6. Risk Management

Introduction

- Information security departments are created primarily to manage IT risk
- Managing risk is one of the key responsibilities of every manager within the organization
- Risk management processes:
  1. Risk identification and assessment
  2. Risk control

Knowing Our Environment

- Identify, Examine and Understand
  - information and how it is processed, stored, and transmitted
- Initiate an in-depth risk management program
- Risk management is a process which means
  - safeguards and controls that are devised and implemented are not install-and-forget devices

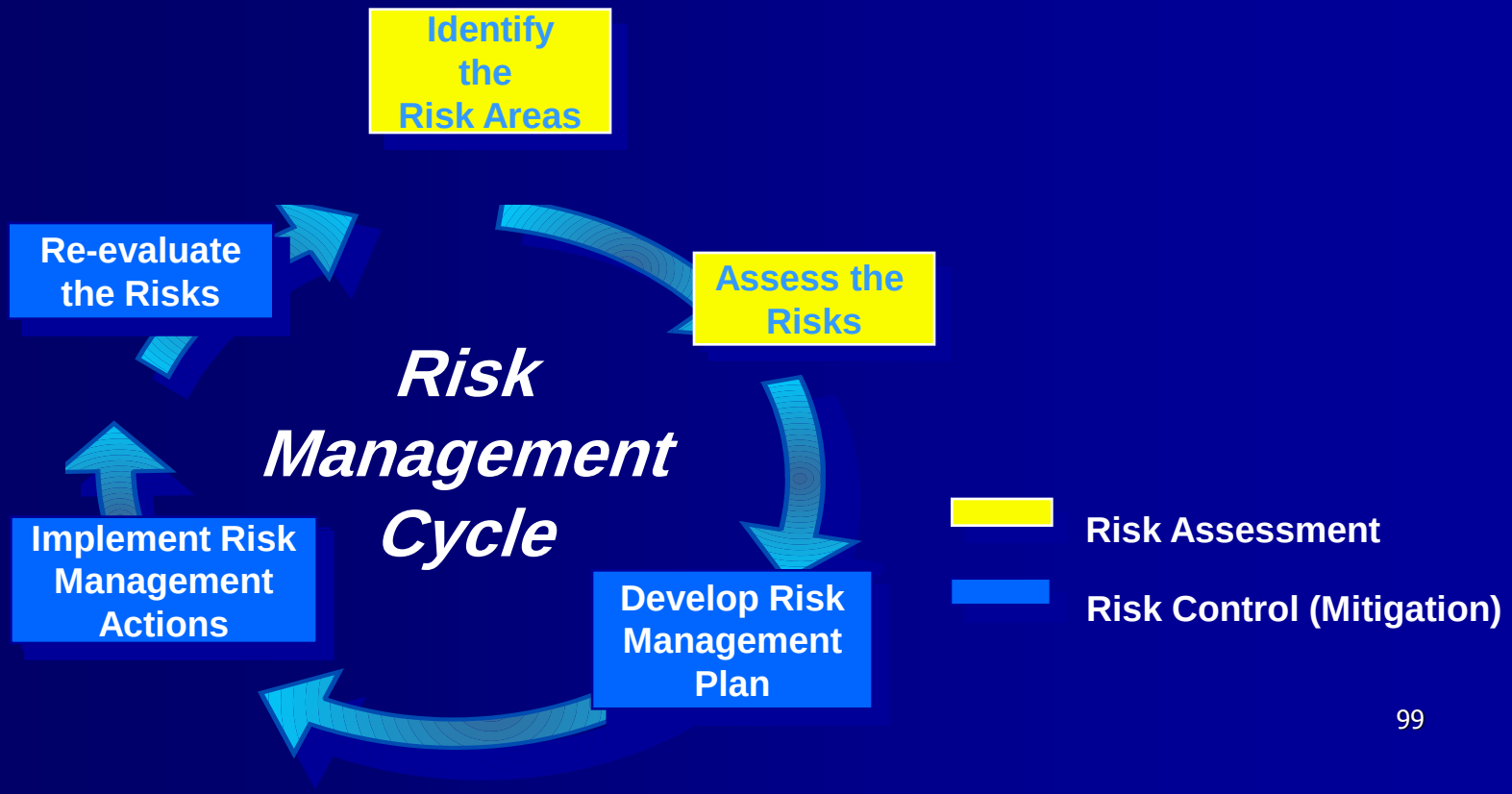
Knowing the Enemy

- Identify, examine, and understand
  - *the threats*
- Managers must identify threats that pose risks to the organization and the security of its information assets

- Risk management is the process of:
  - **Assessing** the risks to an organization's information, and
  - **Determining** how those risks can be controlled or mitigated

Risk Management

"The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected" (NIST)



Risk Identification

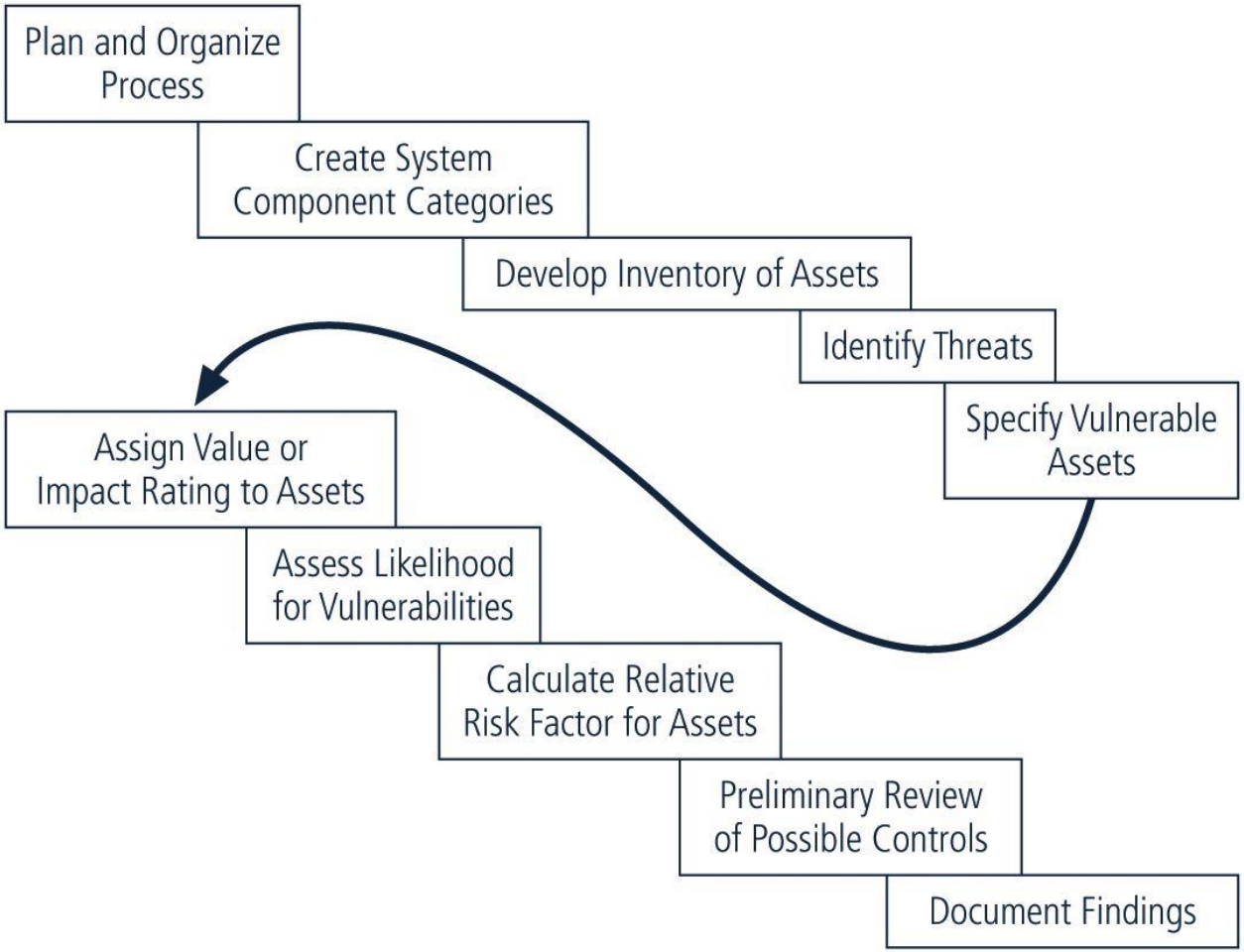


FIGURE 7-1 Risk Identification Process

Risk Identification

- Risk identification
  - begins with the process of self-examination

- Managers
  - identify the organization's information assets,
  - classify them into useful groups, and
  - prioritize them by their overall importance

Assessing Values for Information Assets

- Assign a relative value
  - to ensure that the most valuable information assets are given the highest priority, for example:
    - Which is the most critical to the success of the organization?
    - Which generates the most revenue?
    - Which generates the highest profitability?
    - Which is the most expensive to replace?
    - Which is the most expensive to protect?
    - Whose loss or compromise would be the most embarrassing or cause the greatest liability?
- Final step in the RI process is to list the assets in order of importance
  - Can use a weighted factor analysis worksheet

Identify And Prioritize Threats and Threat Agents

- Each threat presents a unique challenge
  - Must be handled with specific controls that directly address particular threat and threat agent's attack strategy
- Threat assessment
  - each threat must be examined to determine its potential to affect targeted information asset

Vulnerability Assessment

- Steps revisited
  - Identify the information assets of the organization and
  - Document some threat assessment criteria,
  - Begin to review every information asset for each threat
    - Leads to creation of list of vulnerabilities that remain potential risks to organization
- Vulnerabilities
  - specific avenues that threat agents can exploit to attack an information asset
- At the end of the risk identification process,
  - a list of assets and their vulnerabilities has been developed

Risk Assessment

Risk is

The likelihood of the occurrence of a vulnerability

Multiplied by

The value of the information asset

Minus

The percentage of risk mitigated by current controls

Plus

The uncertainty of current knowledge of the vulnerability

Likelihood

- Likelihood
  - of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event
  - is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited

- Using the information documented during the risk identification process,
  - assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc

Assessing Potential Loss

- To be effective, the likelihood values must be assigned by asking:
  - Which threats present a danger to this organization's assets in the given environment?
  - Which threats represent the most danger to the organization's information?
  - How much would it cost to recover from a successful attack?
  - Which threats would require the greatest expenditure to prevent?
  - Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

Mitigated Risk / Uncertainty

- If it is partially controlled,
  - Estimate what percentage of the vulnerability has been controlled
- Uncertainty
  - is an estimate made by the manager using judgment and experience
  - It is not possible to know everything about every vulnerability
  - The degree to which a current control can reduce risk is also subject to estimation error

Risk Determination Example

- Asset A has a value of 50 and has vulnerability #1,
  - likelihood of 1.0 with no current controls
  - assumptions and data are 90% accurate

- Asset B has a value of 100 and has two vulnerabilities
  - Vulnerability #2
    - likelihood of 0.5 with a current control that addresses 50% of its risk
  - Vulnerability # 3
    - likelihood of 0.1 with no current controls

  - assumptions and data are 80% accurate

Risk Determination Example

- Resulting ranked list of risk ratings for the three vulnerabilities is as follows:
  - Asset A: Vulnerability 1 rated as 55 =
    - (50 × 1.0) – 0% + 10%
  - Asset B: Vulnerability 2 rated as 35 =
    - (100 × 0.5) – 50% + 20%
  - Asset B: Vulnerability 3 rated as 12 =
    - (100 × 0.1) – 0 % + 20%

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas

- Three general categories of controls exist:
  - Policies
  - Programs
  - Technical controls

Documenting the Results of Risk Assessment

- The goal of the risk management process:
  - Identify information assets and their vulnerabilities
  - Rank them according to the need for protection

- In preparing this list, collect
  - wealth of factual information about the assets and the threats they face
  - information about the controls that are already in place

- The final summarized document is the ranked vulnerability risk worksheet

Risk Control Strategies

- Choose basic control risks strategy :
  - **Avoidance:**
    - applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability
  - **Transference:**
    - shifting the risk to other areas or to outside entities
  - **Mitigation:**
    - reducing the impact should the vulnerability be exploited
  - **Acceptance:**
    - understanding the consequences and accept the risk without control or mitigation

Risk Handling Action Points

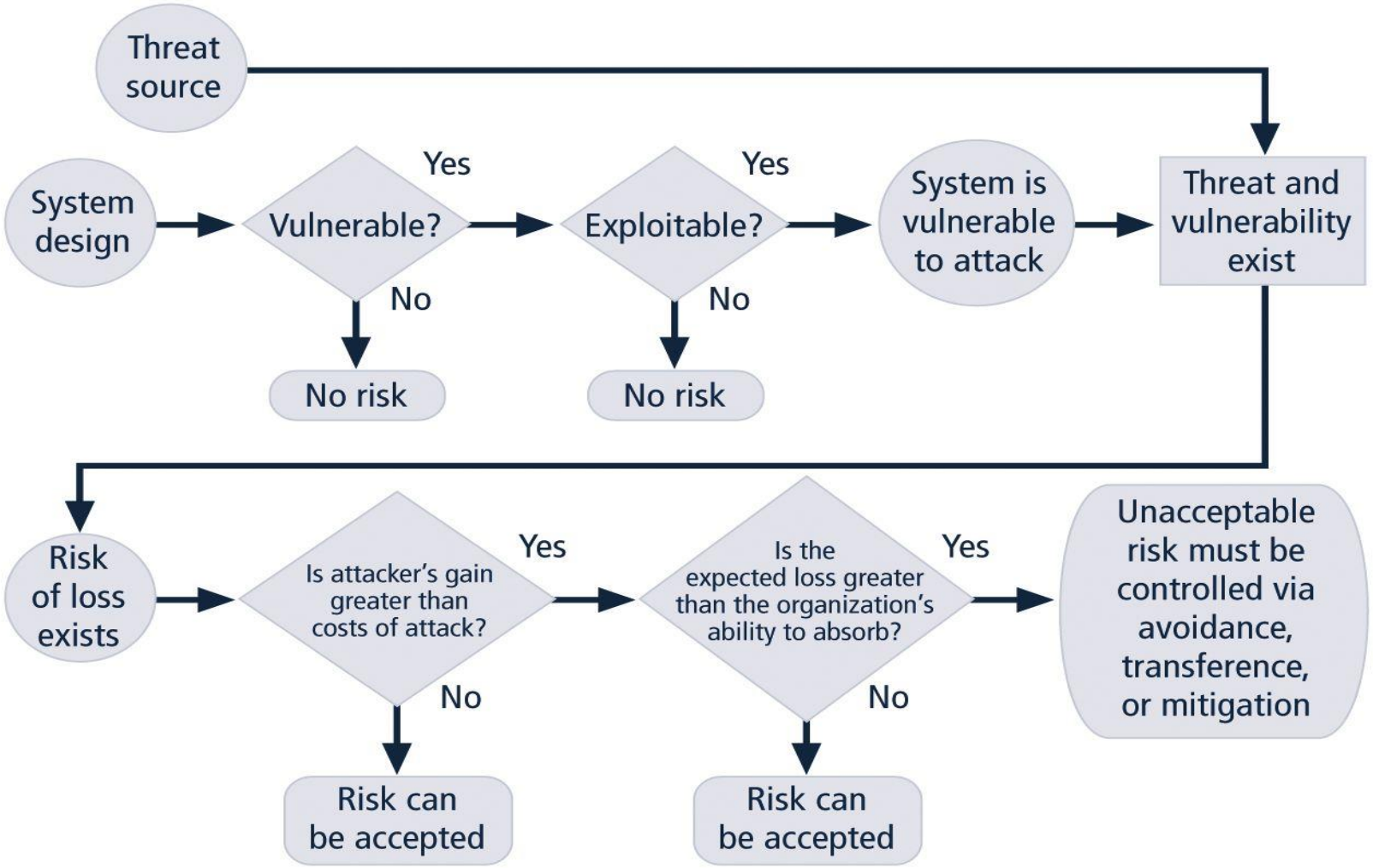


FIGURE 8-2 Risk-Handling Action Points

The Risk Control Cycle

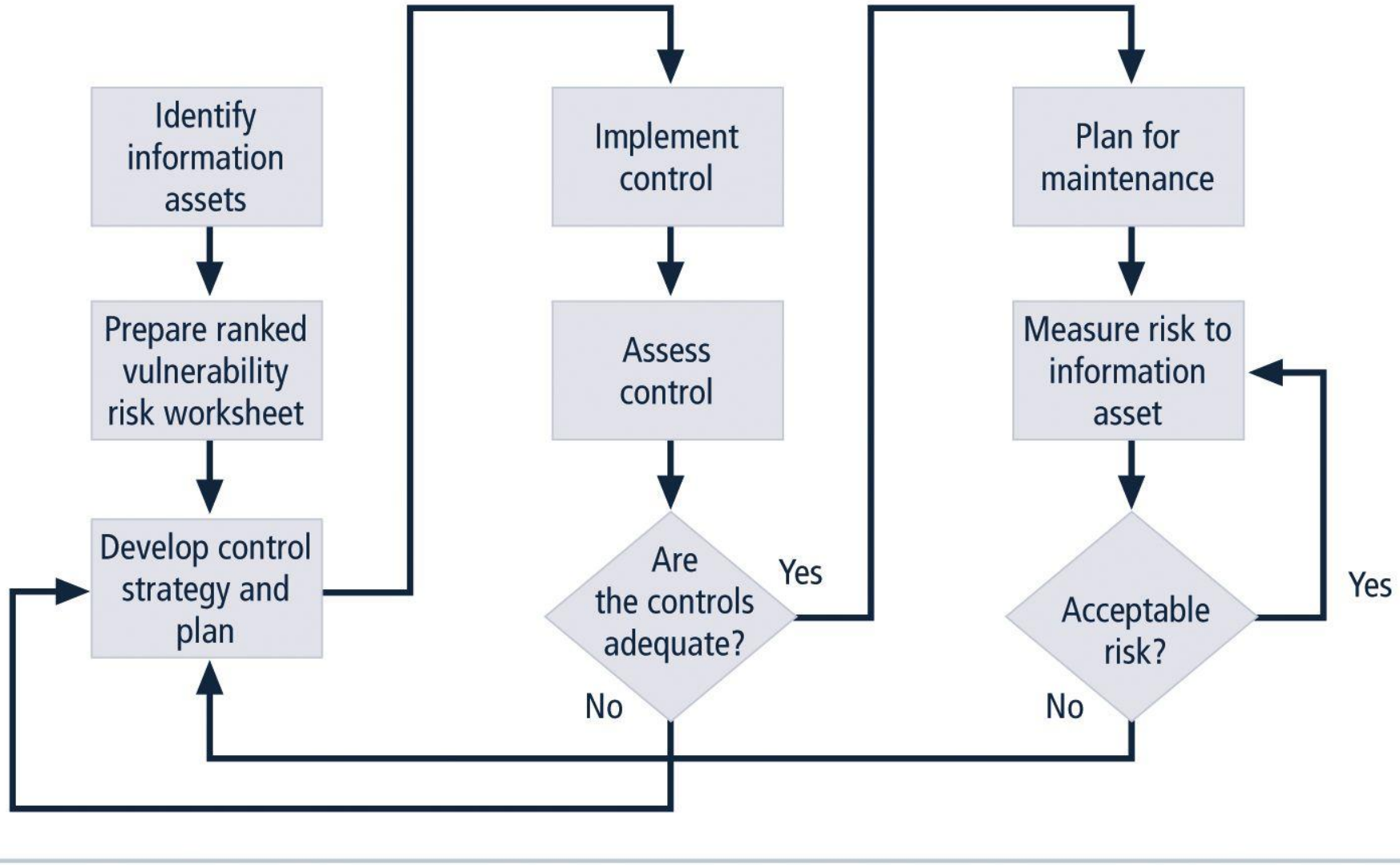


FIGURE 8-3 Risk Control Cycle

Documenting Results

- When risk management program has been completed,
  - Series of proposed controls are prepared
  - Each justified by one or more feasibility or rationalization approaches

- At minimum, each information asset-threat pair should have a documented control strategy that
  - Clearly identifies any residual risk remaining after the proposed strategy has been executed

Documenting Results

- Some organizations document
  - outcome of control strategy for each information asset-threat pair in an action plan
- Includes:
  - Concrete tasks, each with accountability assigned to an organizational unit or to an individual

7. Legal & Ethical Issues