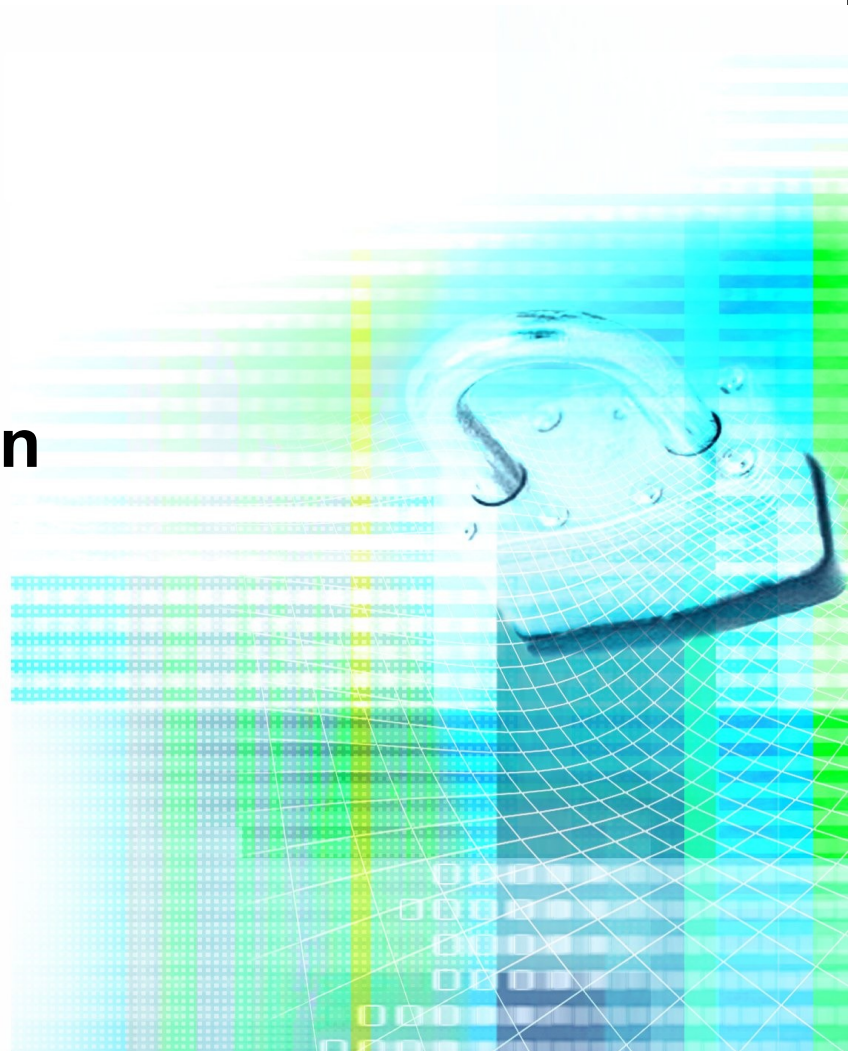
Workshop:
OCTAVE

IMF 2007

Dipl.-Inform. Christian Paulsen

DFN-CERT Services GmbH
paulsen@dfn-cert.de



Introduction

- Who am I?
- What have I done?
- What am I currently doing?

Please interrupt if you have any questions!

Agenda

- Introduction
- Why Risk Analysis?
- Existing methods
- The OCTAVE-Method
- Summary
- Discussion

Introduction: DFN-CERT

- **DFN-CERT Services GmbH**
  - 1993 to 1999: project at University of Hamburg
  - Main Customer: DFN-Verein
- **Structure**
  - Incident Response Team
  - PKI Team
  - Organisation
  - Research Team
- **Events**
  - DFN-Workshop „Security in Networked Systems“
  - Tutorials

Incident Response Team

- **Prevention**
  - Security Advisories, Security Bulletins
  - Vulnerability Analysis, Intrusion Detection
  - Training / education
  - Contact for security questions / „Hotline“
- **Reaction**
  - Incident Response Support
  - Incident Analysis
  - Coordination
  - Cooperation with other IR-Teams

Security Advisories

- **Using "German Advisory Format" (DAF)**
- **Developed and maintained by**
  - Cert-BUND, DFN-CERT, Siemens CERT and PRESECURE
- **Format: XML**
- **Information about vulnerabilities / patches (hardware and software)**

Example Advisory

Plattform Categorisation	Windows, Windows 95/98/ME, Windows NT, Windows 2000, Windows XP, Windows Server 2003

Plattform Description

Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
Microsoft Windows 2000 Service Pack 3 und 4
Microsoft Windows XP, Microsoft Windows XP Service Pack 1 und 2
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server 2003
Microsoft Windows Server 2003 64-Bit Edition
Microsoft Windows 98,
Microsoft Windows 98 Second Edition (SE)
Microsoft Windows Millennium Edition (Me)

Software Categorisation	Client

Software Description

Internet Explorer 5.01, 5.5 und 6

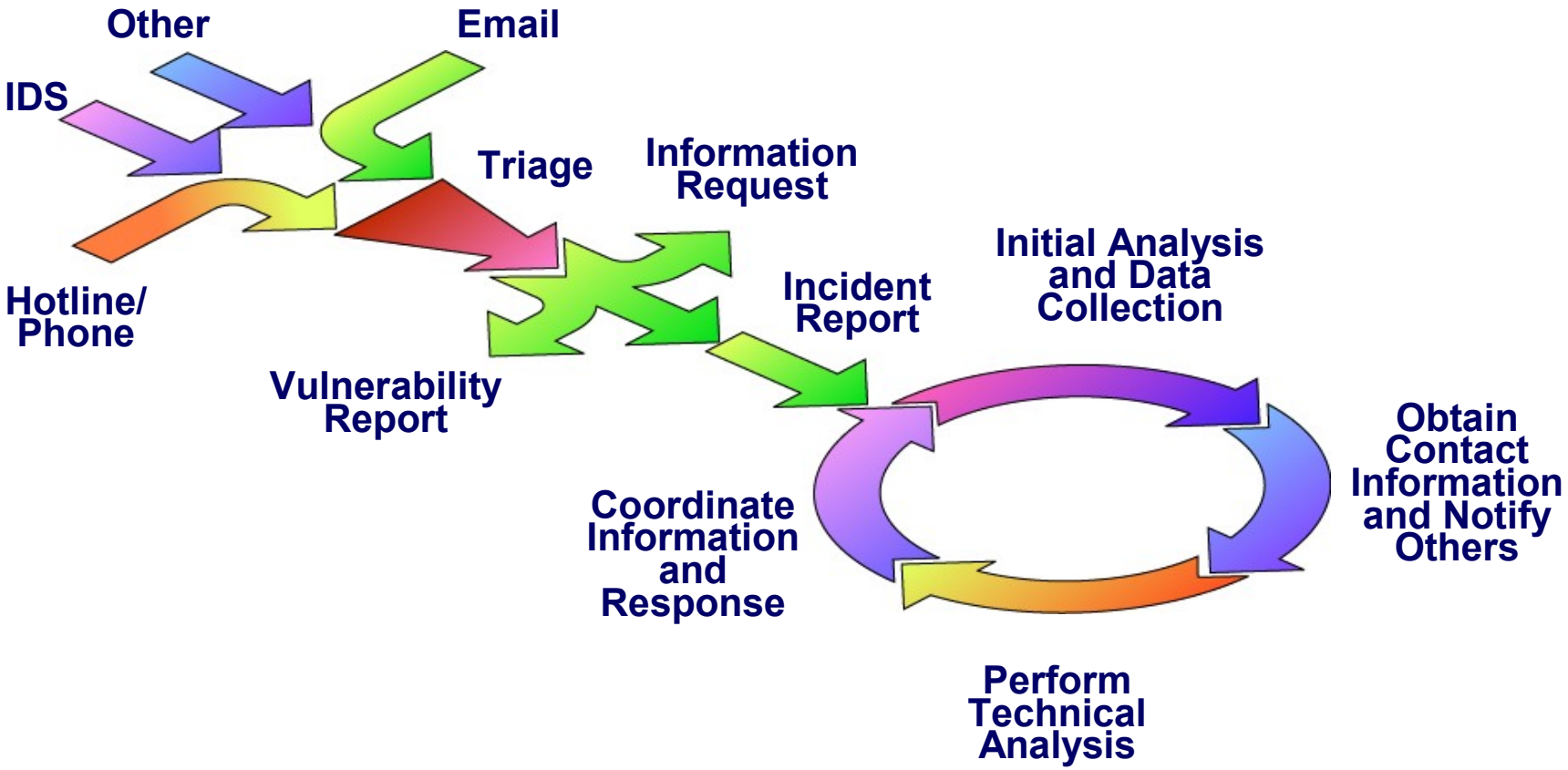
Vulnerabilities

Status	Exploit published
Propagation	Automated
Scope and Loss	Code Execution as Admin (very high impact)
Requirements	Victim interaction: access content
Categorisation	Buffer Overflow, Heap Overflow, Cross-site Scripting
Immediacy	High (Proposal: High)
Current Impact	Very high (Proposal: Very high)

Incident Handling

- **Typical business for Incident Handlers**
  - Analysis of incidents
  - Analysis of incident infos (logfiles, artefacts, etc.)
  - Searching for a contact person
  - Technical support for the “victim” (by phone or mail, less personal)
  - Coordination and spreading of infos
  - Cooperation with other teams

Incident Handling



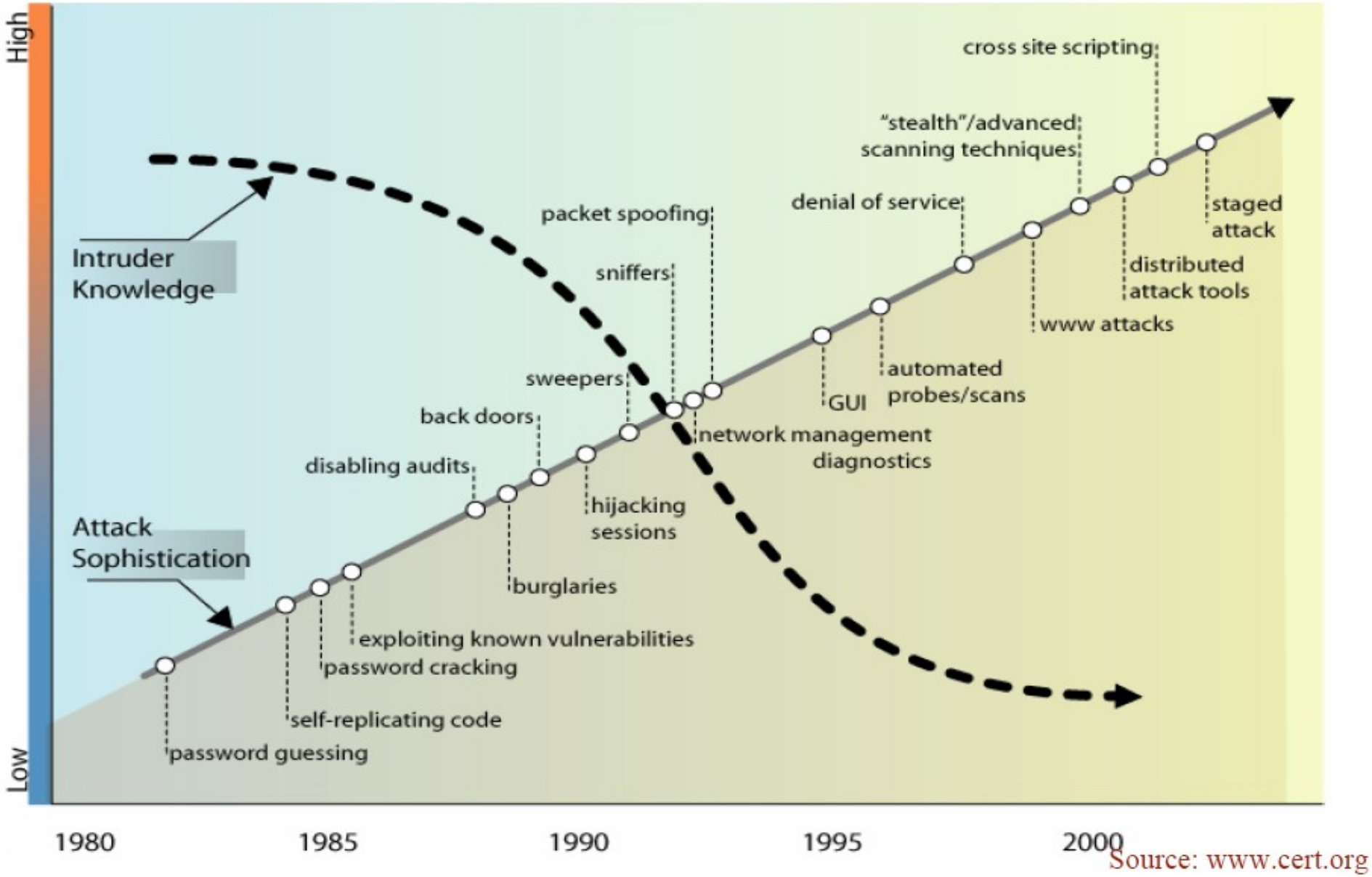
Incidents: Examples

- **Typical examples for incidents:**
- Organisation reports a compromised server
- Another CERT informs about a compromised system
- Portscan-reports (automated and manual)
- Virus- and proxy-reports (mostly automated)
- Requests from law enforcement agencies

Agenda

- Introduction
- Why Risk Analysis?
- Existing methods
- The OCTAVE-Method
- Summary
- Discussion

Impact / Intruder Know-How



Why Risk Analysis?

- **Less time for reaction:**
  - Automated vulnerability scans
  - Automated development of exploits
  - Admins have less time
- **Cooperation of different „black hat“ groups**
- **Underground economy develops**
- **Organized crime joins**

Why Risk Analysis?

- **New generation of malware**
- **Example: PhatBot**
  - Worm and IRCBot
  - Easy created and extended (modular)
  - Lots of mutations
  - Looks for passwords, creditcard numbers, licence keys...
  - More features: DDoS Agent, FTP-Server, HTTP-Proxy, Sniffer, Spam-Agent, ...
  - Link: http://www.lurhq.com/phatbot.html

Why Risk Analysis?

- People using the internet are often unaware of the risks!
- What documented recovery plans exist?
- Who is responsible?
- What is my budget?

Security management requires a plan to recognize, resist and recover!

How it should be

- **Effective IT security risk management requires:**
  - A systematic process
  - Experience and expertise
  - Information (risks, lessons learned)
  - A risk-aware culture

Agenda

- Introduction
- Why Risk Analysis?
- Existing methods
- The OCTAVE-Method
- Summary
- Discussion

Existing Methods

- **Examples for risk evaluation standards:**
  - Baseline Protection Manual of the German BSI (BSI Grundschutzhandbuch)
  - ITIL
  - Common
  - ISO 27001
- **Focus is primarily on technology**
- **Led by experts**
- **Accurate for a very limited timeframe**

Disadvantages of many methods

- Lack of concrete support for the analysis
- Driven by tailored – consultant driven – materials
- Lack of internal participation
- No internal (organizational) learning
- Dependency on experts for doing it
- „Not developed here!“
- Lack of continuity
- Lack of none-technical topics and view

Complexity

A Complex Domain

Threats

- People inside your organization
- People outside your organization
- System problems
- Other problems

Security Practices

- Organizational practices
- Technical practices

People Involved

- Information technology (IT) staff
- General staff
- Managers
- Contractors
- Service providers
- Partners and collaborators

Agenda

- Introduction
- Why Risk Analysis?
- Existing methods
- The OCTAVE-Method
- Summary
- Discussion

What is OCTAVE?

- **OCTAVE =**
  Operationally Critical Threat, Asset and Vulnerability Evaluation
- **Developed at the Carnegie Mellon University by the Software Engineering Institute**
- **Supports self-service**
  - forms
  - check lists
  - working plan and structure
- **Emphasizes a value based analysis of the most relevant risks and security measures**

What is OCTAVE?

- **OCTAVE-S is a risk-based strategic assessment and planning technique for security**
- **Founding Philosophy:**
  - You cannot mitigate all IT-security risks
  - Your budget is limited
  - You cannot prevent all skilled incursions
- **You need to determine the best use of your limited resources to ensure the survivability of your organization!**

Assets

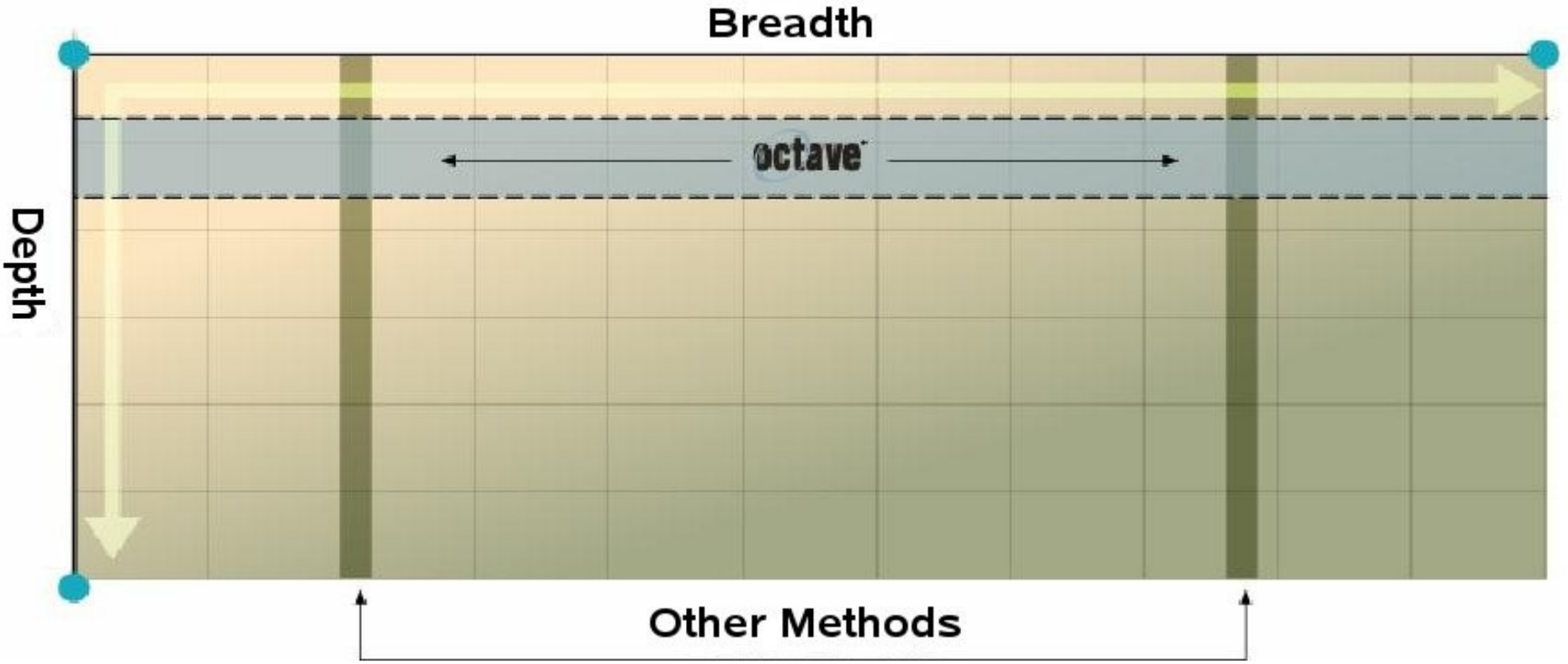
- **OCTAVE deals a lot with assets**

- **An asset is something of value to the organization**
  - information
  - systems
  - services and application
  - people

OCTAVE vs. OCTAVE-S

- OCTAVE-S is designed for smaller organizations / departments
- OCTAVE-S defines a more structured method for evaluating risks
- OCTAVE-S requires less security expertise in analysis team
- OCTAVE-S requires a smaller analysis team

Comparison with other methods



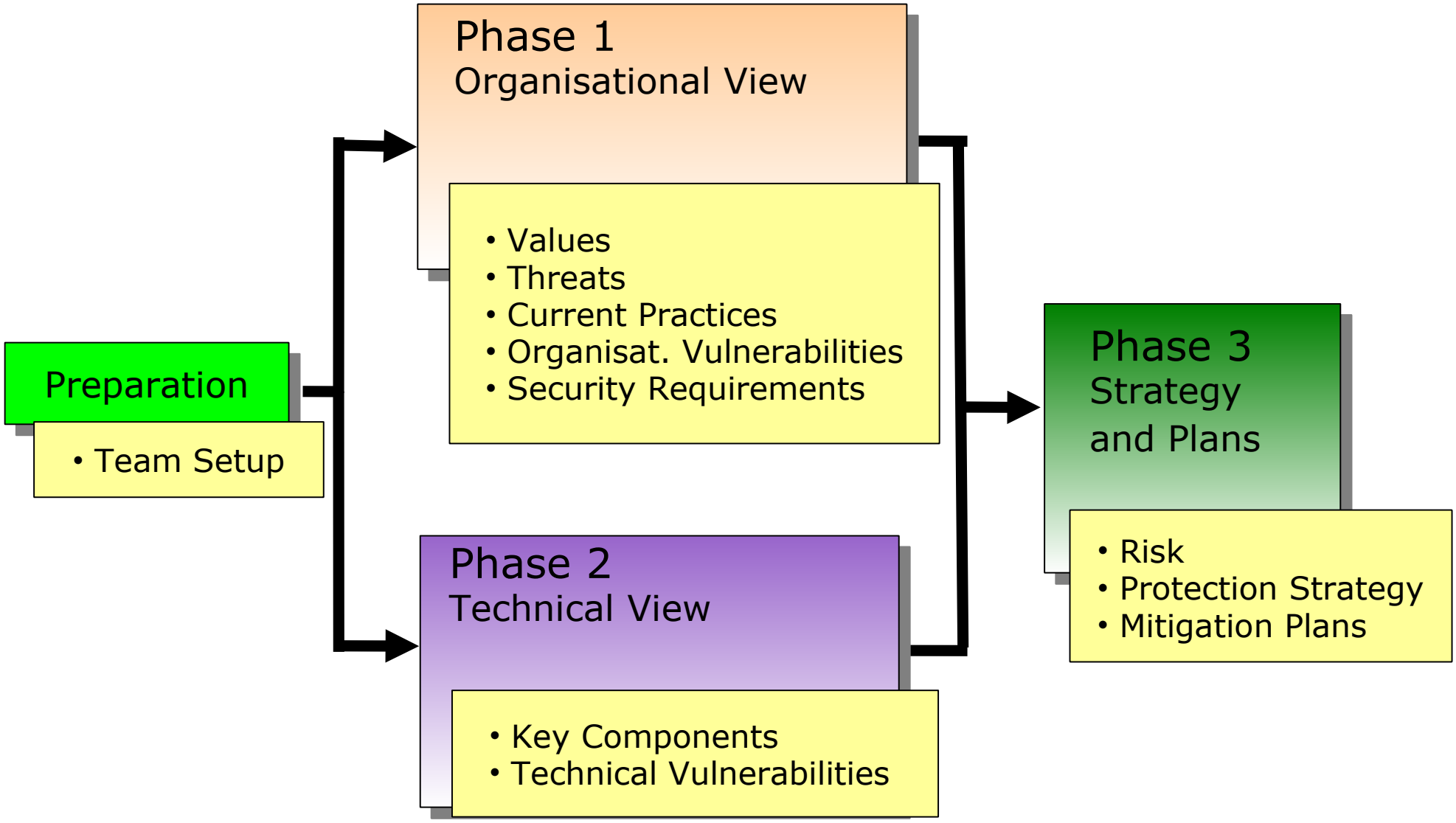
Continuous Risk Management

Covered by OCTAVE

Overview

OCTAVE	Other Evaluations
Organization evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self direction	Expert led

OCTAVE Phases



Preparation – Step A

- **Select team members from (important) business units**
  - Emphasizing the concrete use of systems
  - Knowledge of business processes
  - In depth familiarity with organisational rules, practices and users

Preparation – Step B

- **Select team members from the IT department**
  - Concrete involvement and technical expertise
  - Covering at least the following areas:
    - Desktops, Laptops, PDAs
    - Servers, active network components
    - Networks, local and wide area

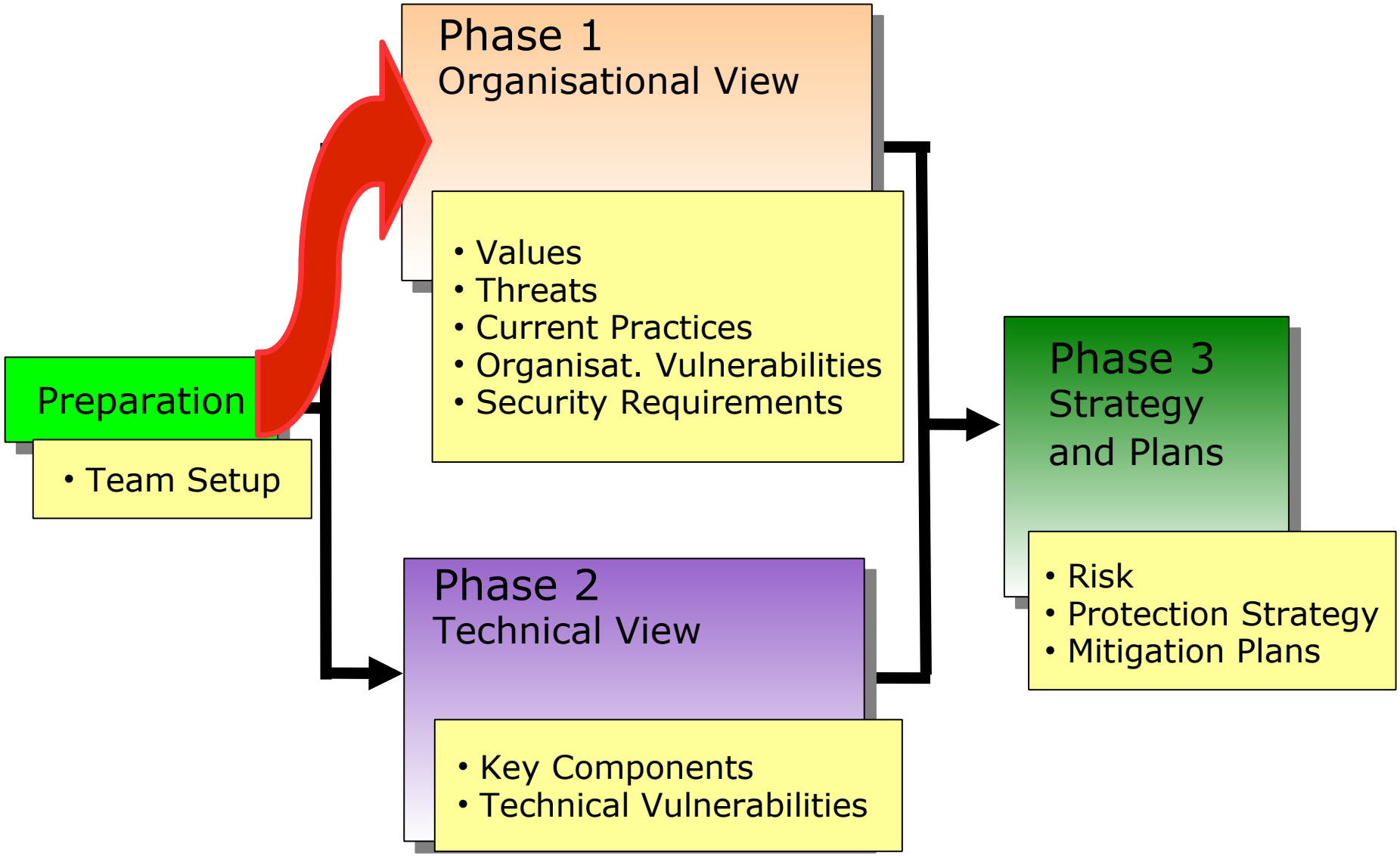
Which unit is important?

- Difficult to get not distracted by „Everything is important!“
- Some units need to be highly available!
- Some processes need to be function at all times!
- Some parts are more vulnerable then others!
- Some areas have been a target before!

Result of Preparation

- **An interdisciplinary team of:**
  - business or mission-related staff
  - information technology staff or people who interface with service providers

OCTAVE Phases

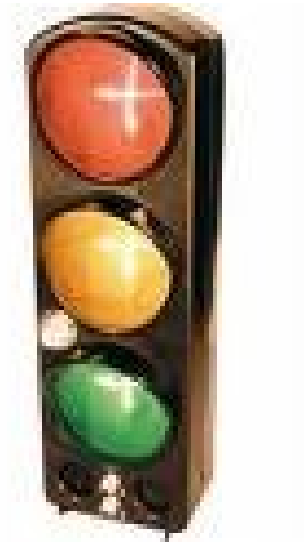


Phase 1 – S1 – Collect Infos

- **Identification of all (considerable) values**
  - Information
  - IT systems
  - Applications
  - Processes
    - Support Processes
    - Control Processes
    - Service Processes
  - Staff members
  - Infrastructure

Phase 1 – S1 - Status Quo

- **Which security measures have been implemented?**
- **Determine current status as:**
  - Low: Not available
  - Medium: Operational
  - High: Optimal
- **Visualization by stoplight status**



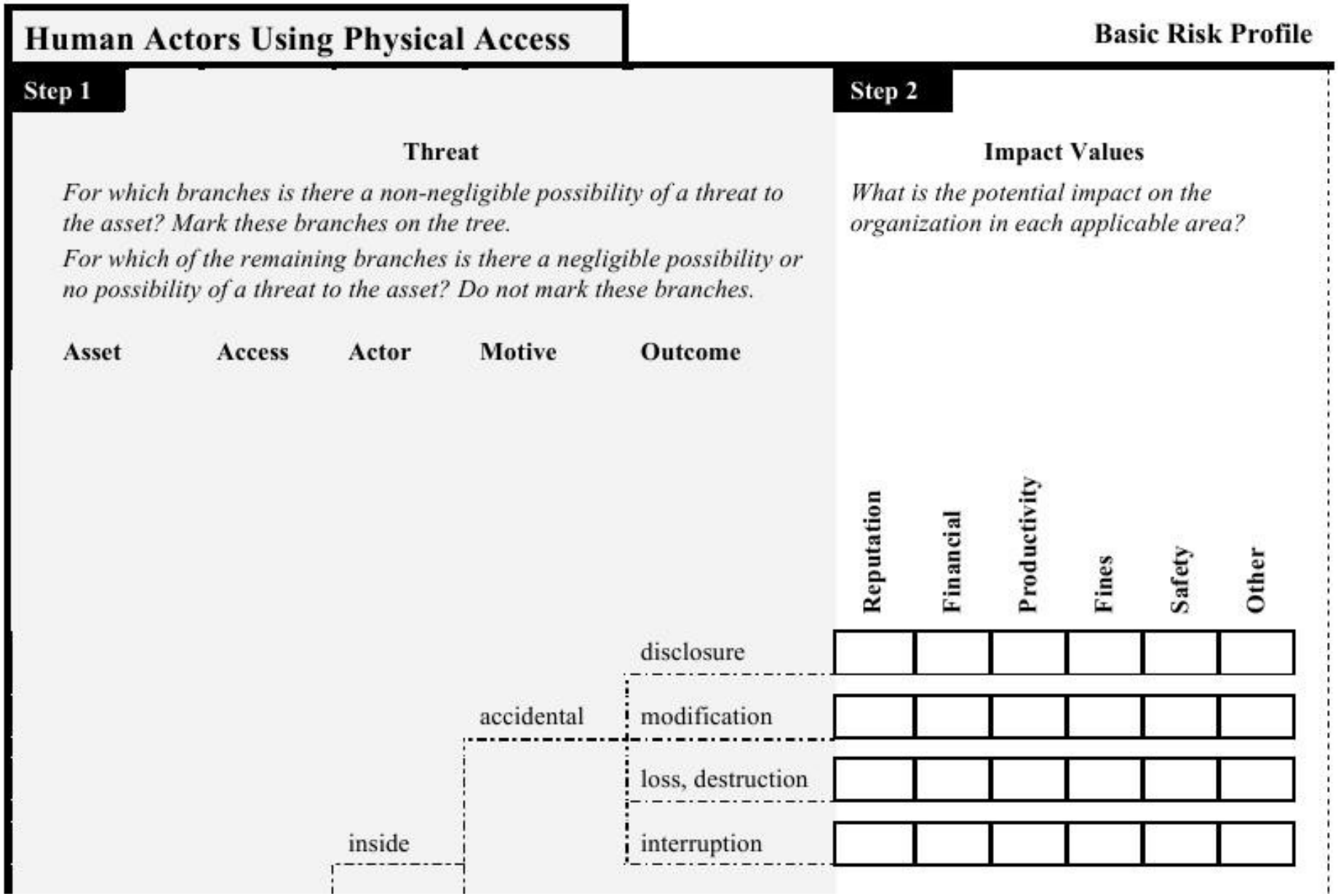
Phase 1 – S2 -Critical Assets

- **Focus on only a few assets**
- **What are the critical assets?**
  - There will be a large impact to the organization if
    - the asset is disclosed to unauthorized people
    - the asset is modified without authorization
    - the asset is lost or destroyed
    - access to the asset is interrupted

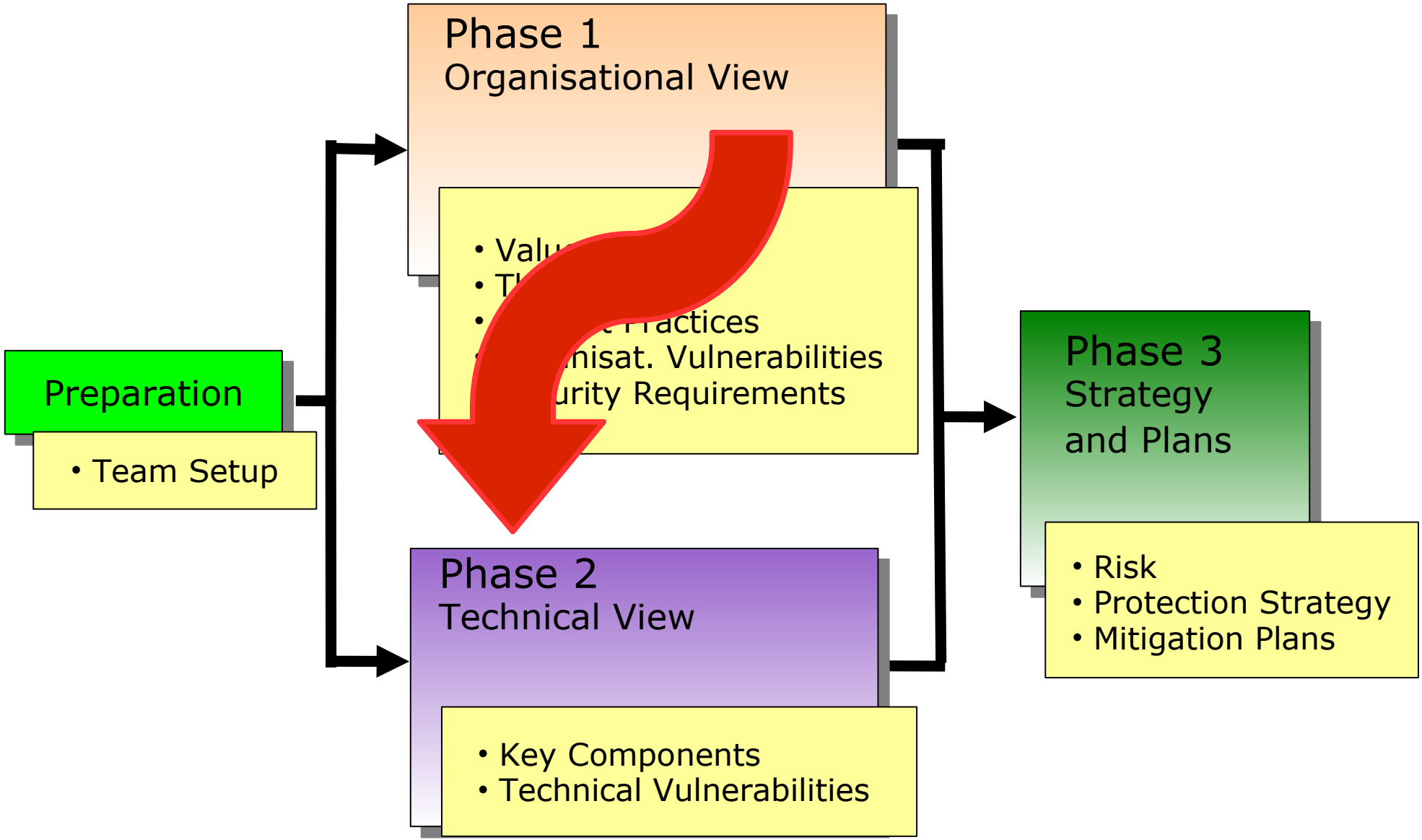
Phase 1 – S2 - Requirements

- **Determine security requirements ONLY for the selected critical assets:**
  - Who uses (depends on) these values?
  - Who is responsible?
  - Which other values are related to it?
  - What security requirements are defined?
    - Confidentiality
    - Integrity
    - Availability
    - Other

Phase 1 – Example



OCTAVE Phases



Phase 2 - Questions

- How do people access each critical asset?
- What infrastructure components are related to each critical asset?
- What are the key components of the computing infrastructure?
- What technological weaknesses expose your critical assets to threats?

Phase 2 - S3

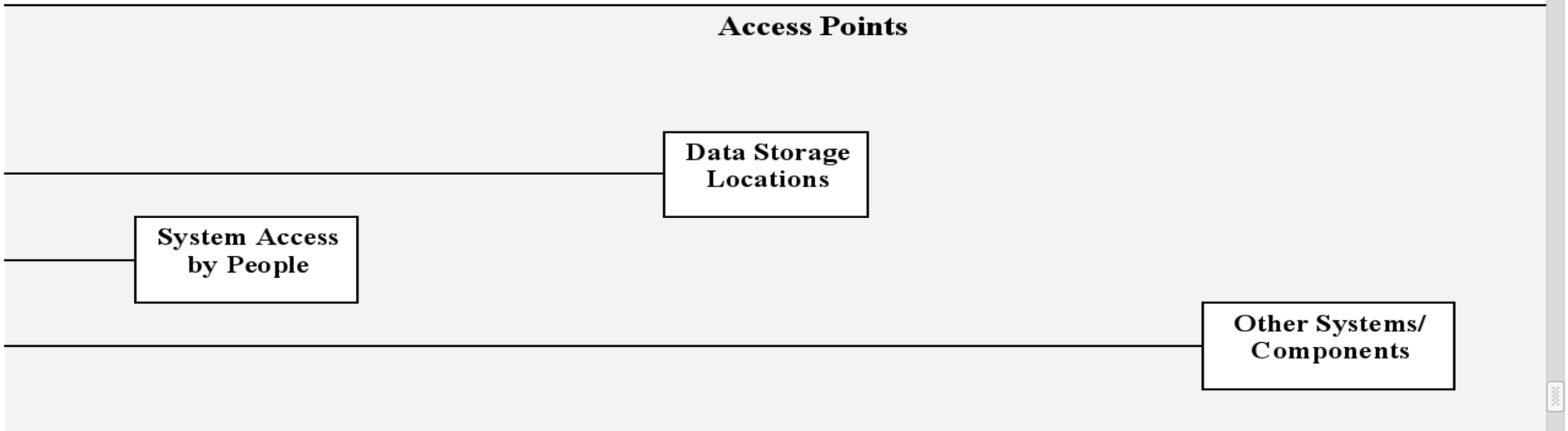
- **Identification of vulnerabilities within the IT infrastructure**
  - Identify network access paths to critical values
  - Identify (other) IT components which are related to the critical values
  - Identify any technical weaknesses related to
    - network access paths
    - IT components

Phase 2 - S3

- **Network access paths are:**
  - Gateways, Proxies
  - System access on user level
  - Access to memory or backups
  - Other components with access

Phase 2 – S3 - Example

Note: When you select a key class of components, make sure that you also document any relevant subclasses or specific examples when appropriate.



Step 18c

System Access by People

From which of the following classes of components can people (e.g., users, attackers) access the system of interest?

Consider access points both internal and external to your

Step 18d

Data Storage Locations

On which classes of components is information from the system of interest stored for backup purposes?

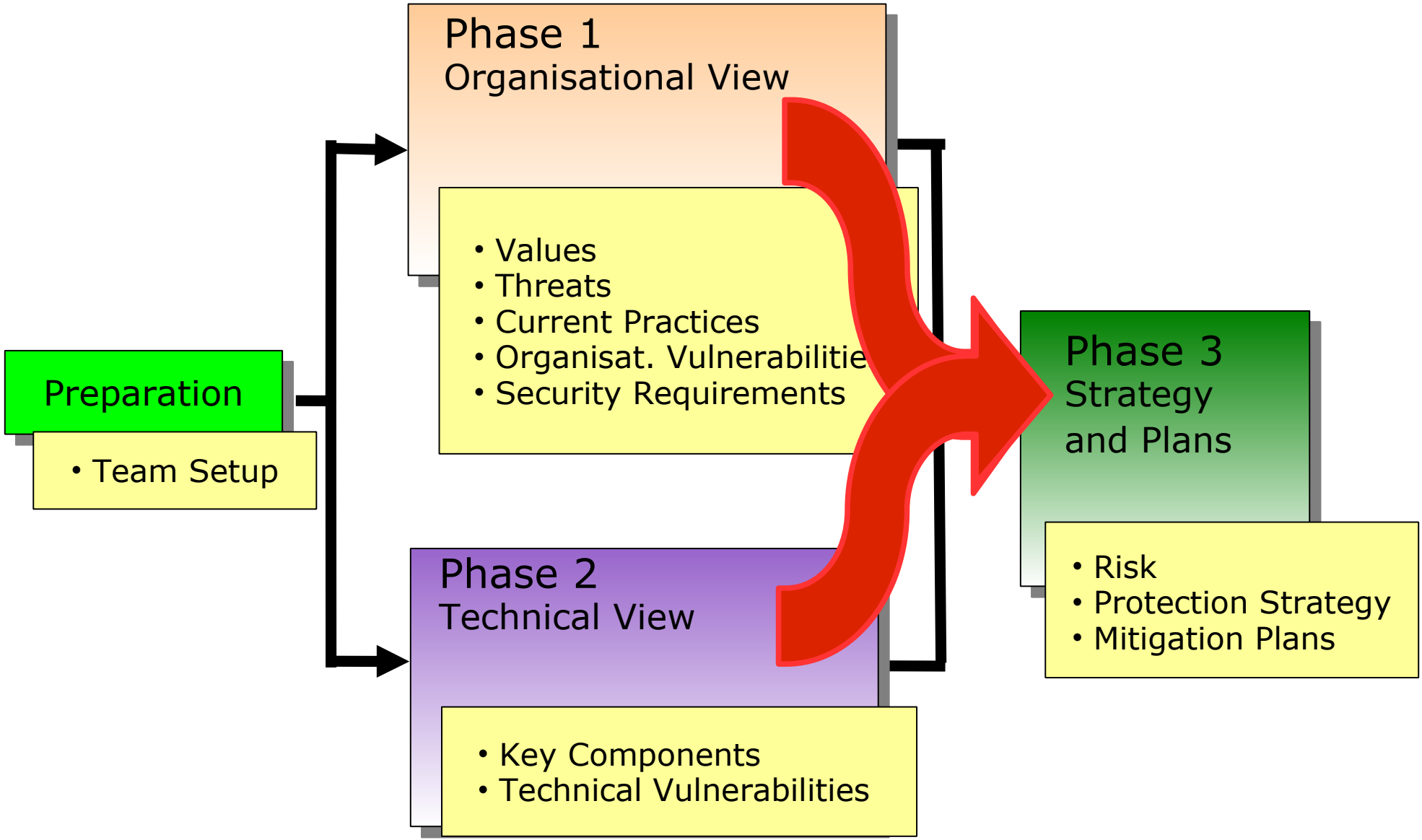
Step 18e

Other Systems and Components

Which other systems access information or applications from the system of interest?

Which other classes of componen can be used to access critical information or applications from

OCTAVE-Phases



Phase 3 - Questions

- What is the potential impact on your organization due to each risk?
- Which are the highest priority risks to your organization?
- What policies and practices does your organization need to adress?
- What actions have the highest priority?
- Which technological weaknesses need to be adressed immediately?

Phase 3 – S4 - S5

- **S4: Analyze Risks**
  - What happens if a threat really occurs?
  - Establish probability evaluation criteria
  - Evaluate probabilities of threats
- **S5: Develop protection strategy and mitigation plans**
  - What can be improved (existing measures)?
  - Develop risk mitigation plans
  - Identify changes to protection strategy
  - Next steps

Outcomes of Phase 3

- **Provides understanding of**
  - Critical values and interrelationship
  - Actual status quo
- **Provides forward looking information for**
  - Impact in case of an incident
  - Need for improvements and new measures
  - Understanding of critical needs (ad-hoc)
  - Setting up a continuous risk management

Phase 3 - Example

12. Vulnerability Management **Stoplight Status**

Third Party A:_____

Step 25: To what extent does your organization formally communicate its requirements in this area to this third party?

Step 29: Will any mitigation activities change how your organization communicates its requirements to this third party? Do you want to make any additional changes to how you communicate requirements to this third party?

Collaborative Issues	Step 25	Step 29
If staff from a third party is partly or completely responsible for this area:		
The organization's vulnerability management requirements are formally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are informally communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
The organization's vulnerability management requirements are not communicated to all contractors and service providers that manage technology vulnerabilities.	❑ Current	❑ Change
_____	❑ Current	❑ Change
_____		

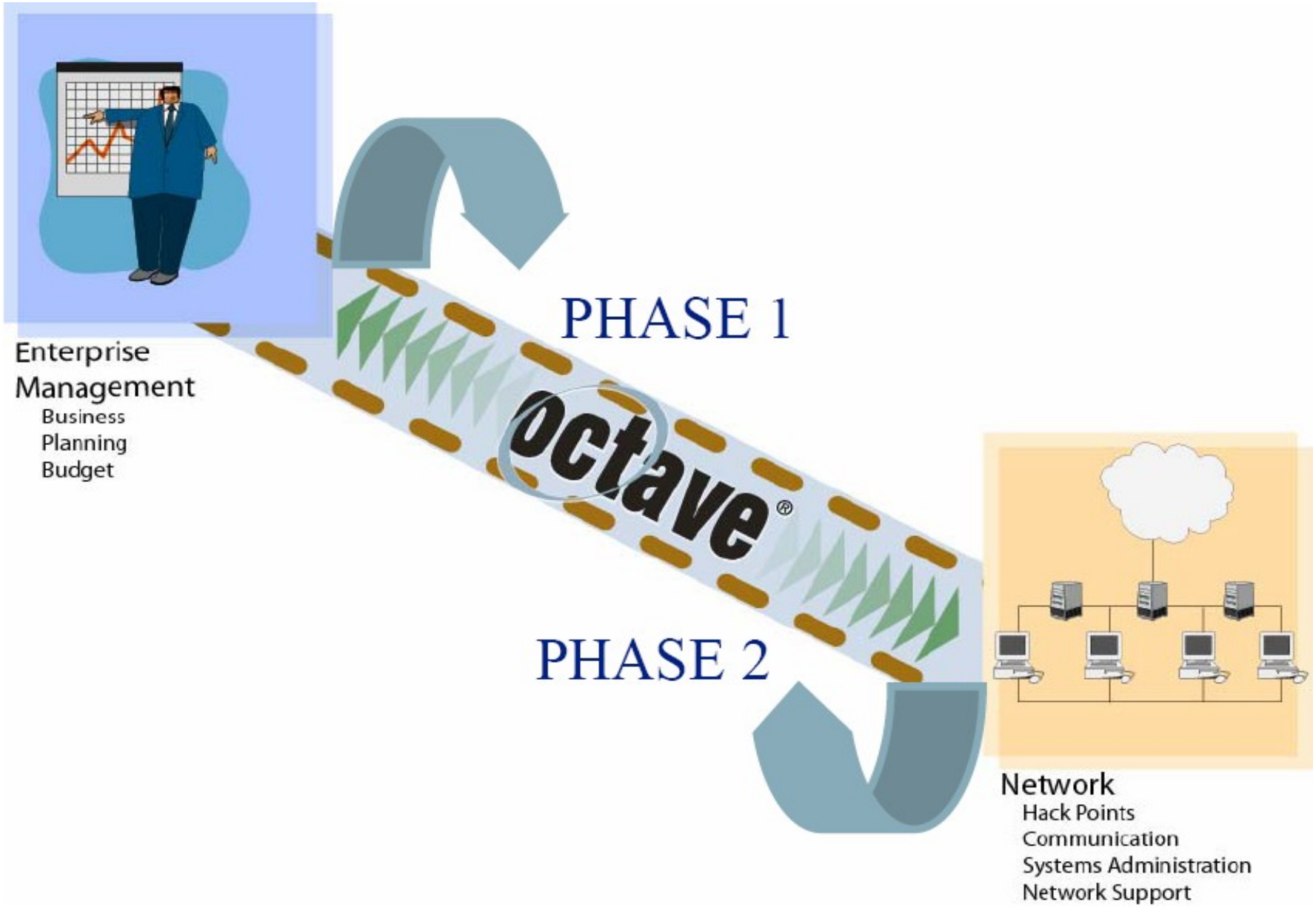
Agenda

- Introduction
- Why Risk Analysis?
- Existing methods
- The OCTAVE-Method
- Summary
- Discussion

Summary

- **Structured Model**
  - Flexible to adapt
  - Provides documentation
  - Involves all stakeholders
  - Extensive support
- **Provides basis for a continuous risk management**
  - Can be utilized to prepare for certifications

Adopting a Common Language



German Version

- Translated and shorted version of OCTAVE-S by DFN-CERT
- Pilot project currently running
- 10 participants
- Final version probably available in 2008
- Adopted to ISO27001
- Support by DFN-CERT (if neccessary)

Thank you for listening!

Questions?

Christian Paulsen
https://www.dfn-cert.de/
paulsen@dfn-cert.de