Co-funded by
the European Union

Course: IT Fundamentals of Cyber Security

Project: Cyber Security 4 ALL(CS4ALL)

CHAPTER III

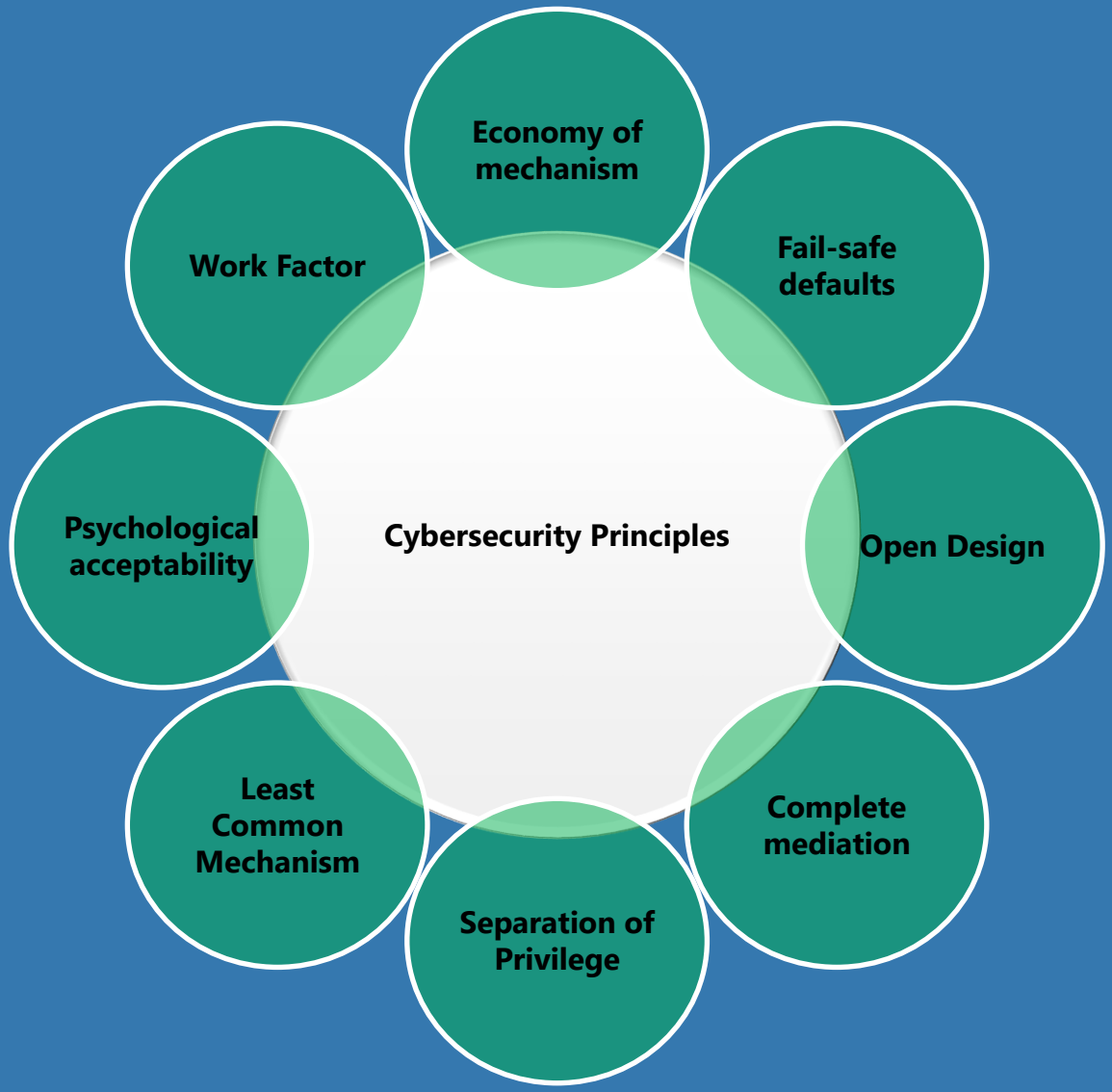
Basics of Cyber Security

Contents

- ✓ **Security Principles and Goals**
  - Definition and Importance of Cybersecurity
  - Overview of Cybersecurity Principles and Goals
- ✓ **Threat Landscape and Cyber Security Trends**
  - Common and Cyber Emerging Threats
  - Creating an Incident Response plan and Best practices
  - Cyber Security Trends and Importance of Threat Intelligence
- ✓ **Overview of Cybersecurity Framework and Standards**
  - NIST Cybersecurity Framework
  - COBIT Framework
  - GDPR and Data Protection Standards
  - Implementing Cybersecurity Framework

Co-funded by the European Union

Cybersecurity Principles



Cybersecurity Goals

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

- **Protect the confidentiality of data.**
- **Reserve the integrity of data.**
- **Promote the availability of data for authorized users.**

Co-funded by
the European Union

Cybersecurity

Co-funded by the European Union

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at assessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Importance of Cybersecurity

Co-funded by the European Union

- Essential for protecting our digital assets, including intellectual property, and critical infrastructure.
- Cyberattacks can have serious consequences, including financial loss & reputational damage.
- As more and more data is stored and transmitted electronically, the risk of cyber-attacks has also increased.
- Cybersecurity is the practice of protecting computer systems, networks, and data from theft, damage, or unauthorized access.

Overview of Cybersecurity Principles and Goals

It provide strategic guidance on how an organization can protect their information technology and operational technology systems, applications and data from cyber threats. These cyber security principles are grouped into five functions:

- ✓ **GOVERN : Develop a strong cyber security culture**
- ✓ **IDENTIFY: Identify assets and associated security risks.**
- ✓ **PROTECT: Implement controls to manage security risks.**
- ✓ **DETECT: Detect and analyse cyber security events to identify cyber security incidents.**
- ✓ **RESPOND: Respond to and recover from cyber security incidents**

Co-funded by the European Union

Threat Landscape and Cyber Security Trends

The threat landscape is the entirety of potential and identified cyberthreats affecting a particular sector, group of users, time period, and so forth.

Co-funded by
the European Union

Common and Cyber Emerging Threats

❑ *Phishing*

Phishing is a common type of cyber attack that targets individuals through email, text messages, phone calls, and other forms of communication.

Malware is a common cyber-attack and an umbrella term for various malicious programs delivered and installed on end-user systems and servers.

❑ *Malware*

❑ *Ransomware*

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and then demands a payment to unlock and decrypt the data.

Co-funded by the European Union

Impact of Cyber Threats

- Financial Loss
- Reputational Damage
- Containing the impact
- Loss of Intellectual Property
- Disruption of Operations
- Legal and Regulatory Consequences
- Psychological and Emotional Consequences

Cyber Security Trends and Importance of Threat Intelligence

Cyber Security Trends

- Rise of AI and Machine Learning
- Increase in Ransomware Attacks
- Cloud Security Internet of Things (IoT) Vulnerabilities
- Cybersecurity Skills Gap

Co-funded by
the European Union

Importance of Threat Intelligence

- Protecting Sensitive Data
- Prevention of Cyber Attacks
- Safeguarding Critical Infrastructure
- Maintaining Business Continuity
- Compliance with Regulations

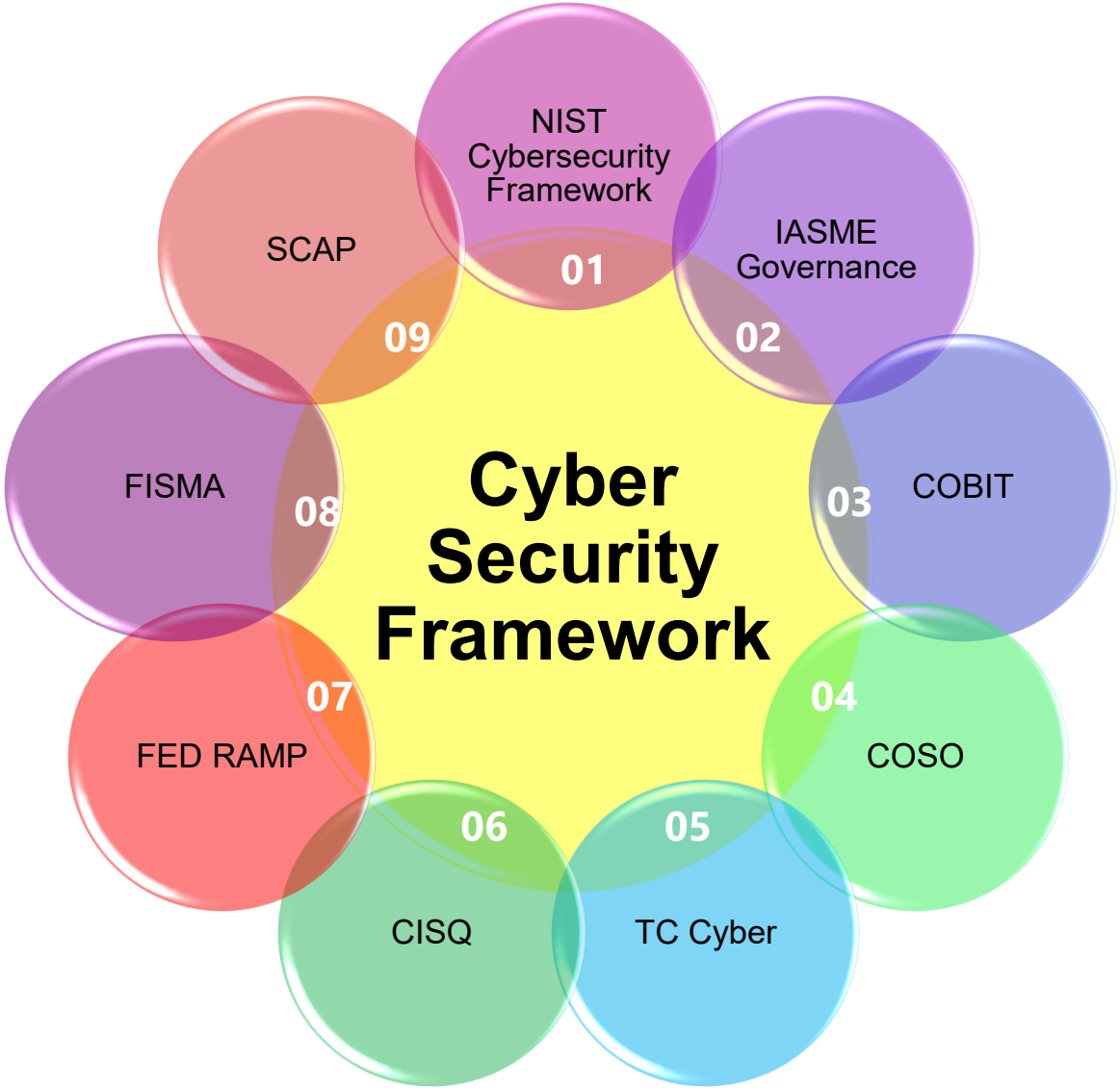
Co-funded by the European Union

Cybersecurity Framework and Standards

- It is a structured set of guidelines and best practices designed to help organizations manage and mitigate cybersecurity risks.
- To reduce the company's exposure to cyberattacks, and to identify the areas most at risk for data breaches.
- It provides a common language and systematic approach

Co-funded by the European Union

Cybersecurity Framework and Standards



Co-funded by the European Union

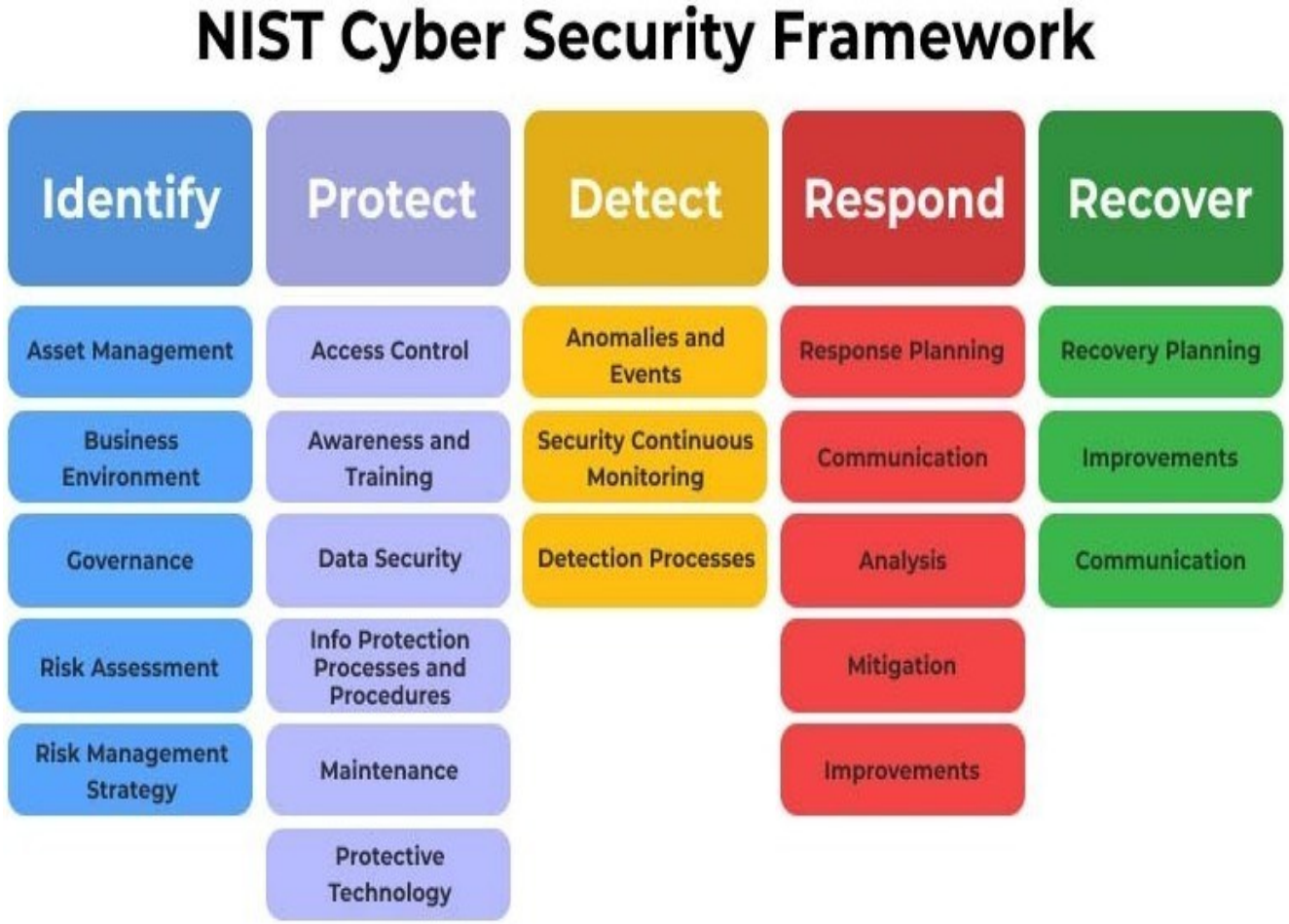
NIST Cybersecurity Framework

The National Institutes of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce, introduced the eponymously named NIST Cybersecurity framework in 2014. Initially designed for the benefit of private sector organizations in the United States.
the NIST Cybersecurity framework is centered around five essential functions, namely:

- Identify
- Protect
- Detect
- Respond
- Recover

Co-funded by the European Union

NIST Cybersecurity framework is centered around five essential functions:



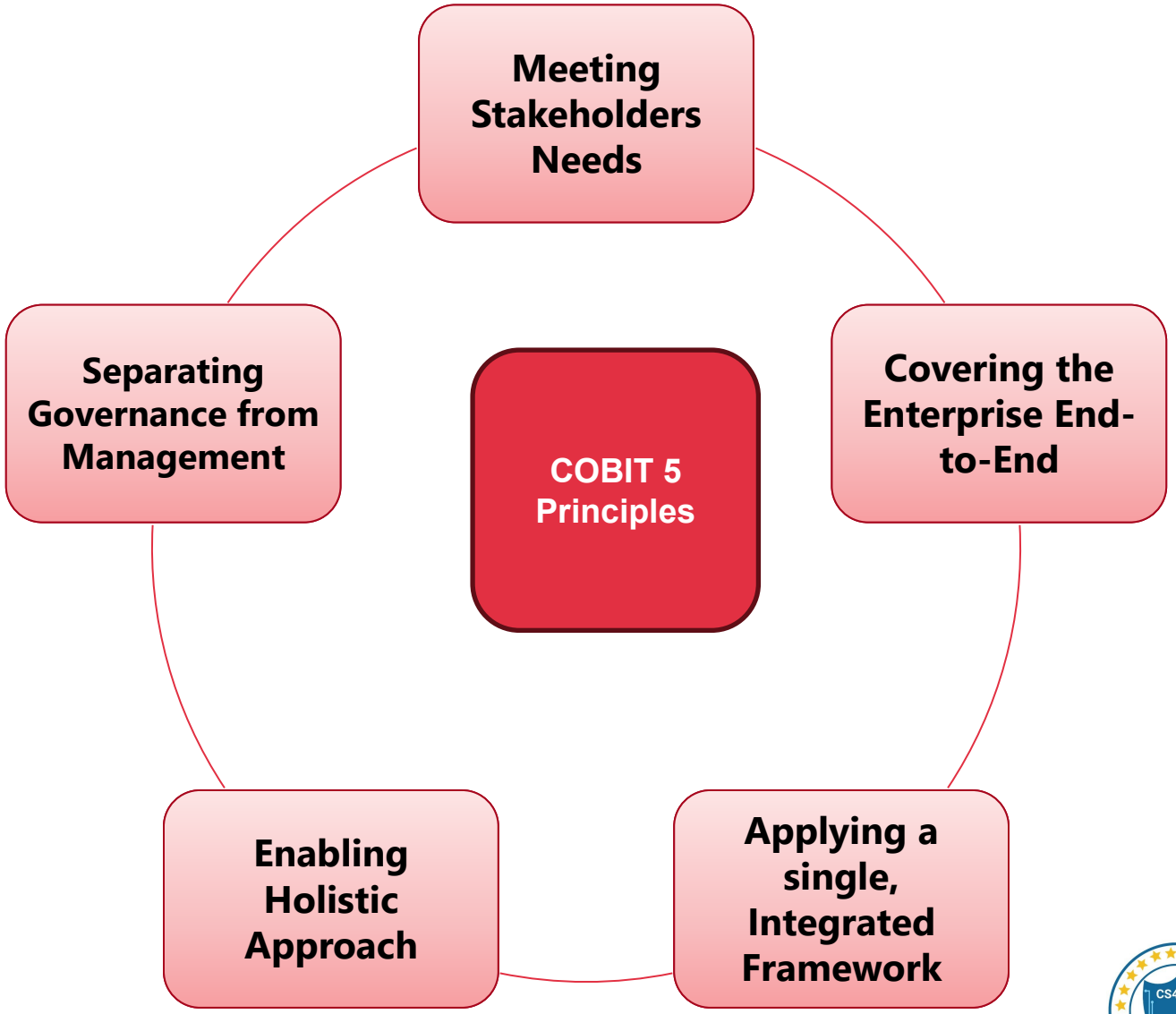
Co-funded by the European Union

COBIT Framework

COBIT (Control Objectives for Information and Related Technologies) is a framework created by the ISACA for IT management and governance. A highly process-oriented framework, COBIT's approach links business and IT goals together to delineate IT and Business teams' responsibilities.

Co-funded by the European Union

COBIT 5 Principles



Co-funded by the European Union

GDPR and Data Protection Standards

The GDPR requires that personal data must be processed securely using appropriate technical and organizational measures. The Regulation does not mandate a specific set of cyber security measures but rather expects you to take 'appropriate' action.

Data protection is a core component of both cybersecurity and GDPR compliance. The GDPR outlines six specific principles required of companies when processing personal data:

- **Lawfulness, fairness, and transparency**
- **Purpose limitation**
- **Data minimization**
- **Storage limitation**
- **Integrity and confidentiality**
- **Overarching accountability**

Co-funded by the European Union

Implementing Cybersecurity Framework

Seven Step Process for Framework Implementation

Prioritize and Scope
Determine Organizational Components to use Framework

Orient
Identify the systems, assets, requirements and risk management approaches

Create Current Profile
Map current cybersecurity and risk management practices to a framework Implementation tire

Conduct a risk assessment
Identify risks above Implementation Tire

Create a Target Profile
Describe a desired Cybersecurity Outcomes & Develop Target Implementation Tire

Determine, Analyze, and Prioritize Gap
Determine resources to address gape and create a prioritized Action Plan

Implement Action Plan
Monitor Cybersecurity Practices against Target Profile

CONCLUSION

The basics of cybersecurity are essential for protecting personal and organizational data from digital threats. By understanding common cyber risks, practicing secure behaviors and implementing protective measures like strong passwords, data encryption, and regular software updates, individuals and organizations can significantly reduce their vulnerability to cyber attacks. Staying informed and proactive is key to maintaining cybersecurity in an evolving digital landscape.

Co-funded by
the European Union

Questions & Answers

Co-funded by
the European Union

Resources

Reference Books:

1. Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press.
4. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J.David Irwin.CRC PressT&FGroup

Reference Links:

1.https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security

2. https://academic.oup.com/cybersecurity

3, https://www.sciencedirect.com/science/article/pii/S2352484721007289

4. https://www.techscience.com/journal/JCS

Co-funded by the European Union