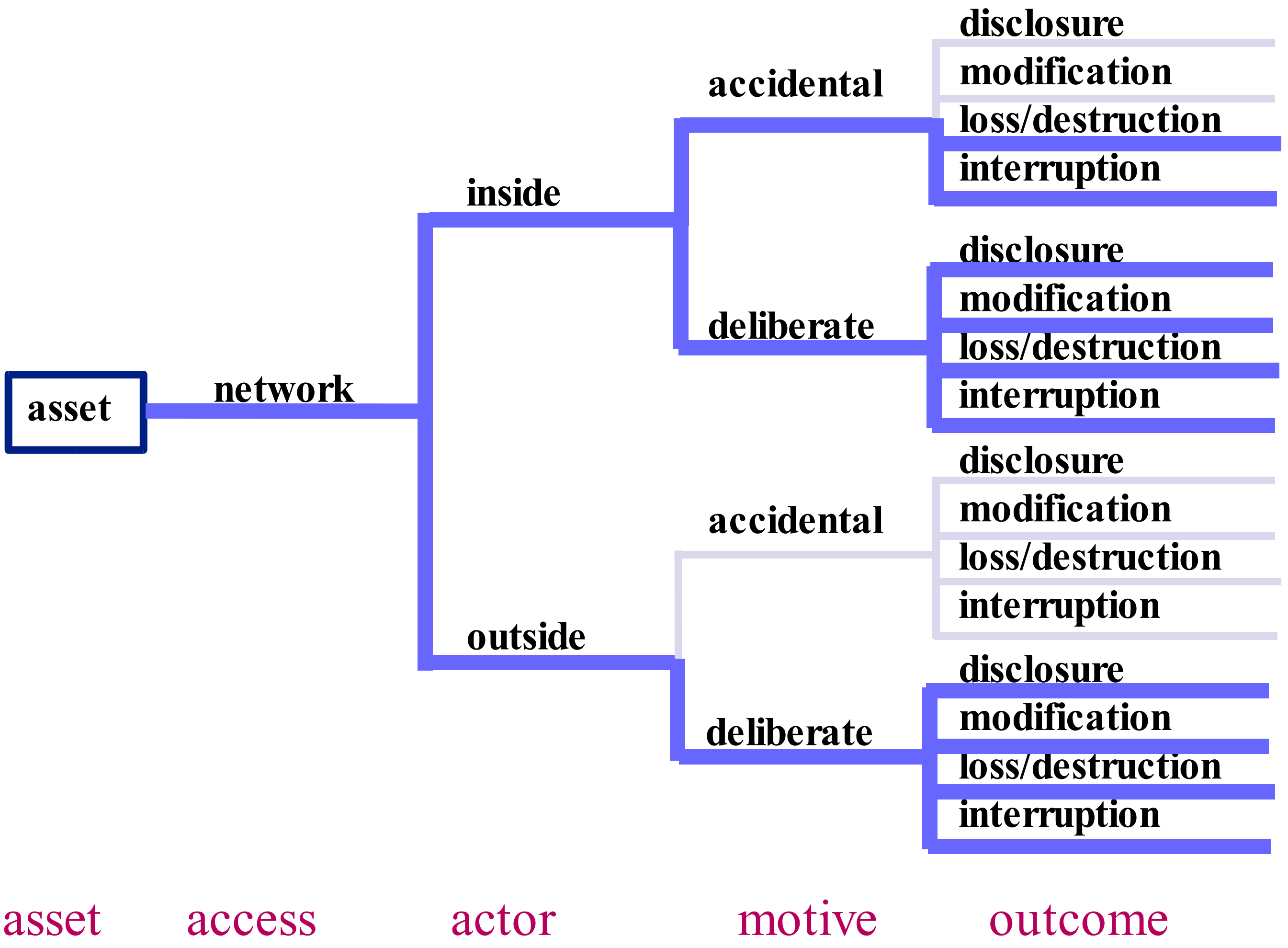
impruve
MANAGE RISK, MAXIMIZE REWARD

Critical Asset - Definition

Those assets that would have a large adverse impact on the organization if they were:

- Disclosed to unauthorized people
- Modified without authorization
- Lost or destroyed
- Access to them is interrupted

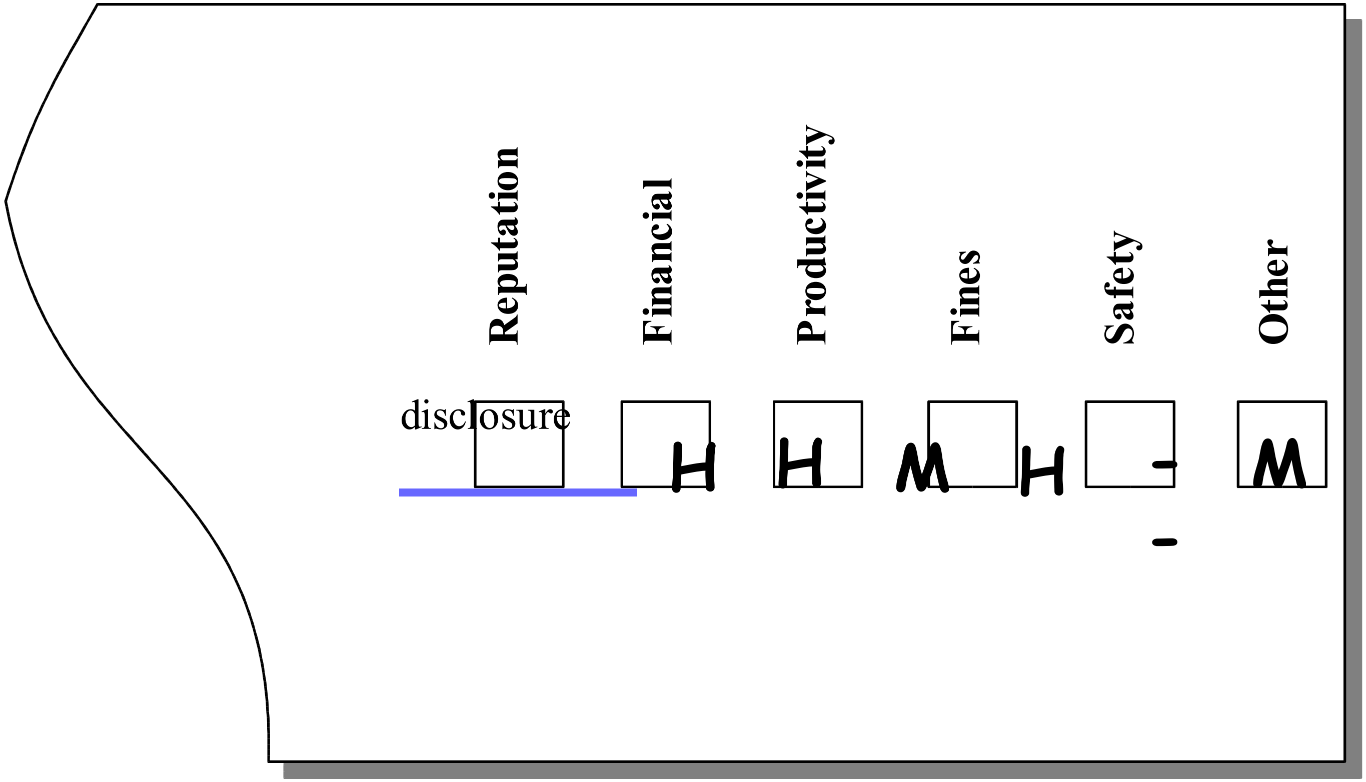
Human Actors - Network Access



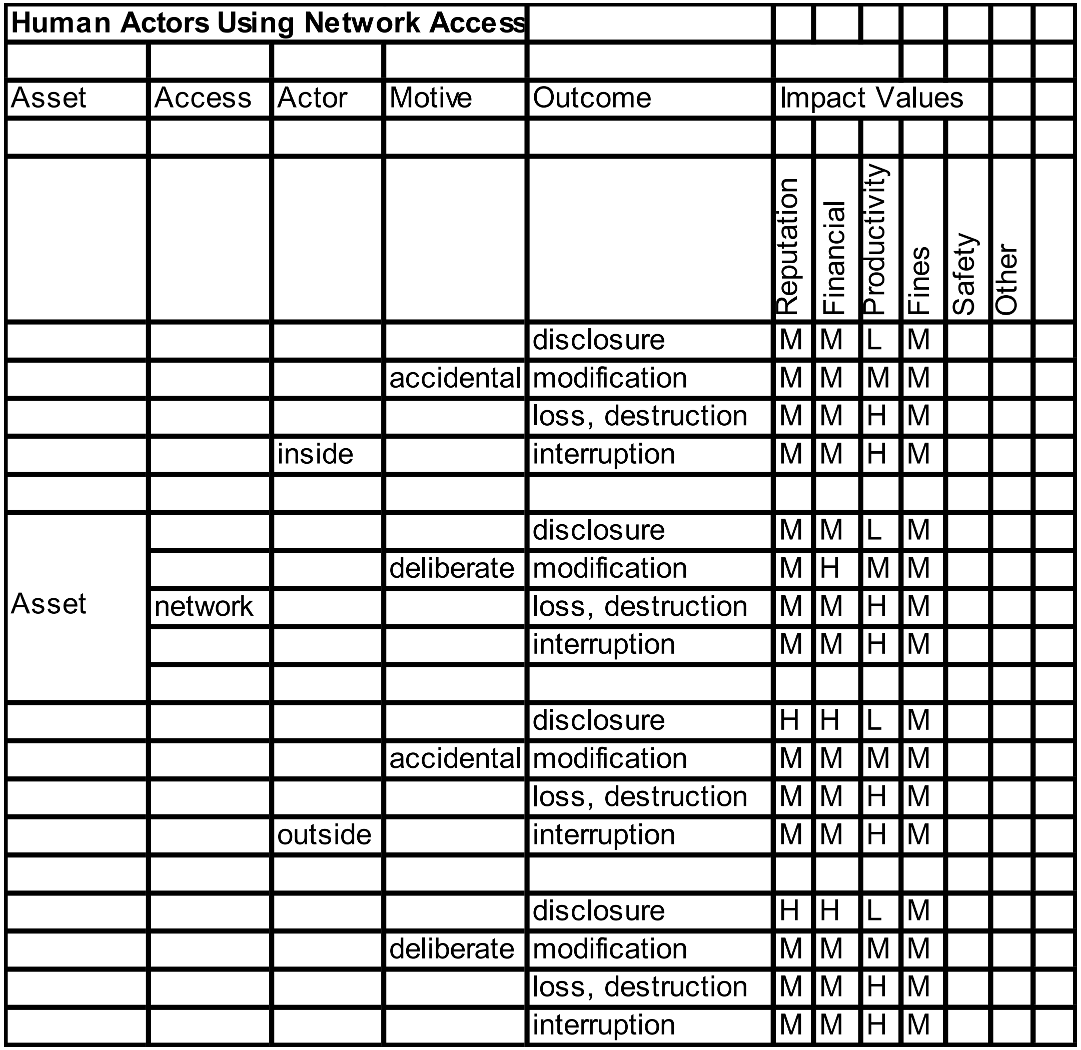
Worksheet Format

Human Actors Using Network Access				
Asset	Access	Actor	Motive	Outcome
				disclosure
			accidental	modification
				loss, destruction
		inside		interruption
Asset				disclosure
			deliberate	modification
	network			loss, destruction
				interruption
				disclosure
			accidental	modification
				loss, destruction
		outside		interruption
				disclosure
			deliberate	modification
				loss, destruction
				interruption

Impact Values Recorded in the Risk Profile

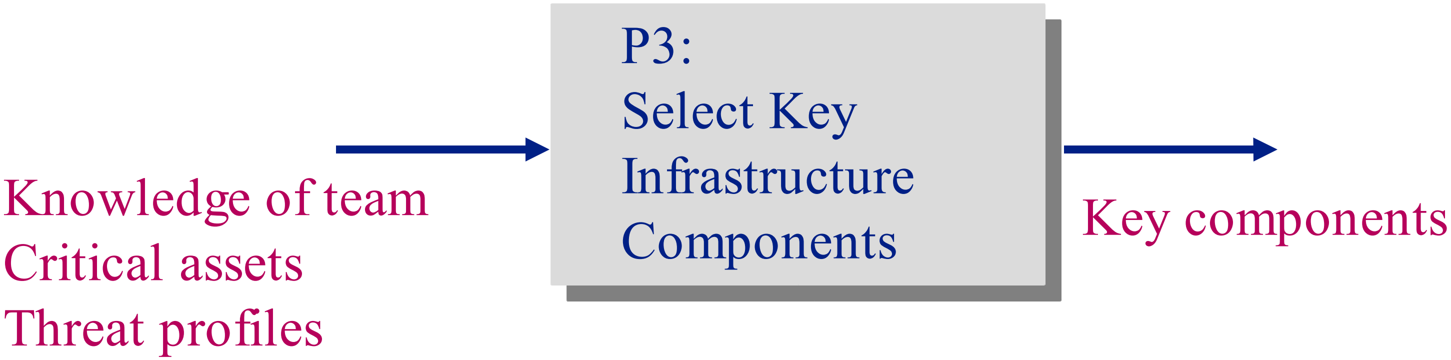


Adding Impact Values



Human Actors Using Network Access											
Asset	Access	Actor	Motive	Outcome	Impact Values						
					Reputation	Financial	Productivity	Fines	Safety	Other	
				disclosure	M	M	L	M			
			accidental	modification	M	M	M	M			
				loss, destruction	M	M	H	M			
		inside		interruption	M	M	H	M			
Asset				disclosure	M	M	L	M			
			deliberate	modification	M	H	M	M			
	network			loss, destruction	M	M	H	M			
				interruption	M	M	H	M			
				disclosure	H	H	L	M			
			accidental	modification	M	M	M	M			
				loss, destruction	M	M	H	M			
		outside		interruption	M	M	H	M			
				disclosure	H	H	L	M			
			deliberate	modification	M	M	M	M			
				loss, destruction	M	M	H	M			
				interruption	M	M	H	M			

Process 3



Knowledge of team
Critical assets
Threat profiles

P3:
Select Key
Infrastructure
Components

Key components

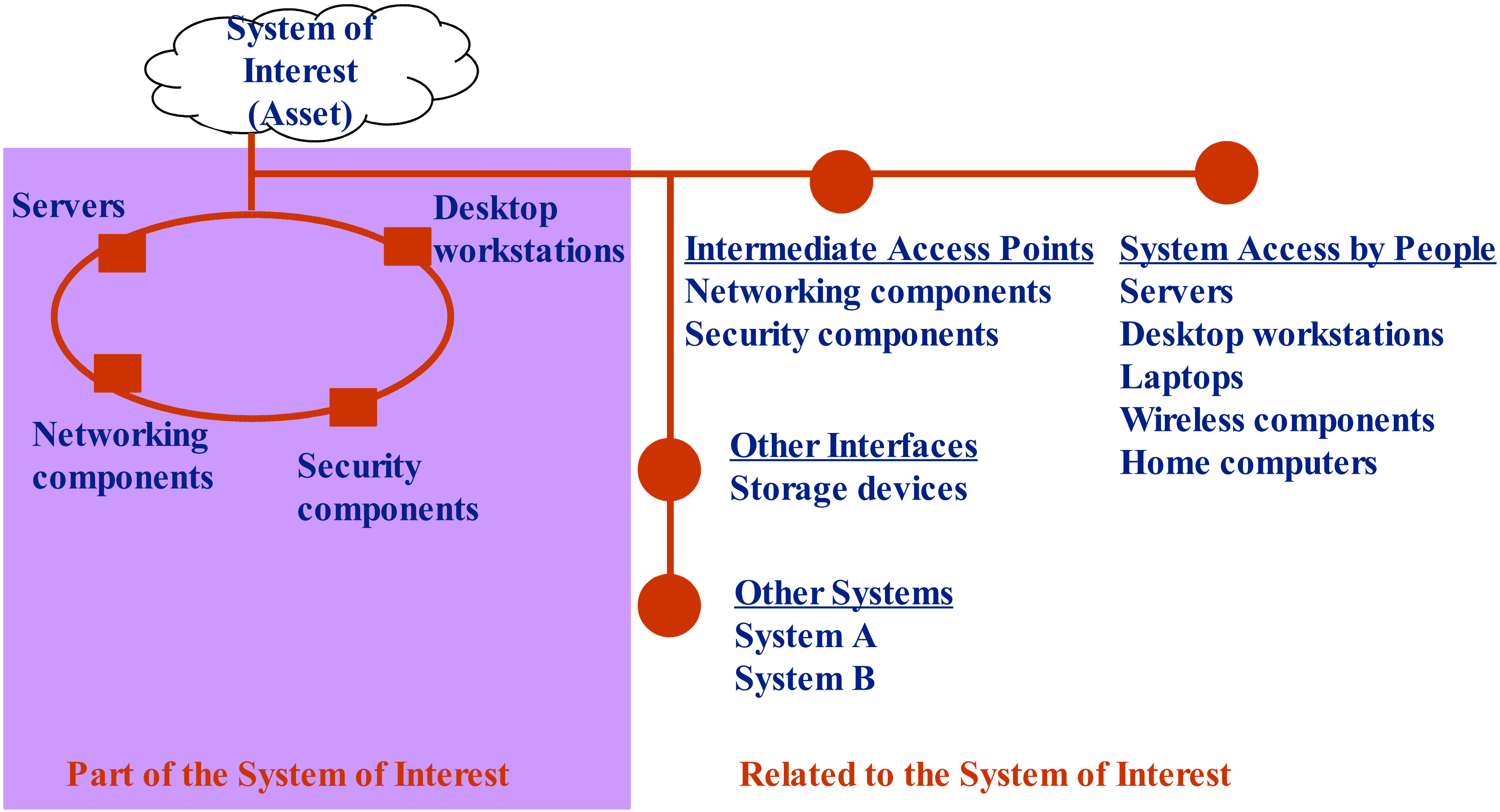
<u>Activities</u>

A3.1 Establish vulnerability evaluation strategy

A3.2 Identify key classes of components

A3.3 Select infrastructure components to evaluate

Key Classes of Components -2



System of Interest (Asset)

Servers

Desktop workstations

Networking components

Security components

Part of the System of Interest

Intermediate Access Points
Networking components
Security components

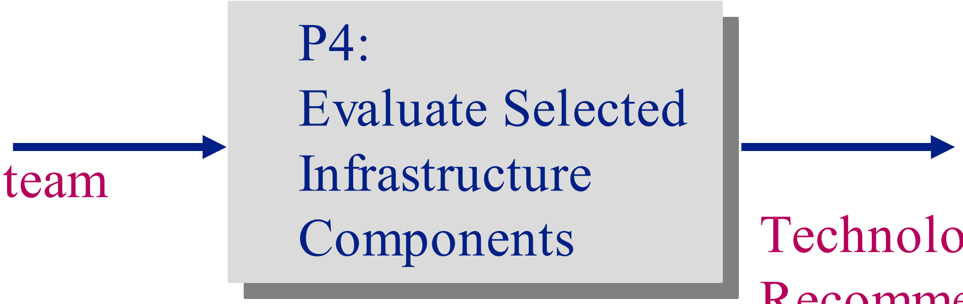
System Access by People
Servers
Desktop workstations
Laptops
Wireless components
Home computers

Other Interfaces
Storage devices

Other Systems
System A
System B

Related to the System of Interest

Process 4



P4:
Evaluate Selected Infrastructure Components

Knowledge of team
Critical assets
Threat profiles
Key components
Catalog of vulnerabilities

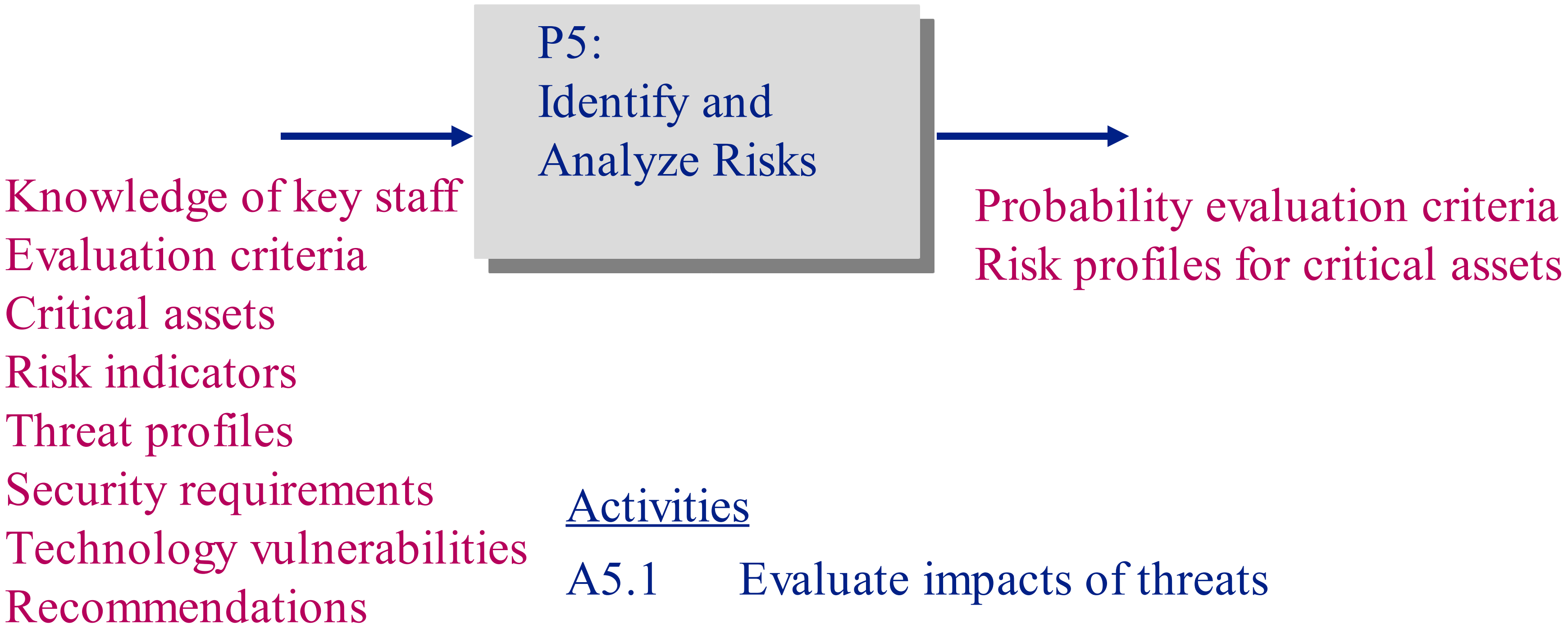
Technology vulnerabilities
Recommendations

Activities

A4.1 Run vulnerability evaluation tools

A4.2 Analyze technology vulnerabilities

Process 5



P5:
Identify and
Analyze Risks

Knowledge of key staff
Evaluation criteria
Critical assets
Risk indicators
Threat profiles
Security requirements
Technology vulnerabilities
Recommendations

Probability evaluation criteria
Risk profiles for critical assets

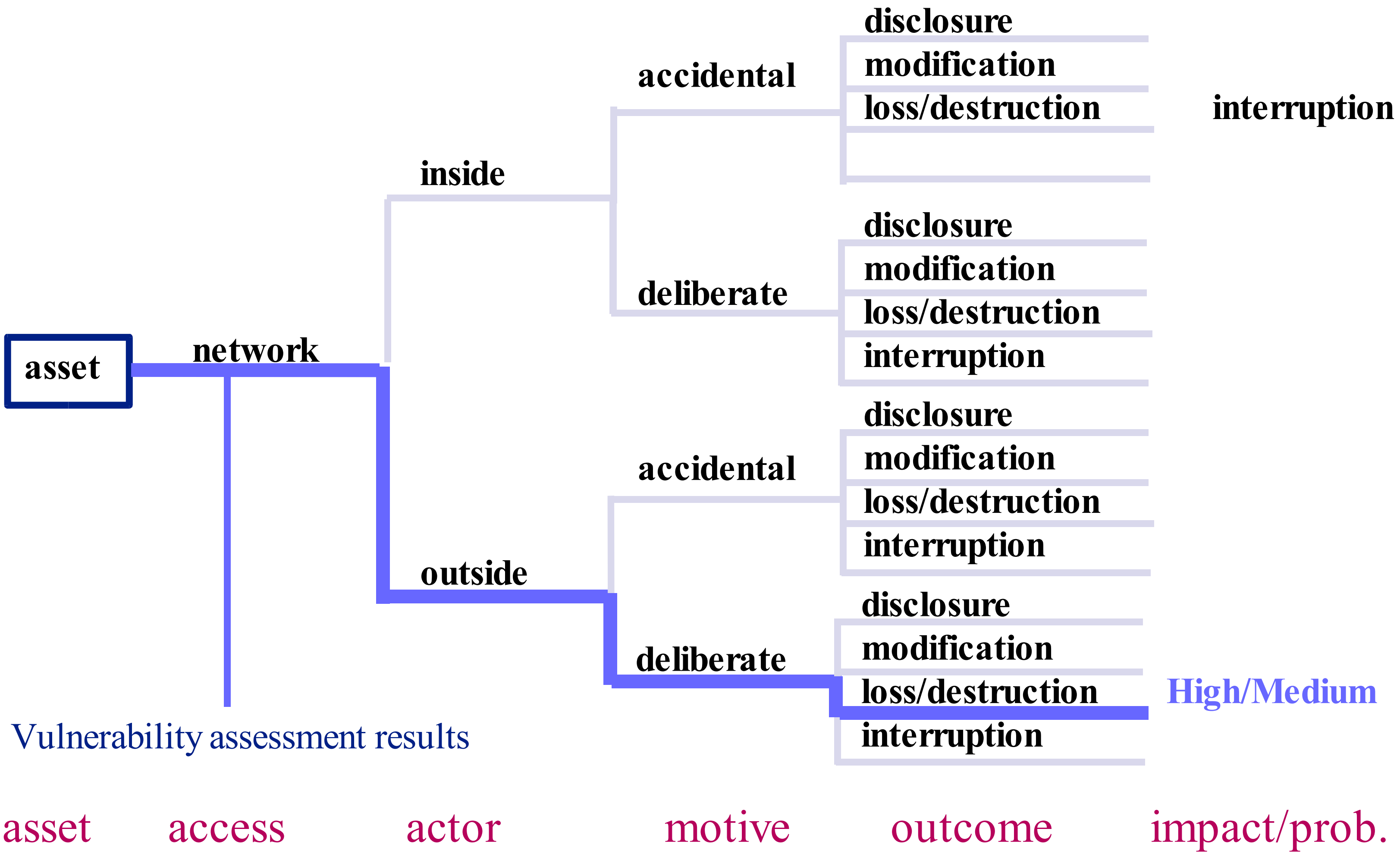
Activities

A5.1 Evaluate impacts of threats

A5.2 Establish probability evaluation criteria

A5.3 Evaluate probabilities of threats

Expression of Risk -2



asset

network

inside

accidental

disclosure

modification

loss/destruction

interruption

deliberate

disclosure

modification

loss/destruction

interruption

outside

accidental

disclosure

modification

loss/destruction

interruption

deliberate

disclosure

modification

loss/destruction

High/Medium

interruption

Vulnerability assessment results

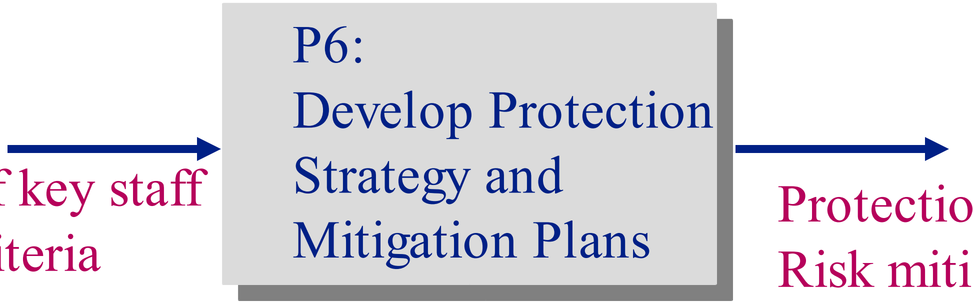
asset access actor motive outcome impact/prob.

impruve
MANAGE RISK, MAXIMIZE REWARD

Probabilities in Worksheet

Human Actors Using Network Access															
Asset	Access	Actor	Motive	Outcome	Impact Values							Probability			
												Value	Confidence		
					Reputation	Financial	Productivity	Fines	Safety	Other			Very Much	Somewhat	Not at All
				disclosure	H	H	M	M		L		M		X	
			accidental	modification										X	
				loss, destruction										X	
		inside		interruption										X	
Asset				disclosure	H	H	M	M		L		L		X	
			deliberate	modification										X	
	network			loss, destruction										X	
				interruption										X	
				disclosure	H	H	M	M		L		L			X
			accidental	modification											X
				loss, destruction											X
		outside		interruption											X
				disclosure	H	H	M	M		L		L		X	
			deliberate	modification										X	
				loss, destruction										X	
				interruption										X	

Process 6



P6:
Develop Protection Strategy and Mitigation Plans

Knowledge of key staff
Evaluation criteria
Critical assets
Risk indicators
Security requirements
Technology vulnerabilities
Recommendations
Risk profiles for critical assets

Protection strategy
Risk mitigation plans
Next steps

Activities

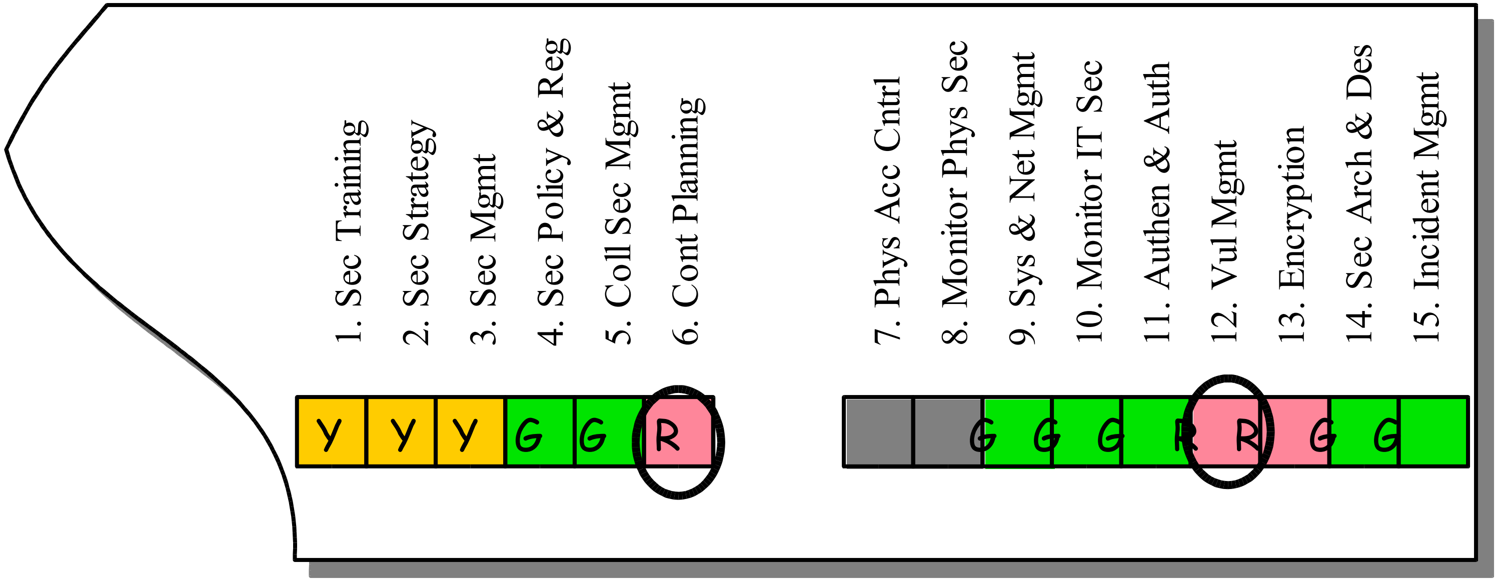
A6.1	Describe current protection strategy
A6.2	Select mitigation approaches
A6.3	Develop risk mitigation plans
A6.4	Identify changes to protection strategy
A6.5	Identify next steps

Worksheet with Practice Areas

Human Actors Using Network Access																																			
Step 11					Step 25							Step 27					Step 29																Step 30		
Asset	Access	Actor	Motive	Outcome	Impact Values							Probability					Security Practice Areas																Approach		
												Value	Confidence						Strategic						Operational										
					Reputation	Financial	Productivity	Fines	Safety	Other			Very Much	Somewhat	Not at All		1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt		Accept	Defer	Mitigate
				disclosure	M	M	L	M				M		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
			accidental	modification	M	M	M	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨			X	
				loss, destruction	M	M	H	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨			X	
		inside		interruption	M	M	H	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨			X	X
				disclosure	M	M	L	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
			deliberate	modification	M	H	M	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
Asset	physical			loss, destruction	M	M	H	M				M		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
				interruption	M	M	H	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
				disclosure	H	H	L	M				L			X		🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
			accidental	modification	M	M	M	M				L			X		🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨		X		
				loss, destruction	M	M	H	M				L			X		🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
		outside		interruption	M	M	H	M				L			X		🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
				disclosure	H	H	L	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
			deliberate	modification	M	M	M	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨		X		
				loss, destruction	M	M	H	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X
				interruption	M	M	H	M				L		X			🟩	🟨	🟥	🟩	🟥	🟨	▒	▒	🟨	🟨	🟨	🟨	🟨	🟥	🟨				X

Mitigating Risks

For risks that you intend to mitigate, you must determine which security practice areas need to be addressed.



1. Sec Training	2. Sec Strategy	3. Sec Mgmt	4. Sec Policy & Reg	5. Coll Sec Mgmt	6. Cont Planning	7. Phys Acc Cntrl	8. Monitor Phys Sec	9. Sys & Net Mgmt	10. Monitor IT Sec	11. Authen & Auth	12. Vul Mgmt	13. Encryption	14. Sec Arch & Des	15. Incident Mgmt
Y	Y	Y	G	G	[✓ R]			G	G	G	[✓ R]	R	G	G

Note: The security practice areas for which mitigation activities will be implemented are circled.

impruve
MANAGE RISK, MAXIMIZE REWARD

Example: Mitigation Plan

Mitigation Activity	**Rationale**
Which mitigation activities are you going to implement in this security practice area?	*Why did you select each activity?*
☒ Document business continuity or emergency operation plans, disaster recovery plan(s), and contingency plan(s) for responding to emergencies. (*Documented Plans*)	□ *Recognize* threats as they occur □ *Resist* threats to present them from occurring ☒ *Recover* from threats after they occur *Additional Notes* The organization currently has no business continuity plan, emergency operation plan, or disaster recovery plan

Mitigation Responsibility	**Additional Support**
Who needs to be involved in implementing each activity? Why?	*What additional support will be needed when implementing each activity (e.g., funding, commitment of staff, sponsorship)?*
The analysis team needs to present this plan to the senior management team. Senior managers need to assign responsibility for developing all required contingency plans.	Senior management needs to endorse this activity, assign staff to complete it, and provide any necessary funds to support it.

Outputs of OCTAVE

Protection Strategy →

Defines organizational direction

Mitigation Plan →

Plans designed to reduce risk

Action List →

Near-term action items

- Enables you to effectively communicate critical information security issues
- Provides a foundation for future security improvements
- Positions your organization for compliance with data security requirements or regulations

Business Value

- Reduces risk/exposure
- Regulatory compliance
- Alignment of IT strategy with the organization’s mission and objectives
- Provides a baseline for security best practices
- IT expenditure justification for organization’s capital budgeting decisions
- Due diligence
- Protection of corporate reputation
- Builds customer confidence

OCTAVE Advantages

- Systematic and non-proprietary risk assessment methodology (no vendor lock-in)
- Superior pedigree and project sponsor (developed by Carnegie Mellon University/SEI)
- Leverages academic research and industry best practices
- Tailor-able to the individual organization’s strategic mission and objectives (others are much more rigid)
- Results in specific deliverables and action items
- Periodic updates may be performed by an organization’s internal teams using gap analysis techniques

Conclusion

- A technology risk assessment that’s both well-respected and thorough
- The robustness of tools, workshops, and publications to OCTAVE significantly enhances an effective assessment
- Asset-centric vs. perimeter-centric approach--focuses on the targets, not the attackers
  - More manageable
  - More organizationally relevant
  - Addresses the issues involving the evolution of modern IT systems
- Ensures business continuity and survivability

References

OCTAVE Materials www.cert.org/octave

Managing Information Security Risks, the OCTAVE Approach Alberts and Dorofee. Published by Addison Wesley

Certified OCTAVE Facilitators/Trainers

Impruve www.impruve.com

650 341-9133