



# SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone Soderi



## M2.2 - Planning for Cybersecurity

# Contents

---

## 1. Security Governance

- Governance vs Management
- Principles and Outcomes
- Governance Components
- Approach
- Evaluation

## 2. Risk Assessment

- Concepts
- Asset, Threat, Control, and Vulnerability Identification
- Risk Assessment Approaches
- Likelihood and Impact Assessments
- Risk Determination
- Risk Treatment

## 3. Methods

- STRIDE (Threat Modelling)
- DREAD (Risk Classification)
- OCTAVE ( Risk Management)

## 4. Security Management

- Key aspects
- Planning



# Contents

---

## 3. Methods

- STRIDE (Threat Modelling)
- DREAD (Risk Classification)
- OCTAVE ( Risk Management)



# Threat Modelling (1/2)

WAYS TO FIND SECURITY ISSUES



**Threat Modelling:** a strategic process **aimed at considering possible attack scenarios and vulnerabilities** within a proposed or existing application environment **for the purpose of clearly identifying risk and impact levels**



## WHY THERAT MODELING

- **Think** and **find** security issue early
- **Understand** your security requirements better
- **Develop** and **delivery** better product

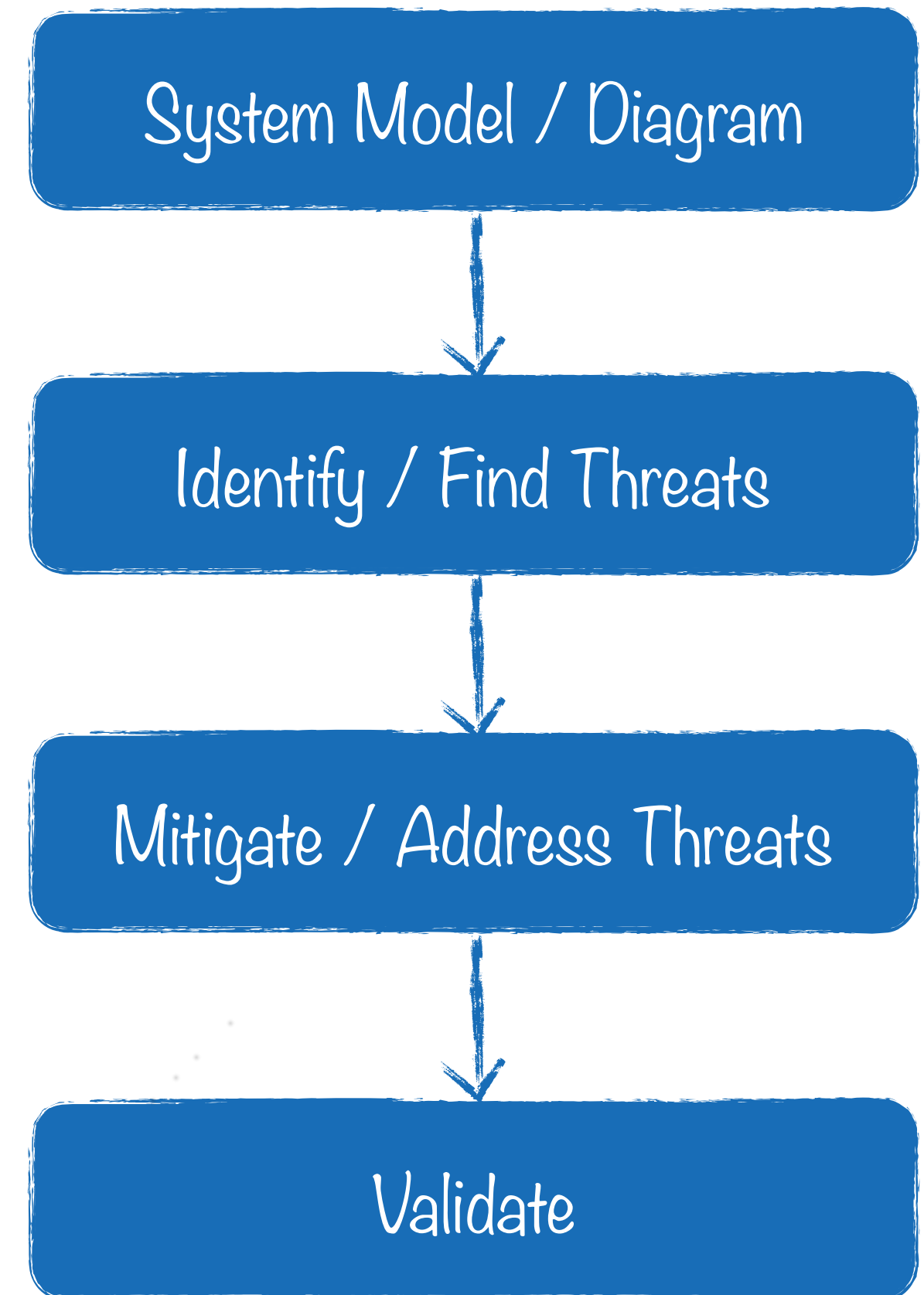
# Threat Modelling (2/2)

FOUR STEPS



A **FOUR STEP PROCESS**: questions we need to answer!

- What you are building?
- What can go wrong with it once it's built?
- What should you do about those things that can go wrong?
- Did you do a decent job of analysis?



# Create Diagrams

FIRST STEP



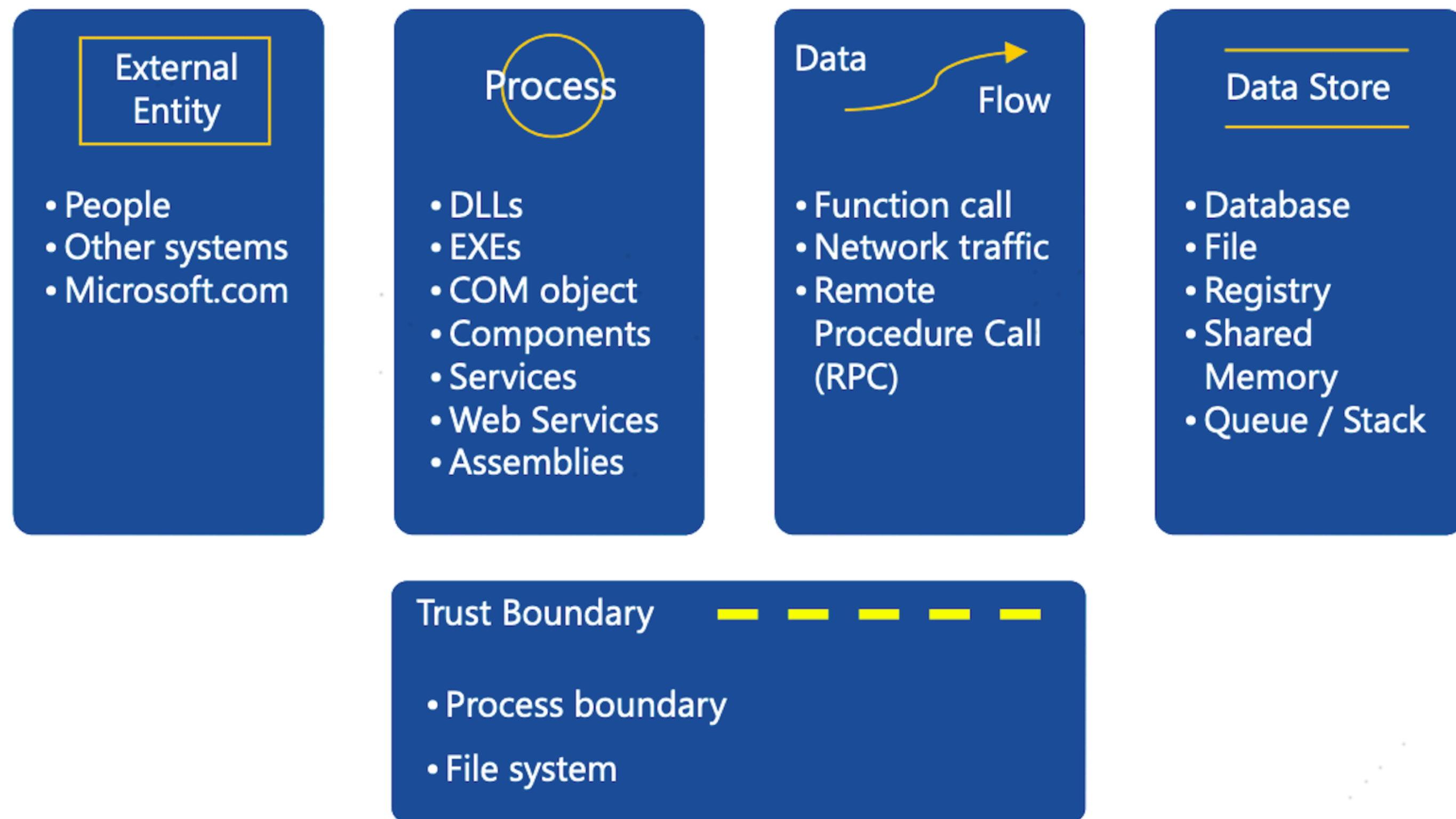
## HOW TO CREATE DIAGRAMS:

- Go to the **whiteboard**
- Start with an **overview** which has:
  - ▶ A few external interactions
  - ▶ One or two processes
  - ▶ One or two data stores (maybe)
  - ▶ Data flows to connect them
- Identification of **the trust boundaries**
  - ▶ Can you tell a story without edits?
  - ▶ Does it match reality?
- Use **Data Flow Diagrams** (DFDs)
  - ▶ Include processes, data stores, data flows
  - ▶ Include trust boundaries
  - ▶ Diagrams per scenario may be helpful



# Diagram Elements

EXAMPLE



These threats will be graphically represented in the [Microsoft Threat Modeling Tool](#) and in the diagrams used for visualization and investigation.  
Useful for STRIDE Threat Modelling tool.

# STRIDE Threat Model

THREAT CLASSIFICATION SYSTEM DEVELOPED BY MICROSOFT

**STRIDE** is a threat classification system **developed by Microsoft** that is a useful way of **categorizing attacks** that **arise from deliberate actions**

## Spoofing identity

- **Illegally accessing** and then **using another user's authentication information**, such as username and password
- *Security controls to counter such threats are in the area of **authentication***

## Tampering with data

- Involves the **malicious modification of data** and unauthorised changes
- *Relevant security controls are in the area of **integrity***

## Repudiation

- **Deny performing a malicious action.**
- *Relevant security controls are in the **area of non-repudiation (users who deny performing an action)***

## Information disclosure

- Threats that involve the **exposure of information to individuals who are not supposed to have access to it**
- *Relevant security controls are in the area of **confidentiality***

## Denial of service (DoS)

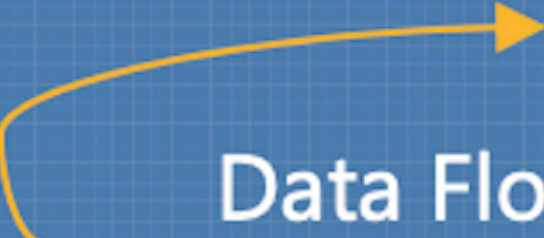
- Attacks that **deny service to valid users**
- *Relevant security controls are in the area of **availability***

## Elevation of privilege

- An **unprivileged user gains privileged access** and thereby has sufficient access to compromise or destroy the entire system; an attacker has effectively penetrated all system defenses and become part of the trusted system itself
- *Relevant security controls are in the area of **authorization***



# Different Threats Affect Each Element Type

| ELEMENT   | S | T | R | I | D | E |
|---|---|---|---|---|---|---|
| <br>External Entity | ✓ |   | ✓ |   |   |   |
| <br>Process         | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| <br>Data Store    |   | ✓ | ? | ✓ | ✓ |   |
| <br>Data Flow     |   | ✓ |   | ✓ | ✓ |   |

# Threats Evaluation with DREAD (1/3)

DREAD THREAT CLASSIFICATION



Evaluation of the threats that will be subject to security analysis.



## **DREAD:**

- **D**amage Potential
- **R**eproducibility
- **E**xploitability
- **A**ffected users
- **D**iscoverability



The evaluation of the threats can be carried out through the application of the **DREAD methodology**, which foresees the **evaluation of the threats through a rating defined on ten levels** and applied **to five risk categories**.

The levels are grouped into **three categories**, corresponding respectively to a **High** (8-10), **Medium** (4-8), and **Low** (0-4) risk level.

**Qualitative** risk assessment!



# Threats Evaluation with DREAD (2/2)

## DREAD THREAT CLASSIFICATION

| RATING VALUES    |  |   |  |
|------------------|--|---|--|
|                  | High = 3   | Medium = 2  | Low = 1  |
| Damage potential | It is able to subvert all security controls and gain full confidence in taking control of the ecosystem. | Possible leakage of sensitive information.  | Possible leakage of low-sensitive information.   |
| Reproducibility  | The attack is always reproducible.   | The attack can only be replayed within a timed window or specific condition.  | It is very difficult to reproduce the attack, even with a specific set of vulnerability information. |
| Exploitability   | A malicious user can execute the exploit.  | A skilled attacker could execute the attack repeatedly.   | Allows a skilled attacker with in-depth knowledge to execute the attack.                             |
| Affected users   | All users, default configurations, all devices.  | It affects some users, some devices, and custom configurations.   | It affects a small percentage of users and/or devices through a specific feature.                    |
| Discoverability  | An explanation of the attack can easily be found in a publication.                                       | Influence on a rarely used feature where a malicious user would have to be very creative to discover malicious use. | It is unlikely that an attacker would discover a way to exploit the error.                           |

# Threats Evaluation with DREAD (3/3)

EXAMPLE

|  | D | R | E | A | D | TOTAL | RATING |
|--|---|---|---|---|---|-------|--------|
| Attacker obtain authentication credentials by monitoring the network | 3 | 3 | 2 | 2 | 2 | 12    | HIGH   |
| SQL commands injection   | 3 | 3 | 3 | 3 | 2 | 14    | HIGH   |

**Risk Rating:**

- HIGH = 12-15
- MEDIUM = 8-11
- LOW = 5-7

# Mitigate/Address Threats

THIRD STEP



## MITIGATION IS THE POINT OF THREAT MODELLING

- **Address each threat**
- **Four ways to address threats**
  - ▶ **Redesign** to eliminate
  - ▶ **Apply standard** mitigations
  - ▶ What have **similar software** packages done and **how has that worked out** for them?
  - ▶ **Invent new mitigations** (riskier)
- **Accept vulnerability** in design
- **Address each threat**





# Standard Mitigation

APPLY WITH STRIDE

|                                |                 |   |
|--------------------------------|-----------------|---|
| <b>S</b> poofing               | Authentication  | <p>To authenticate principals:</p> <ul style="list-style-type: none"><li>● Cookie authentication</li><li>● Kerberos authentication</li><li>● PKI systems such as SSL/TLS and certificates</li></ul> <p>To authenticate code or data:</p> <ul style="list-style-type: none"><li>● Digital signatures</li></ul> |
| <b>T</b> ampering              | Integrity       | <ul style="list-style-type: none"><li>● Windows Vista Mandatory Integrity Controls</li><li>● Access Control Lists (ACLs)</li><li>● Digital signatures</li></ul>   |
| <b>R</b> epudiation            | Non Repudiation | <ul style="list-style-type: none"><li>● Secure logging and auditing</li><li>● Digital Signatures</li></ul>  |
| <b>I</b> nfomantion Disclosure | Confidentiality | <ul style="list-style-type: none"><li>● Encryption</li><li>● ACLs</li></ul>   |
| <b>D</b> enial of Serice       | Availability    | <ul style="list-style-type: none"><li>● ACLs</li><li>● Filtering</li><li>● Quotas</li></ul>   |
| <b>E</b> levation of Privilege | Authorization   | <ul style="list-style-type: none"><li>● ACLs</li><li>● Group or role membership</li><li>● Privilege ownership</li><li>● Input validation</li></ul>  |

# Validate the Threat Model

FOURTH STEP



## Checking the model:

- Completeness
- Accurateness
- Coverage of all the security decisions
- Enumerate threats
- Is each threat mitigated?



## Updating the diagram

- Focus con data flow rather than control flow
- Update periodically your model
- Change vague arguments that might create unclear requirements

# OCTAVE Risk Management

SINGLE SOURCE APPROACH



**OCTAVE (Operationally, Critical, Threat, Asset, and Vulnerability Evaluation)** is an approach to **identify, assess, and manage risks to IT assets**.



This process identifies the **critical components** of information security and the **threats** that could affect their confidentiality, integrity, and availability.



This **helps** them understand **what information is at risk and design a protection strategy to reduce or eliminate** the risks to IT assets.



**Defines** the essential components of a comprehensive, systematic, **context-driven, self-directed information security risk evaluation**

# OCTAVE Methods

SINGLE SOURCE APPROACH



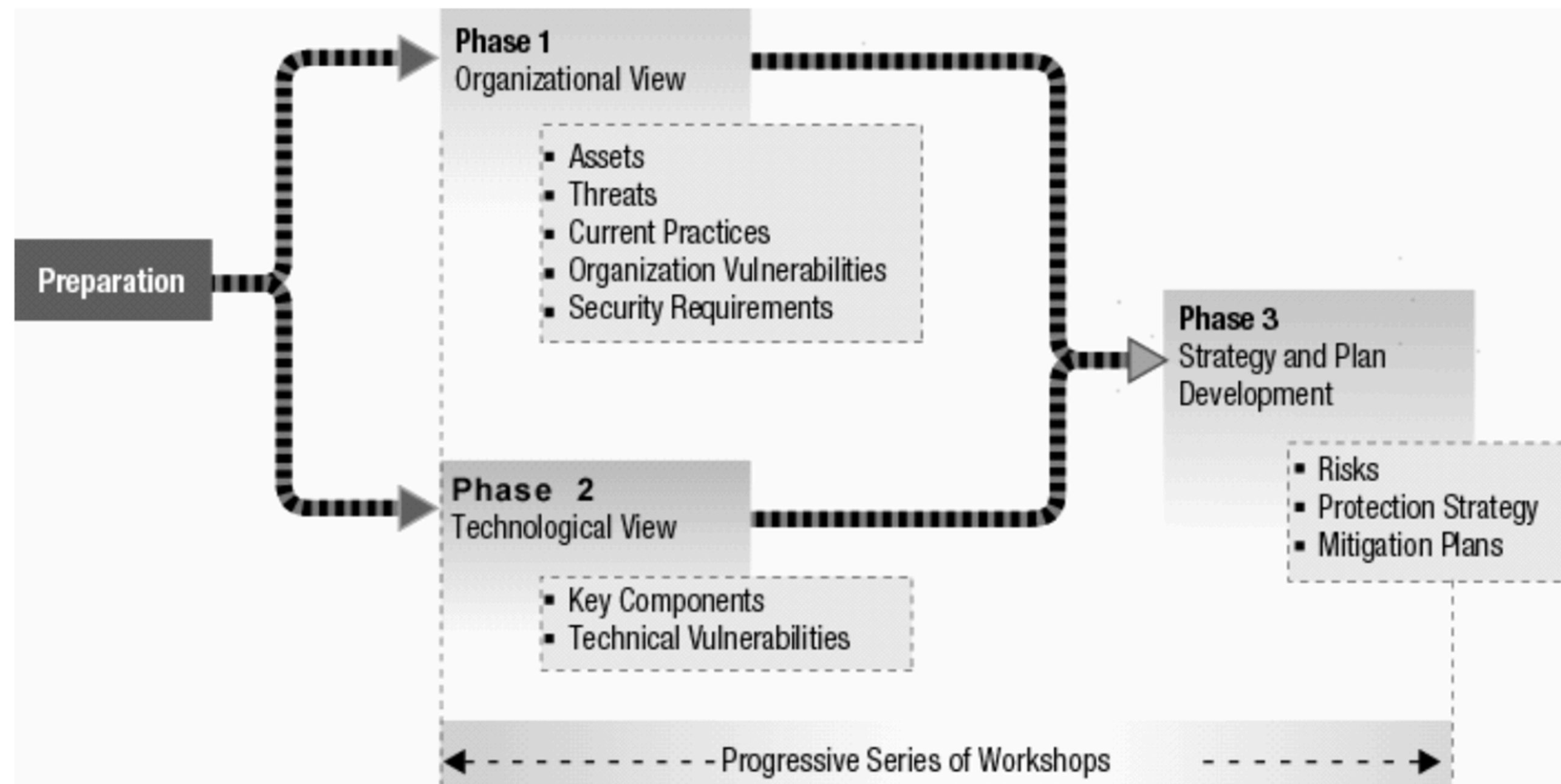
## Three variations of the OCTAVE method:

1. The **original OCTAVE method**, (forms the basis for the OCTAVE body of knowledge)
  - ▶ Was designed for larger organizations with **300 or more users**
  - ▶ The method was also designed to allow for tailoring by organizations adopting it
  - ▶ It was created by the CERT Division of the SEI in 2003 and refined in 2005.
2. **OCTAVE-S**
  - ▶ For smaller organizations of about **100 users or less**
3. **OCTAVE-Allegro**
  - ▶ A streamlined approach for information security assessment and assurance



# OCTAVE Original Method

3 PHASES



The method is performed in a **series of workshops** conducted and facilitated by an **interdisciplinary analysis team** drawn from business units throughout the organization

- Phase 1:** the analysis team identifies **important information-related assets** and the current protection strategy for those assets. The team then determines which of the identified assets are most critical to the organization's success, documents their security requirements, and **identifies threats that can interfere** with meeting those requirements.
- Phase 2:** the analysis team performs an **evaluation of the information infrastructure to integrate the threat analysis performed in phase 1** and to **inform mitigation decisions** in phase 3.
- Phase 3:** the analysis team performs **risk identification** activities and develops a **risk mitigation** plan for the critical assets



# OCTAVE-S

FOR SMALL ORGANIZATION



OCTAVE-S is **consistent** with the OCTAVE criteria. The OCTAVE-S approach consists of **three similar phases**.

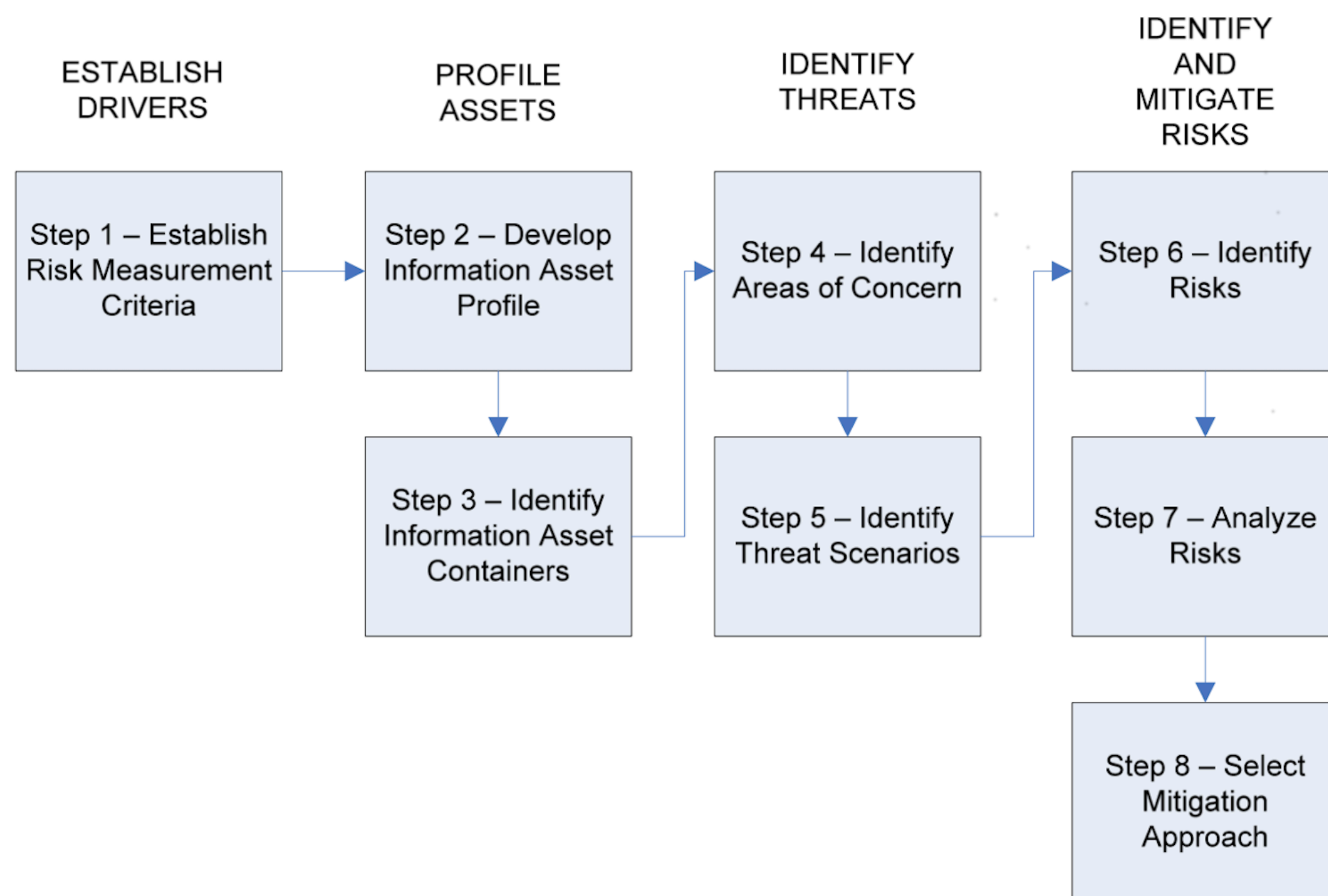


However, **OCTAVE-S is performed by an analysis team that has extensive knowledge of the organization**.

Thus, OCTAVE-S does not rely **on formal knowledge conducting workshops** to gather information because it **is assumed that the analysis team** (typically consisting of three to five people) **has working knowledge** of the important information-related **assets**, security requirements, **threats**, and security **practices** of the organization.

# OCTAVE Allegro

FOR SMALL ORGANIZATION



Octave Allegro roadmap

- This approach **differs from previous OCTAVE approaches** by **focusing** primarily on information **assets** in the context of **how they are used, where they are stored, transported, and processed**, and **how they are exposed** to threats, vulnerabilities, and disruptions as a result.
- Allegro can be performed in a **workshop-style**, collaborative setting and is supported with guidance, worksheets, and **questionnaires**, which are included in the appendices of this document.
- However, OCTAVE Allegro is also well suited for use by individuals who want to perform risk assessment **without extensive organizational involvement, expertise, or input**.

# Contents

---

## 4. Security Management

- Key aspects
- Planning



# The Security Management Function



The **security management function** entails establishing, implementing, and monitoring an information security program, **under the direction of a senior responsible person**



**Security management involves multiple levels of management** and should be complementary so that each can help the others be more effective



**Security Governance defines two individual roles:**

- **Chief Information Security Officer (CISO)**

- ▶ Has overall **responsibility** for the enterprise information security program
- ▶ Is the **relation between** executive management and the information security program
- ▶ Should **communicate and coordinate** closely with key business **stakeholders** to address information protection needs

- **Information Security Manager (ISM)**

- ▶ Has **responsibility** for the management of information security efforts

# What are the main tasks for the CISO? (1/2)

SUMMARY OF THE TASKS THAT COMPRISE INFORMATION SECURITY MANAGEMENT



**NISTIR 7359** “*Information Security Guide for Government Executives*”, provides a useful summary of the tasks that comprise information security management



## Key security program areas include:

### ● Security planning

- ▶ A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

### ● Capital planning:

- ▶ A decision-making process for ensuring that IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of an organization's missions and business needs.

### ● Awareness and training

- ▶ *(People management during next classes)*

### ● Information security governance

- ▶ *(discussed during previous classes)*

### ● System development life cycle



# What are the main tasks for the CISO? (2/2)

SUMMARY OF THE TASKS THAT COMPRISE INFORMATION SECURITY MANAGEMENT



## Key security program areas include [CONTINUE]:

### ● Security products and services acquisition

### ● Risk management:

▶ *(discussed during previous classes)*

### ● Configuration management

▶ The process of controlling modifications to a system's hardware, software, and documentation

### ● Incident response

▶ Incident response, which occurs after the detection of a security event, seeks to minimize the damage of the event and facilitate rapid recovery.

### ● Contingency planning

▶ Information system contingency planning involves management policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

### ● Performance measures

▶ The CISO should ensure that an organization wide performance measures are defined and used.

# CISO: Monitoring the Security Policies

REMEMBER!



The **CISO** should **designate** an individual or a group responsible for monitoring the implementation of the security policy



The **responsible entity (individual or group)** should **periodically review policies** and make any changes needed to reflect changes in the organization's environment, asset suite, or business procedures



A violation reporting mechanism is needed to encourage employees to report

# Security Planning (1/2)



**NIST SP 800-18** “*Guide for Developing Security Plans for Federal Information Systems*”, indicates that the **purpose of a system security plan is to provide** an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements



The **system security plan also delineates responsibilities and expected behaviour** of all individuals who access the system



The system **security plan is basically documentation of the structured process of planning adequate, cost-effective security protection for a system**

# Security Planning (2/2)



**NIST SP 800-18** recommends that **each information system** in an organization have a **separate plan document** with the following elements:

- Information system **name/identifier**
- Information system **owner**
- **Authorizing** individual
- Assignment of security **responsibility**
- Security **categorization**
- Information system operational status
- Information system type

- **Description**/purpose
- System **environment**
- System interconnections/information sharing
- **Related laws/regulations/policies**
- **Existing** security controls
- **Planned** security controls
- Information system security plan **completion date**
- Information system security plan **approval date**

# CISO Oversees all Security Projects

REMEMBER!



**The security planning enables the CISO to oversee all security projects** throughout the organization. The CISO should also coordinate a process for developing and approving these plans.



This process **involves three steps**, each of which has **goals, objectives**, implementing activities, **and output products** for formal inclusion in agency enterprise architecture and capital planning processes:

1. **Identify:** Encompasses the **research and documentation activities** necessary to identify security and privacy requirements in support of the mission objectives so that they can be incorporated into the enterprise architecture.
2. **Analyze:** Involves an **analysis** of organization security and privacy **requirements** and the **existing or planned capabilities** that support security and privacy.
3. **Select:** Involves an enterprise evaluation of the **solutions proposed** in the preceding phase and the selection of major investments.



# Information Security Costs

| Direct Costs  | Products, procedures, and personnel that have an incidental or integral component and/or a quantifiable benefit for the specific IT investment  | Allocated security control costs for networks that provide some or all necessary security controls for associated applications   |
|---|---|--|
| <ul style="list-style-type: none"> <li>•Risk assessment</li> <li>•Security planning and policy</li> <li>•Certification and accreditation</li> <li>•Specific security controls</li> <li>•Authentication or cryptographic applications</li> <li>•Education, awareness, and training</li> <li>•System reviews/evaluations</li> <li>•Oversight or compliance inspections</li> <li>•Development or maintenance of security reports</li> <li>•Contingency planning and testing</li> <li>•Physical and environmental controls for hardware and software</li> <li>•Auditing and monitoring</li> <li>•Computer security investigations and forensics</li> <li>•Reviews, inspections, audits, and other evaluations performed on contractor facilities and operations</li> <li>•Privacy impact assessments</li> </ul> | <ul style="list-style-type: none"> <li>•Configuration or change management control</li> <li>•Personnel security</li> <li>•Physical security</li> <li>•Operations security</li> <li>•Privacy training</li> <li>•Program/system evaluations</li> <li>•System administrator functions</li> <li>•System upgrades with new features that obviate the need for other stand-alone security controls</li> </ul> | <ul style="list-style-type: none"> <li>•Firewalls</li> <li>•Intrusion detection/prevention systems</li> <li>•Forensic capabilities</li> <li>•Authentication capabilities</li> <li>•Additional ‘add-on’ security considerations.</li> </ul> |

Apply security in the organization has a **cost**.

**The costs typically** incurred or contemplated are usually **in three categories**



# SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**



[simone.soderi@unipd.it](mailto:simone.soderi@unipd.it)



## M2.2 - Planning for Cybersecurity

*Thanks for your attention!*