Co-funded by
the European Union

Course: Security Analysis and Risk Management

Project: Cyber Security 4 ALL(CS4ALL)

Chapter 1

Understanding Risks in Cyber Systems

Overview

- Understanding Risks in Cyber Systems
- Fundamental concepts and terms in cybersecurity
- Overview of cybersecurity principles and risk management in cyber systems
- Introduction to threats, vulnerabilities, risks, controls
- Differences and intersections between IT Security, Information Assurance, and Risk Management

Introduction

- **Understanding risks in cyber systems is crucial to managing and mitigating potential threats that can affect the security, integrity, and functionality of these systems.**
- **The risk in cyber system has changed over the years and has become more challenging topic of the day.**
- **It is important to know the different areas to focus on when evaluating and understanding these risk**

Co-funded by
the European Union

Key Areas

Co-funded by
the European Union

Fundamental Concepts and Terms in Cybersecurity

- **Cybersecurity: Protecting systems, networks, and data from cyber threats.**
- **Threat: Potential harm from malicious actions (e.g., malware, hacking).**
- **Vulnerability: Weakness in a system that can be exploited.**
- **Risk: Likelihood of a threat exploiting a vulnerability to cause harm.**
- **Control: Measure to mitigate or manage risks (e.g., firewalls, encryption).**

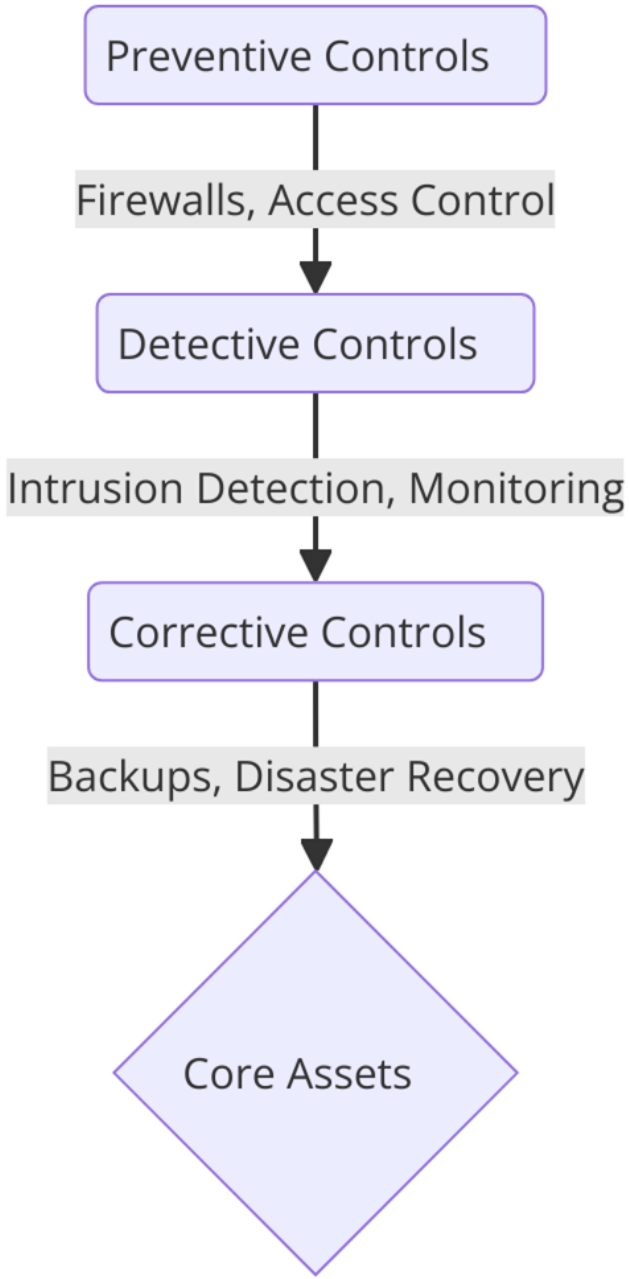
Co-funded by the European Union

Cybersecurity

- **Protects digital assets, including systems, networks, and data, against unauthorized access, attacks, and damage.**
- **Aims to uphold the Confidentiality, Integrity, and Availability (CIA triad) of information, ensuring data remains protected, accurate, and accessible only to authorized users.**
- **Encompasses several disciplines, such as threat detection, incident response, risk management, and compliance with industry regulations.**

Co-funded by
the European Union

Layered Cybersecurity Defense Model



Co-funded by the European Union

Threat

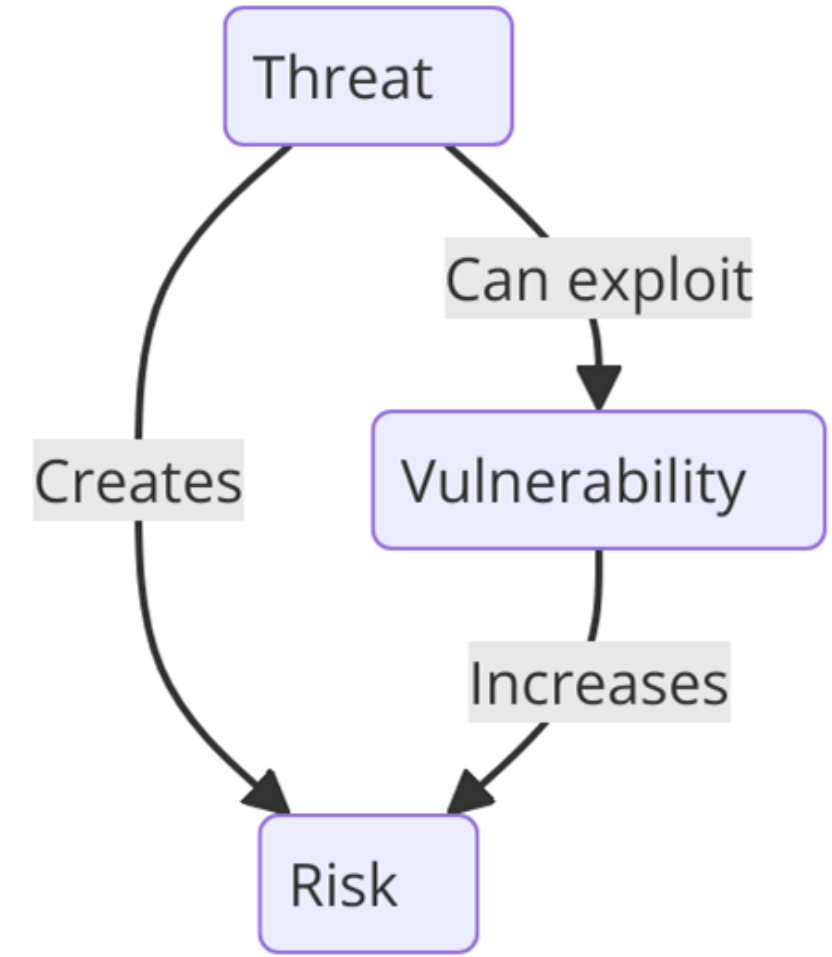
Potential harm from malicious actions

Categories:

- **External Threats: Such as cybercriminals, hacktivists, and state-sponsored attackers targeting organizations for financial or political gain.**
- **Internal Threats: Insiders with access to sensitive data who might misuse it, either intentionally (disgruntled employees) or unintentionally (human error).**

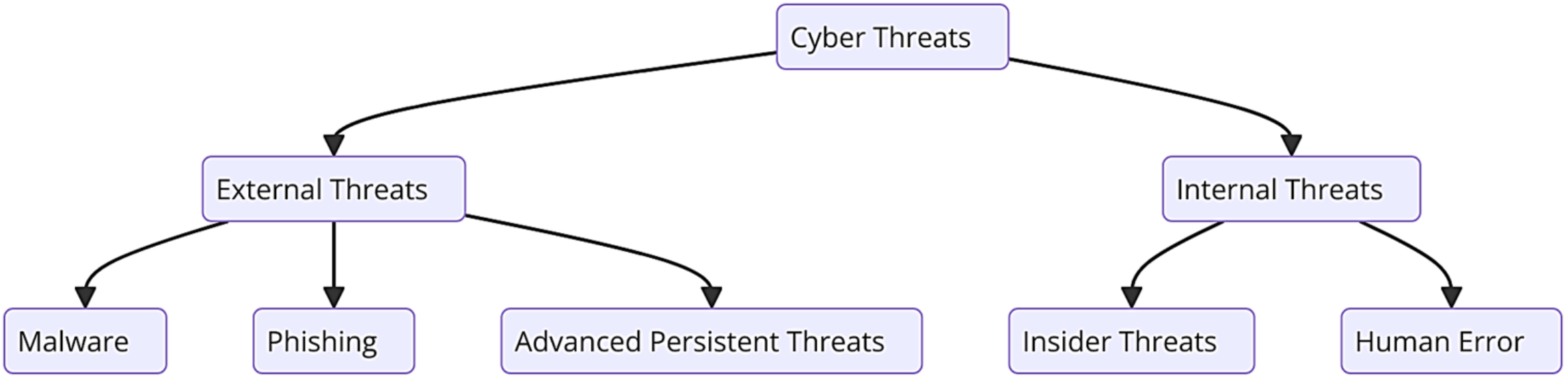
Types of Threats:

- **Malware: Includes viruses, worms, and spyware intended to disrupt, damage, or gain control of systems.**
- **Social Engineering: Psychological manipulation to gain unauthorized access or information.**
- **Advanced Persistent Threats (APTs): Prolonged attacks by sophisticated actors, often targeting sensitive government or corporate data.**



Co-funded by
the European Union

Cybersecurity Threats Landscape Map



Co-funded by
the European Union

Vulnerability

Weaknesses in software, hardware, or organizational practices that can be exploited by threats to gain unauthorized access or cause harm.

Common Sources:

- **System Flaws: Unpatched software or hardware flaws that make systems susceptible to attacks.**
- **Weak Authentication: Lack of multi-factor authentication or reliance on weak, easily guessable passwords. Lack of Employee**
- **Training: Employees unaware of phishing or social engineering tactics increase susceptibility to attacks.**

Mitigation: Regular updates, patch management, secure coding practices, and training programs help reduce vulnerabilities.

Co-funded by
the European Union

Risk

The likelihood that a given threat will exploit a vulnerability and impact the organization.

Risk Factors:

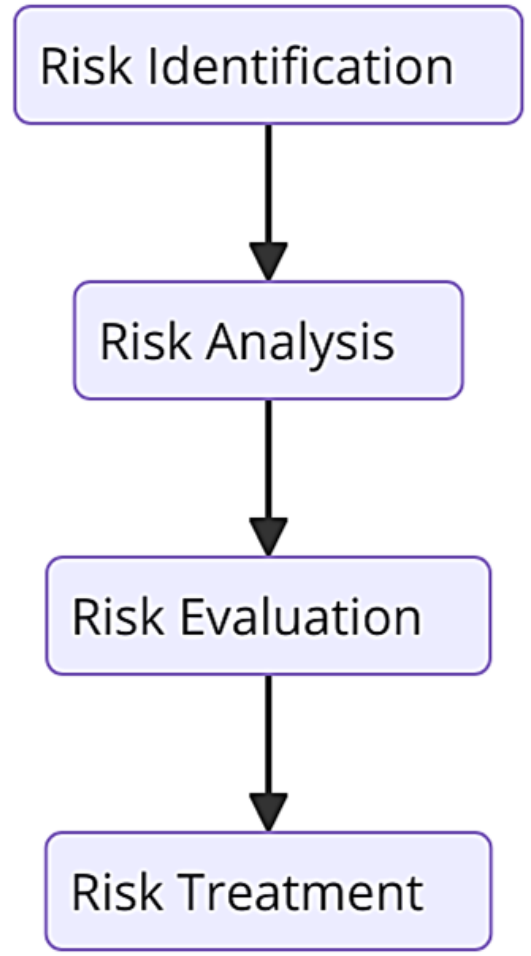
- **Exposure: The extent to which a system is exposed to potential threats, both internal and external.**
- **Impact: The severity of potential damage or loss if a vulnerability is exploited (e.g., financial loss, data breach, reputational harm).**
- **Probability: The chance that a particular threat will exploit a vulnerability within a specified timeframe.**

Co-funded by the European Union

Risk Assessment

Risk Assessment Process

- **Identification: Identifying potential risks that could impact the organization.**
- **Analysis: Evaluating the severity of each risk based on its probability and potential impact.**
- **Mitigation Planning: Deciding on risk treatment methods such as accepting, transferring, mitigating, or avoiding the risk.**



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Control

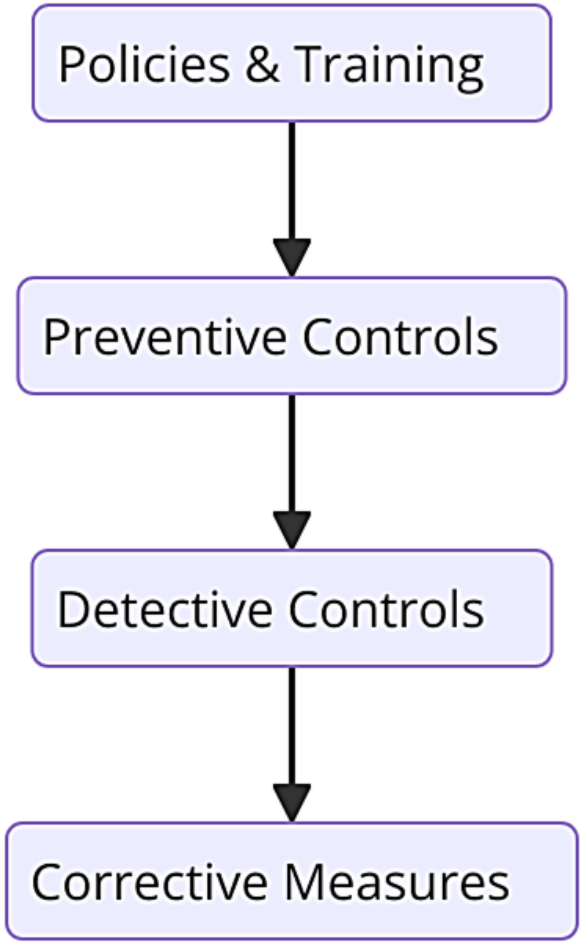
Actions or tools put in place to minimize risks and protect against threats by preventing, detecting, or responding to incidents.

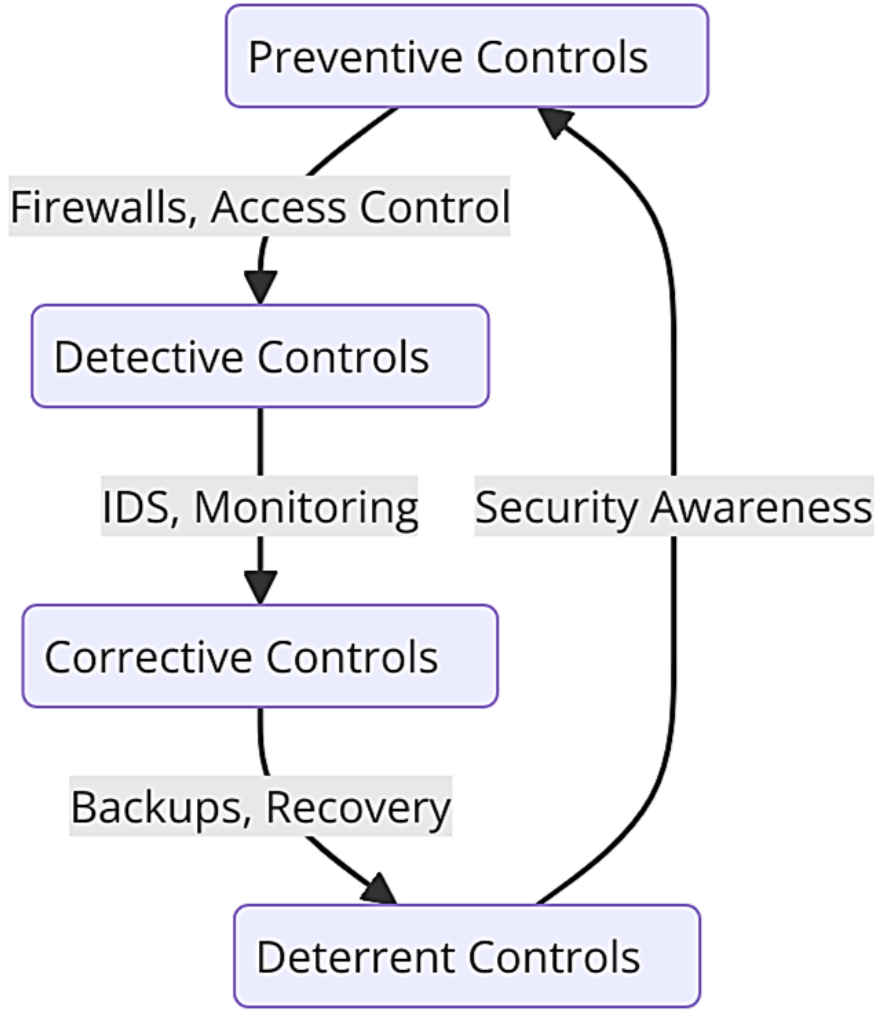
Categories of Controls:

- **Preventive: Stop attacks before they happen, using firewalls, strong authentication, and secure configurations.**
- **Detective: Identify and alert on suspicious activity; examples include log analysis, network monitoring, and IDS/IPS (Intrusion Detection/Prevention Systems).**
- **Corrective: Restore systems and data after an incident, including backup and disaster recovery plans.**
- **Deterrent: Discourage attackers by increasing the perceived risk, such as by employing visible security measures.**

Co-funded by the European Union

Control Framework and Quadrant





Co-funded by
the European Union

Cybersecurity Principles

- **Confidentiality: Protecting information from unauthorized access.**
- **Integrity: Ensuring information accuracy and trustworthiness.**
- **Availability: Ensuring reliable access to information for authorized users.**
- **Non-repudiation: Ensuring that actions cannot be denied (e.g., digital signatures).**
- **Authentication: Verifying identity before granting access.**

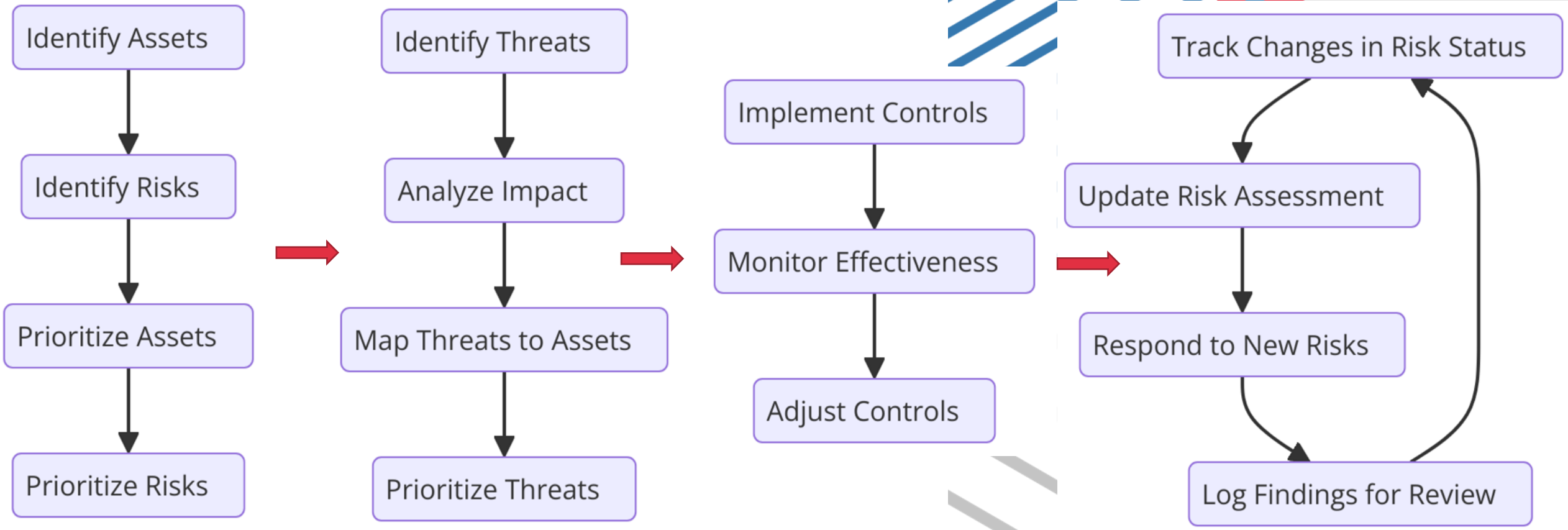
Co-funded by
the European Union

Risk Management in Cyber Systems

- **Risk Assessment: Identifying and prioritizing assets and risks.**
- **Threat Modeling: Understanding potential threats and their impact.**
- **Risk Mitigation: Implementing controls to minimize risk.**
- **Continuous Monitoring: Tracking changes in risk status over time.**

Co-funded by the European Union

Risk Management in Cyber Systems



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by
the European Union

Differences and Intersections Between Key Areas

- **IT Security: Focuses on protecting technology infrastructure.**
- **Information Assurance: Ensures integrity, availability, and protection of information.**
- **Risk Management: Identifies, assesses, and mitigates risks across IT and business.**

Co-funded by the European Union

Conclusion

- Cybersecurity Risks: Evolving threats require proactive risk management.
- Foundational Principles: Confidentiality, integrity, and availability are essential.
- Integration: Effective cybersecurity requires combining IT security, information assurance, and risk management.

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union

Resources

List the resources :

- https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
- https://cybermap.kaspersky.com/
- https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

Co-funded by
the European Union