جامعة الامير سلطان
PRINCE SULTAN
UNIVERSITY

Lecture 1: Cyber Security: Introduction

CYS401: Fundamental of Cyber Security

جامعة الامير سلطان
Prince Sultan University

Outline

- What is security?
- Critical characteristics of information,
- Components of an Information System,
- The system development life cycle,
- The security system development life cycle.

ICE-BREAKING

About you.

- Simple quiz on cybersecurity
- https://www.pewresearch.org/internet/quiz/cybersecurity-knowledge/

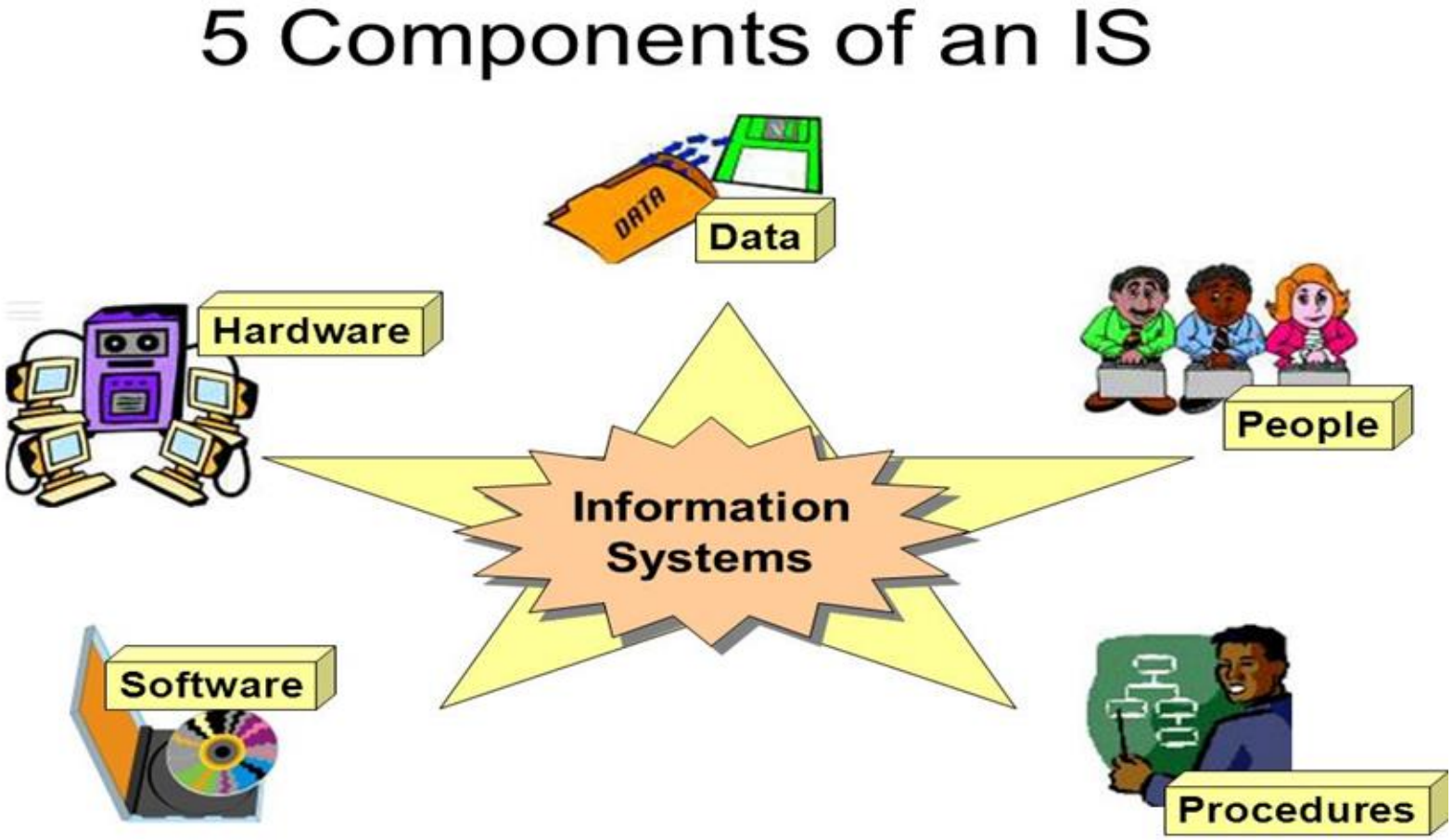
Introduction

Cyber security is:

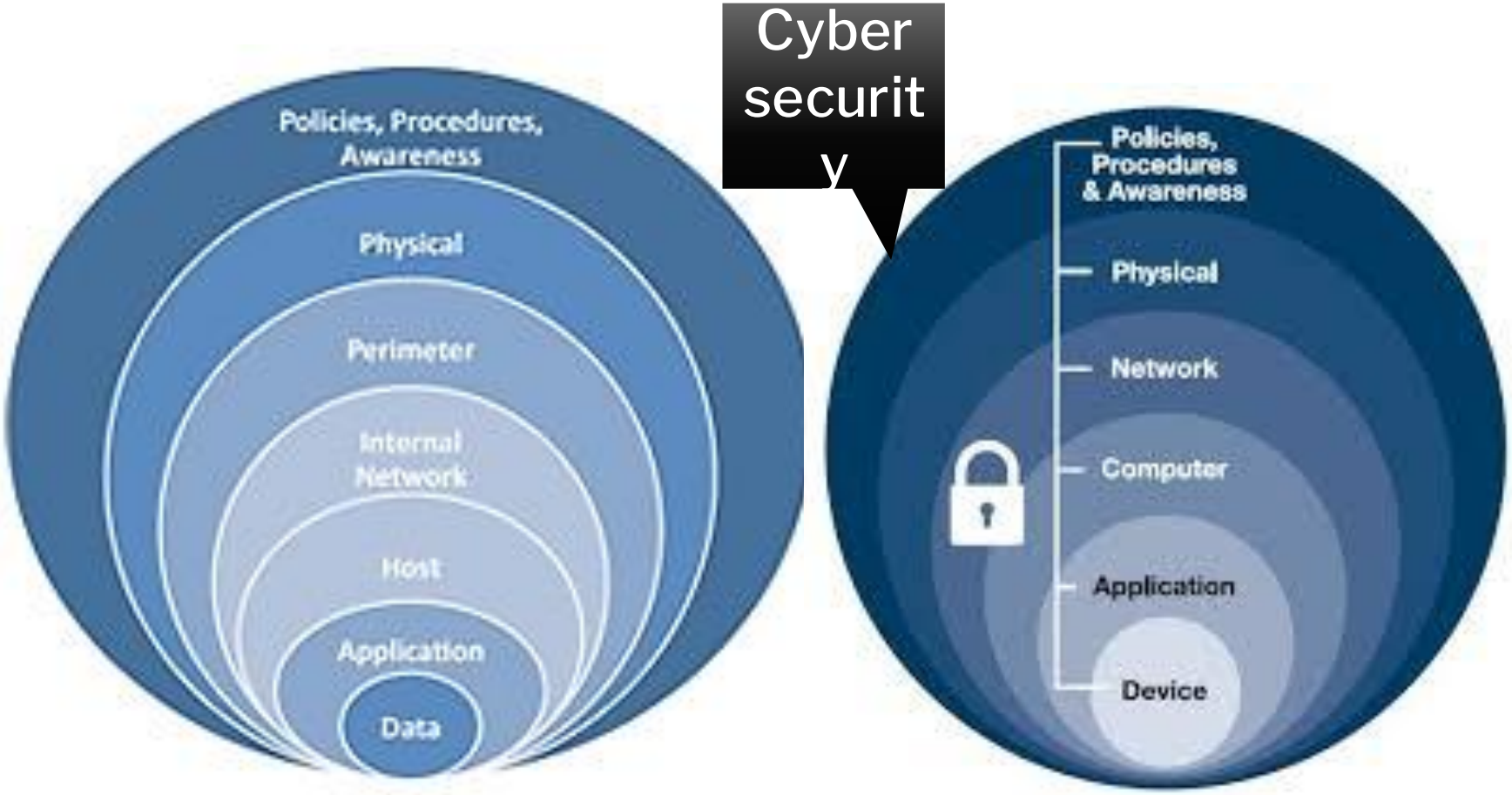
- the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

GETTING STARTED!

Introduction

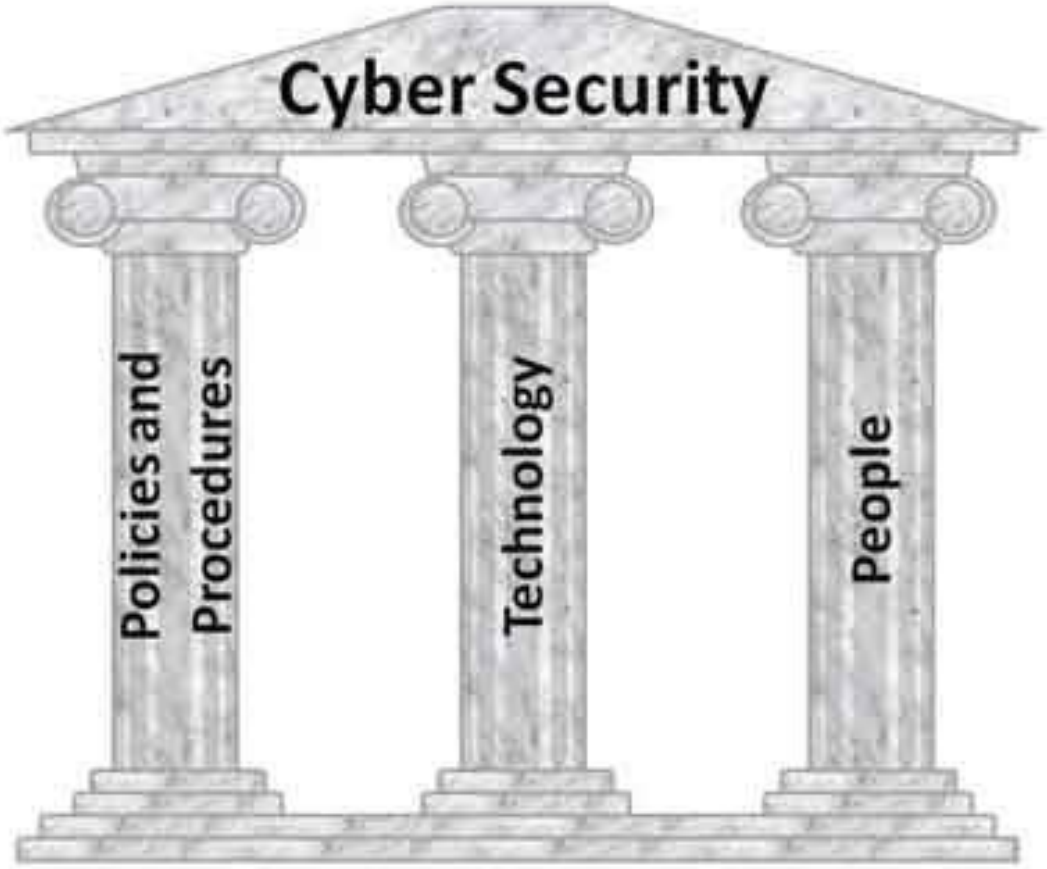


Introduction



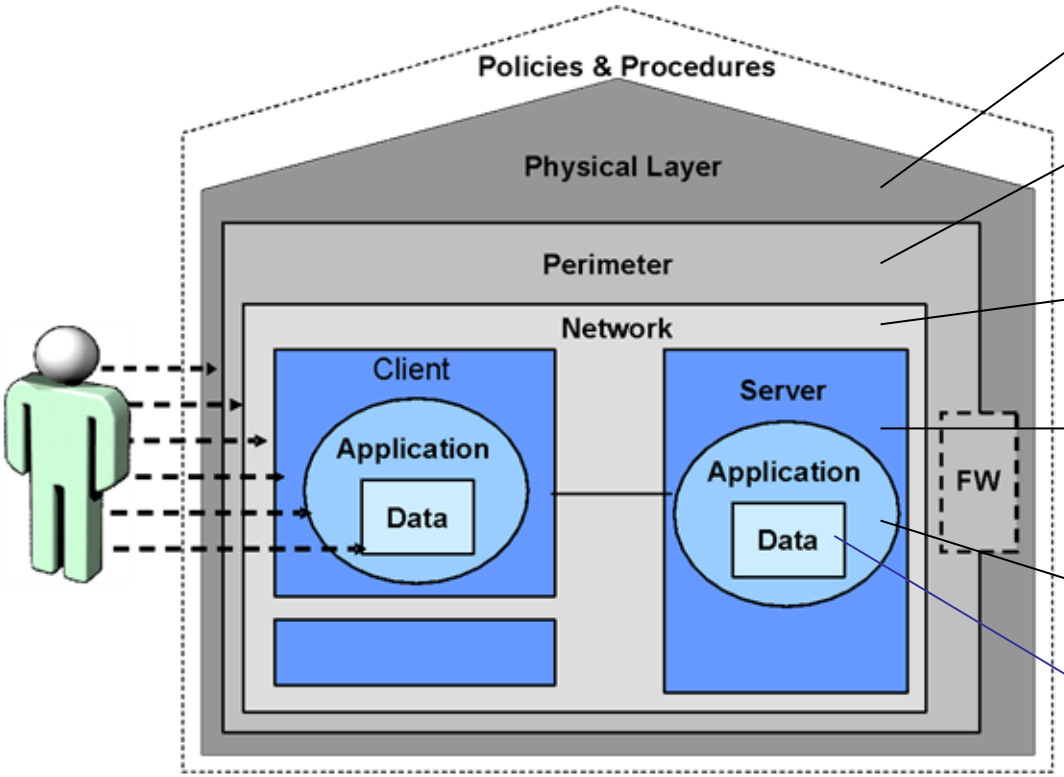
Introduction

- Cybersecurity pillars:



Introduction

Cyber security aims to build a **defense-in-depth approach**



Guards, locks, tracking devices

Firewalls, boarder routers, VPNs with quarantine procedures

Network segments, NIDS

OS hardening, authentication, security update management, antivirus updates, auditing

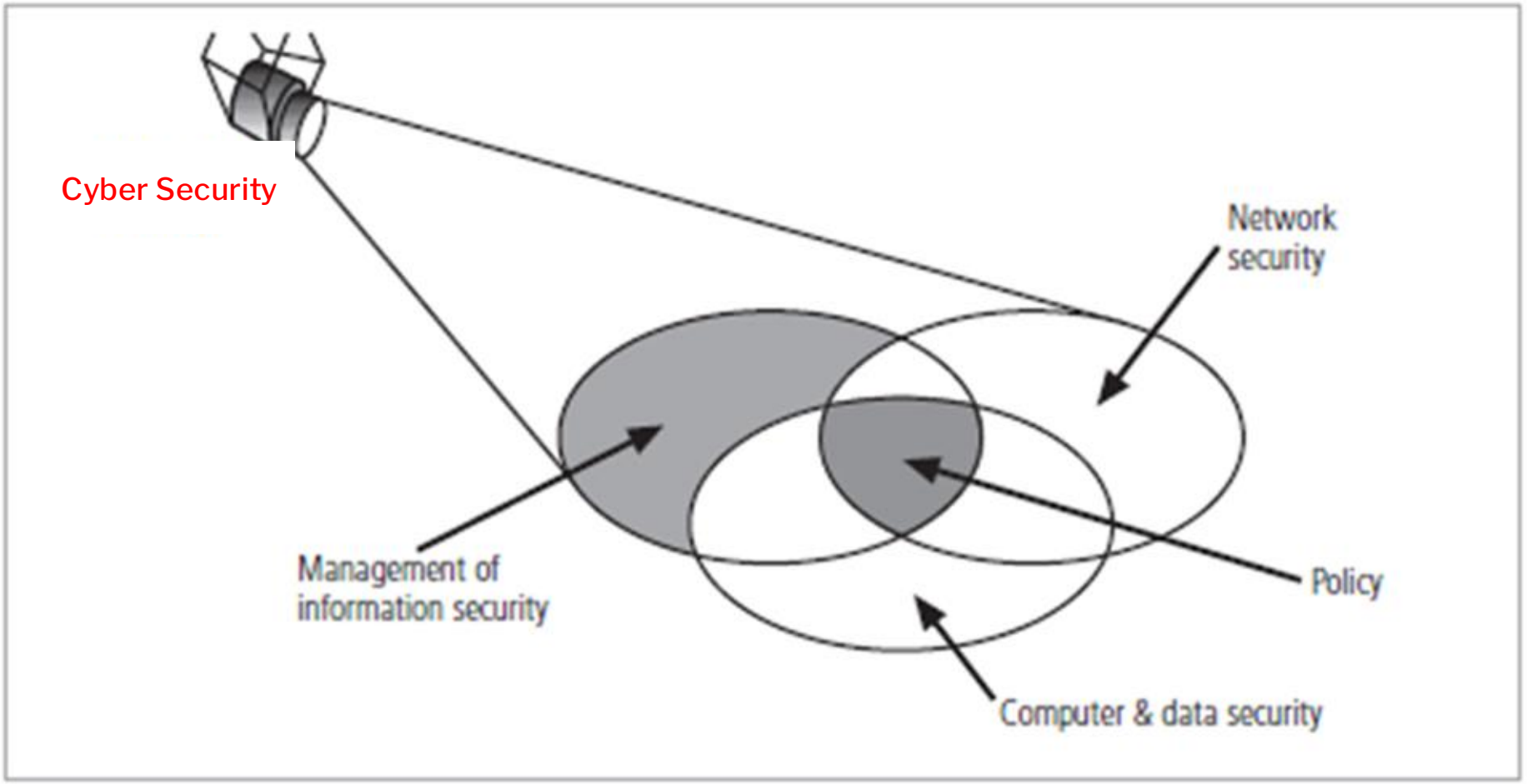
Application hardening

Strong passwords, ACLs, backup and restore strategy

Introduction

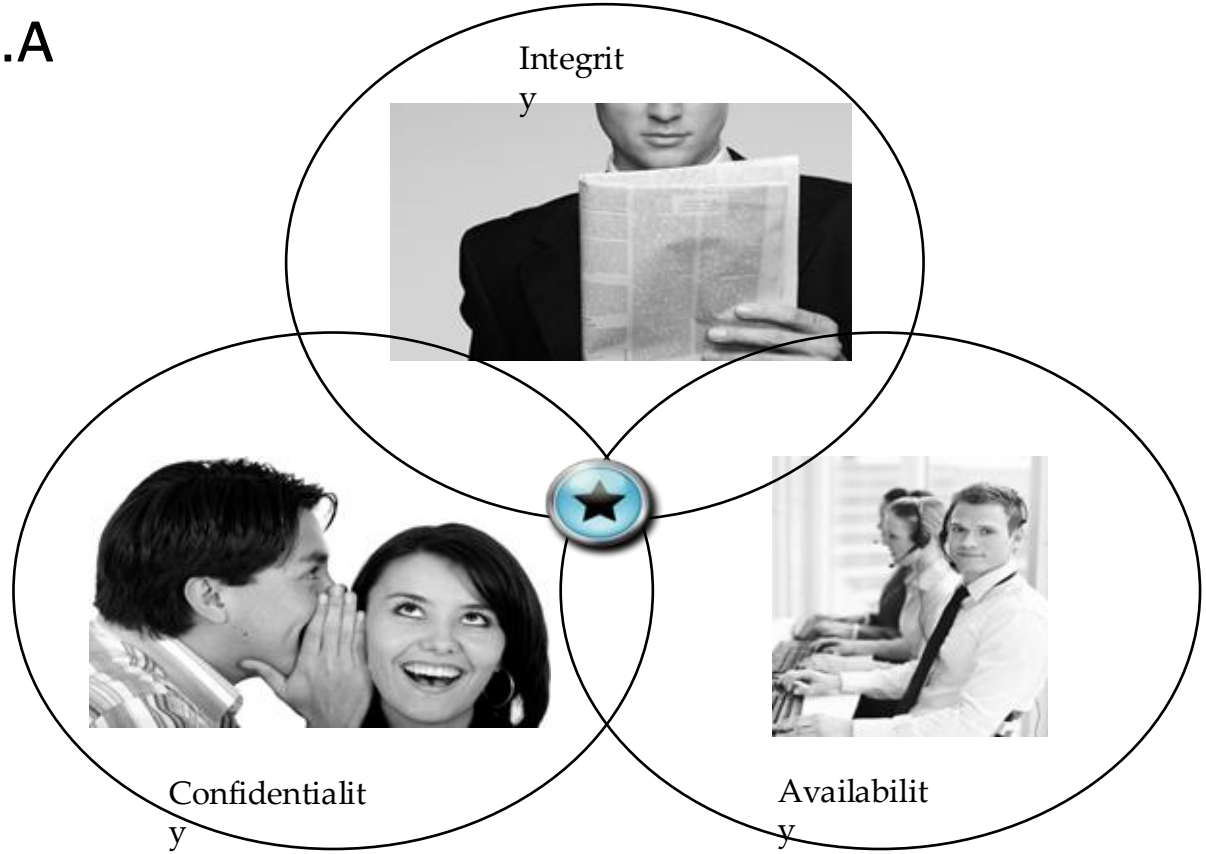
- A successful organization should have a multi-layer of security in place.
  - **Physical security**
    - Secure **physical items, objects** – from unauthorized access and misuse
  - **Personnel security**
    - Protect the **individual(s)** who are authorize to access the organization and its operations
  - **Operations security**
    - Protect the details of a particular **operations / activities**
  - **Communications security**
    - Protect **communications media / technology**
  - **Network security**
    - Protect **network components / connection**
  - **Data security**
    - Protects **C**onfidentiality / **I**ntegrity and **A**vailability of information assets – storage / processing or even during transmission

Introduction



Critical characteristics of information

- The goal of CyberSecurity?
  - C.I.A



Critical characteristics of information

- C.I.A are the ***critical characteristics*** of Information, but there are other characteristics should be considered.
  - Confidentiality
  - Integrity
  - Availability
  - Accuracy
  - Authenticity
  - Utility
  - Possession
  - The value of information comes from the characteristics it possesses:

Critical characteristics of information

- **Confidentiality** – The quality or state of preventing disclosure or exposure to unauthorized individuals or systems.
  - Credit Cards, PII, Health records.
- **Integrity** – The quality or state of being accurate, complete, and authorised.
  - The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.
- **Availability** – Enables authorized users who need to access information to do so without interference or obstruction.
  - The information is said to be available to an authorized user when and where needed and in the correct format.

Critical characteristics of information

- **Accuracy** – Free from mistakes or errors and having the value that the end user expects.
  - If information contains a value different from the user's expectations due to intentional or unintentional modification of the content, it is no longer accurate.
- **Authenticity** –The quality or state of being genuine or original, rather than a reproduction or fabrication.
  - Information is authentic when the information is the same as it was originally created, placed, stored, or transferred.
- **Utility** – The quality or state of having value for some purpose or end.
- Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end user, it is not useful.
- **Possession** – The quality or state of having ownership or control of some object or item.
- Information is said to be in possession if one obtains it, independent of format or other characteristic.

Critical characteristics of information

- While a breach of confidentiality always results in a breach of ownership, a breach of ownership does not always result in a breach of confidentiality.

- Is it correct, **how and why?**

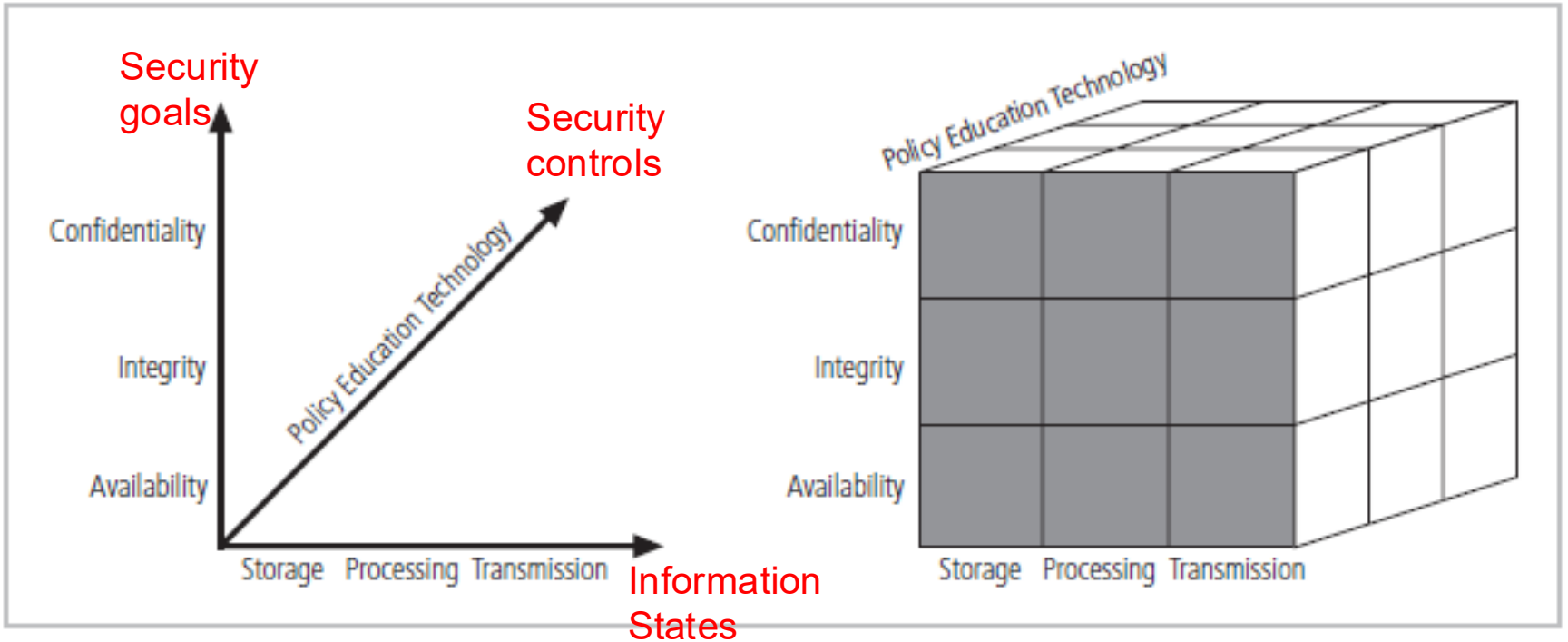
Critical characteristics of information

- In Cybersecurity, there are THREE dimensions
  - Security Goals: **C.I.A.**
  - Security measures/controls: **policy, education/training, Technology.**
  - Information States: **Storage, Transmission, Processing**

- McCumber Cube: graphical explanation to show the interconnections among the different Information security factors.

Critical characteristics of information

- McCumber Cube



Critical characteristics of information

- McCumber Cube: Dimensions and attributes
  - Desired goals: C.I.A
  - Information states
    - **Storage:** Data at rest **(DAR)** in an information system, such as that stored in memory or on a magnetic tape or disk.
    - **Transmission**: transferring data between information systems - also known as data in transit (DIT).
    - **Processing:** performing operations on data in order to achieve a desired objective.
  - Security controls:
    - **Policy and practices**: administrative controls (plans and guidance)
    - **Education**: ensuring that the users of information systems are aware of their roles and responsibilities.
    - **Technology**: software and hardware-based solutions designed to protect information systems.

Components of an Information System

- There are five components work together to achieve the ultimate goal of any information system.
  - Software
  - Hardware
  - Data
  - People
  - Procedures
- Agreeable to say that all components have their strengths and weaknesses – but when in used all together it performs a good secure IS

Components of an Information System

- Software
  - Applications / operating systems / other utilities
  - Most difficult to secure
  - Bugs / errors are just too much to handle which leads to having a insecure information
  - SW is the most important component in IS – but information security is often to not being considered at the first round of implementation – leads to having versions after versions of app.
  - By this – it is an easy target to attack the IS

Components of an Information System

- Hardware
  - Physical technology that houses and executes the SW/ stores and transmit the data and provides interfaces to run the SW
  - Securing physical assets from harm / theft
    - Traditional and still mainly used – locks and keys
    - Biometrics access controls
- Data
  - Most valuable asset possessed by an organization and often the main target of *intentional attacks*

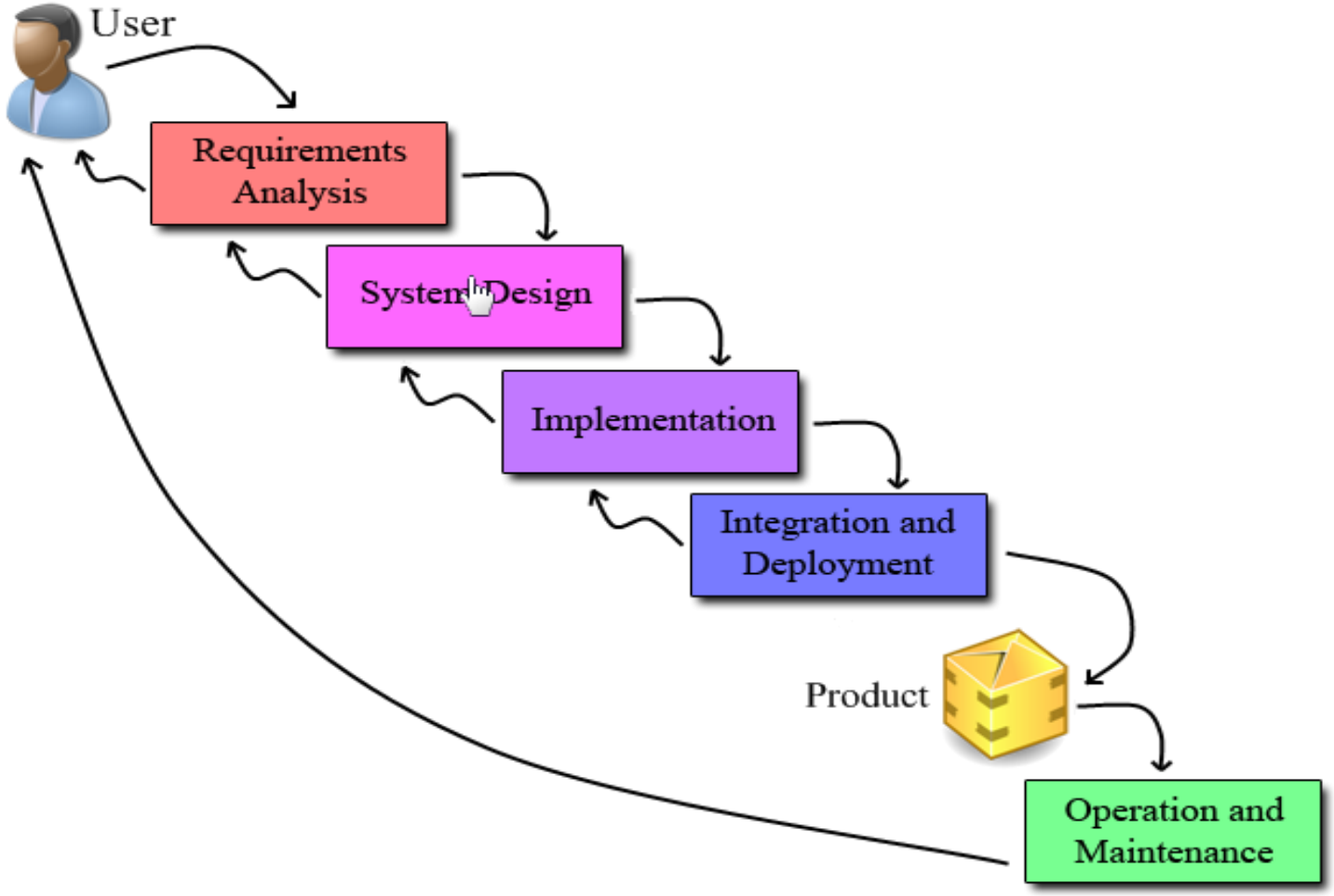
Components of an Information System

- People
  - User of the IS
  - Often threat or being threat for the data
  - Often being **the weakest component** in an IS environment
  - Policy, agreement, education and training plays important rules
- Procedures
  - Written instructions for accomplishing a specific task
  - If a unauthorized user obtains an organization's procedure – this poses a threat to the integrity of the information
  - Most organization distribute procedures to their trustful employees so they can access the IS

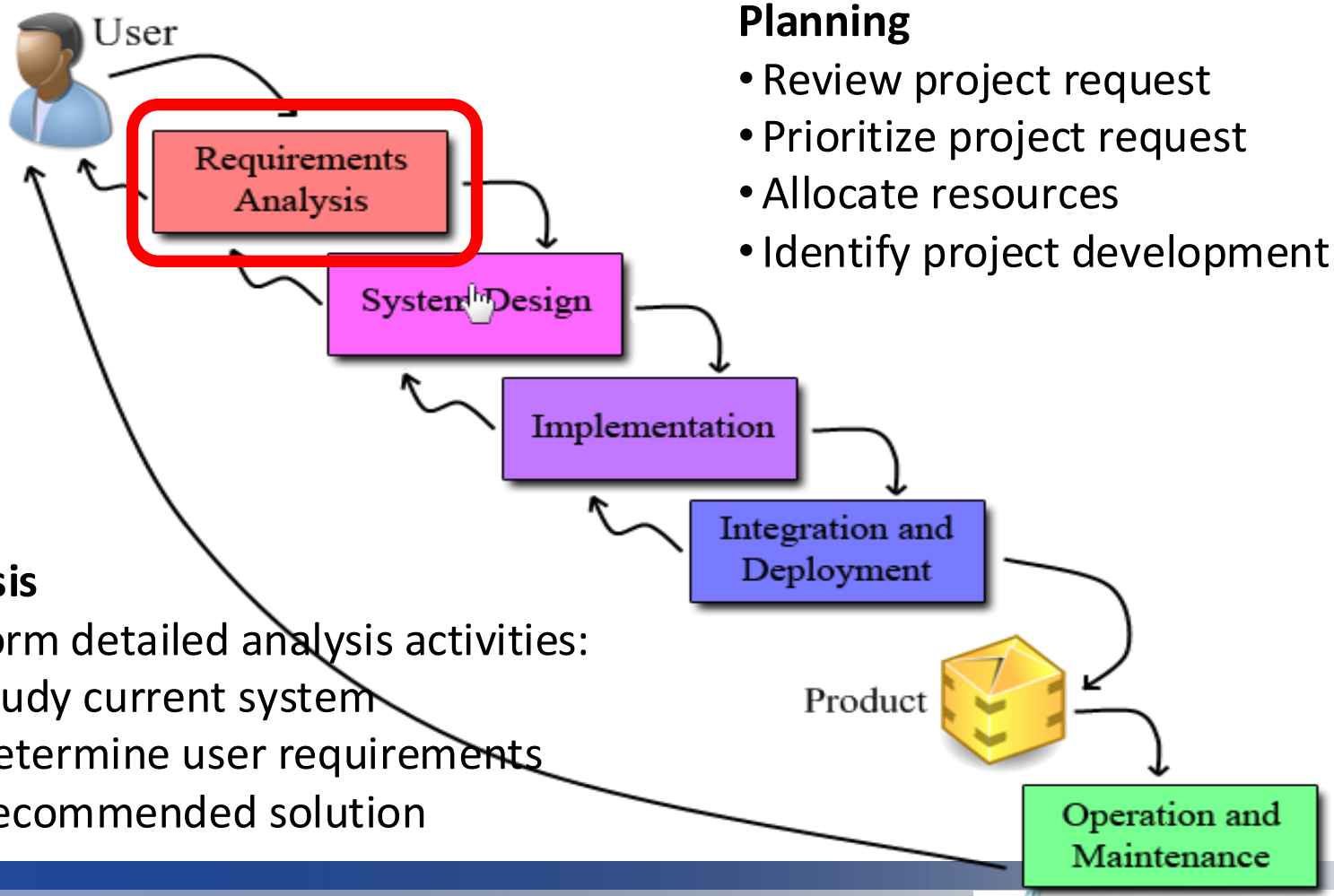
System Development Life Cycle (SDLC)

- Is a methodology / approach for designing and implementing an IS
- Sequence of procedure to solve a problem
- Most common approach – **waterfall model**

System Development Life Cycle (SDLC)



System Development Life Cycle (SDLC)



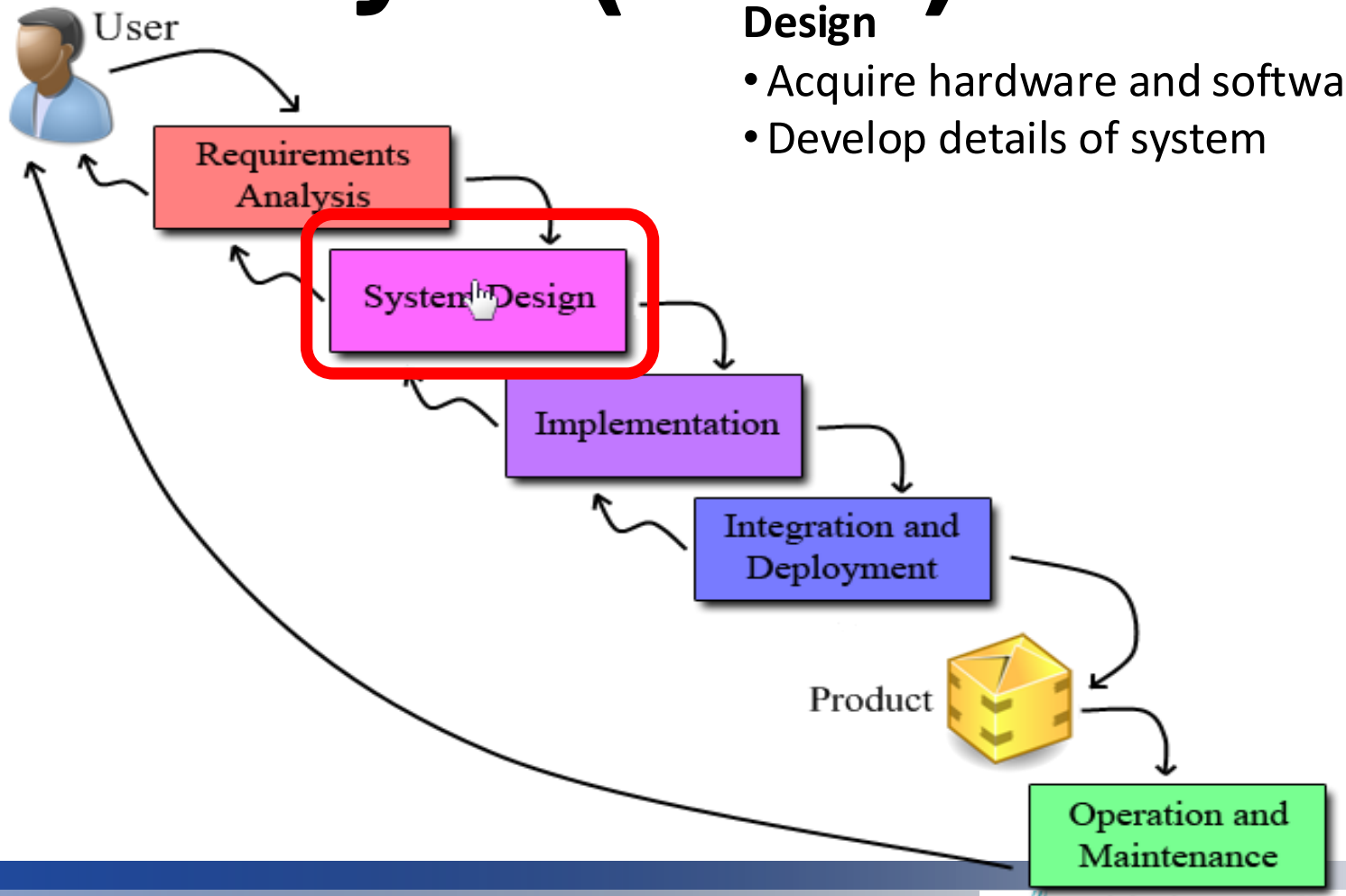
Planning

- Review project request
- Prioritize project request
- Allocate resources
- Identify project development team

Analysis

- Perform detailed analysis activities:
  - Study current system
  - Determine user requirements
  - Recommended solution

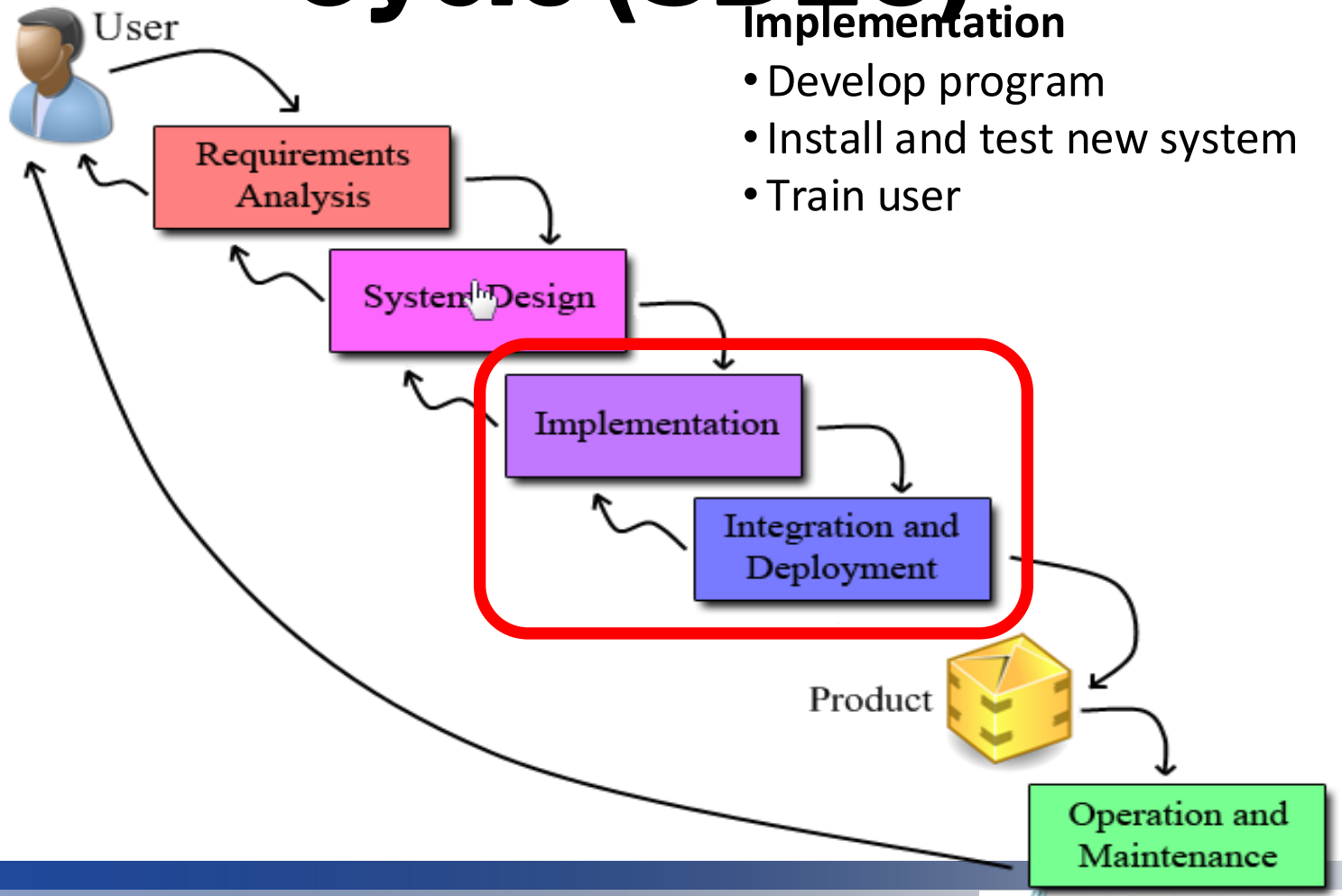
System Development Life Cycle (SDLC)



Design

- Acquire hardware and software
- Develop details of system

System Development Life Cycle (SDLC)

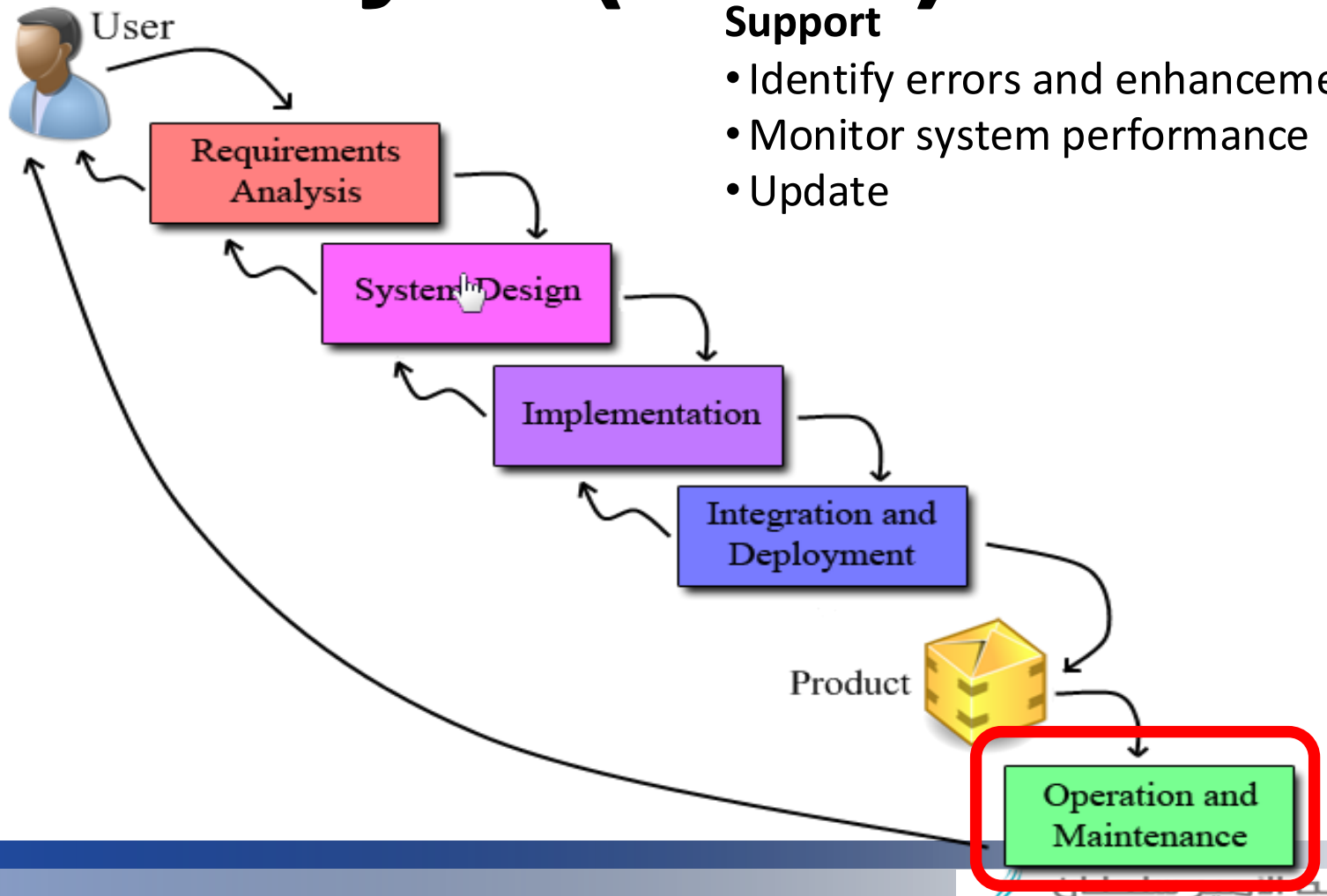


Implementation

- Develop program
- Install and test new system
- Train user

جامعة الأمير سلطان
Prince Sultan University

System Development Life Cycle (SDLC)



Support

- Identify errors and enhancements
- Monitor system performance
- Update

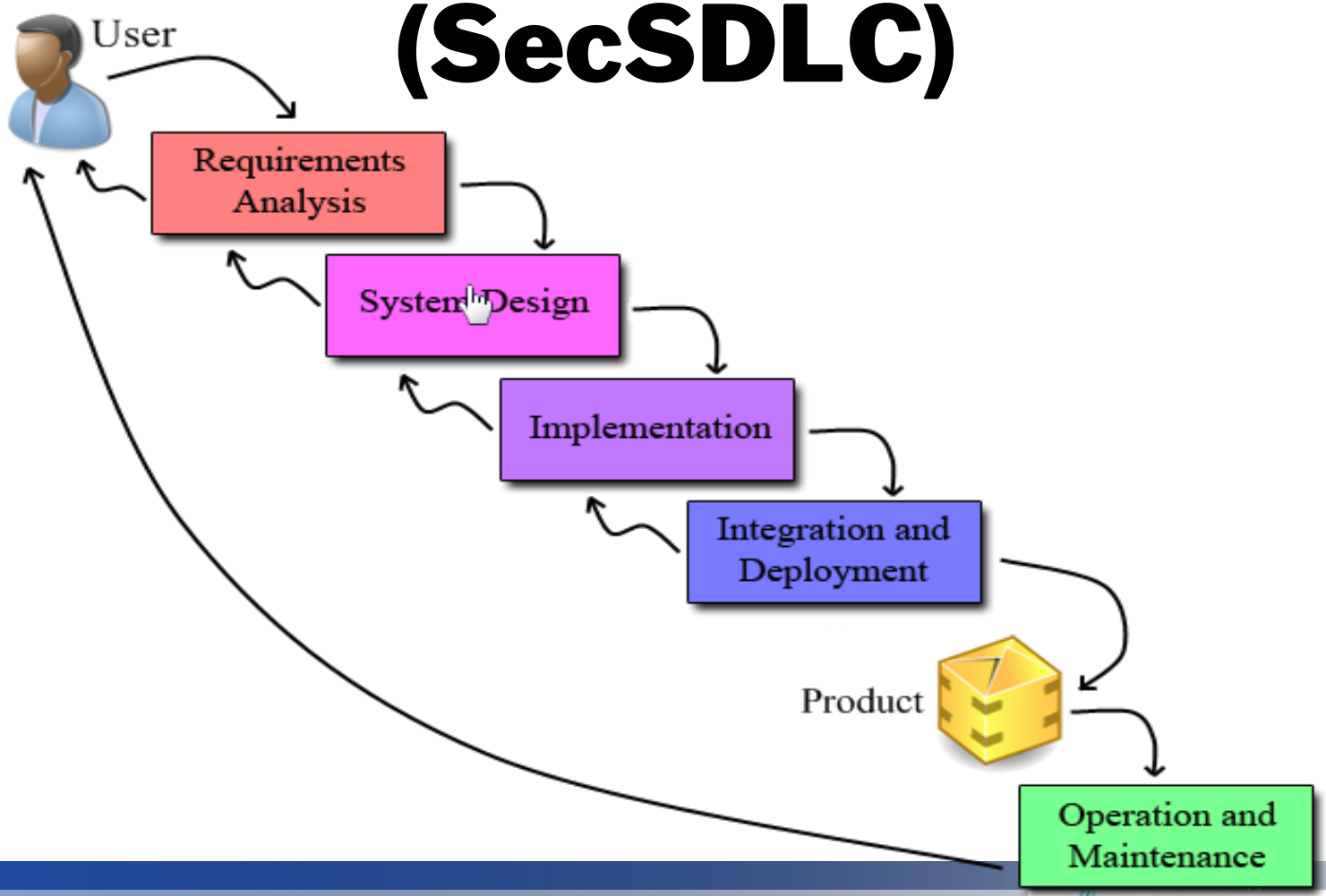
Security System Development Life Cycle (SecSDLC)

- Cybersecurity must be managed in a manner similar to any other system implementation
- One approach for implementing an cybersecurity system with security in place is to use a variation of the SDLC phases, named **Security SDLC** (SecSDLC)

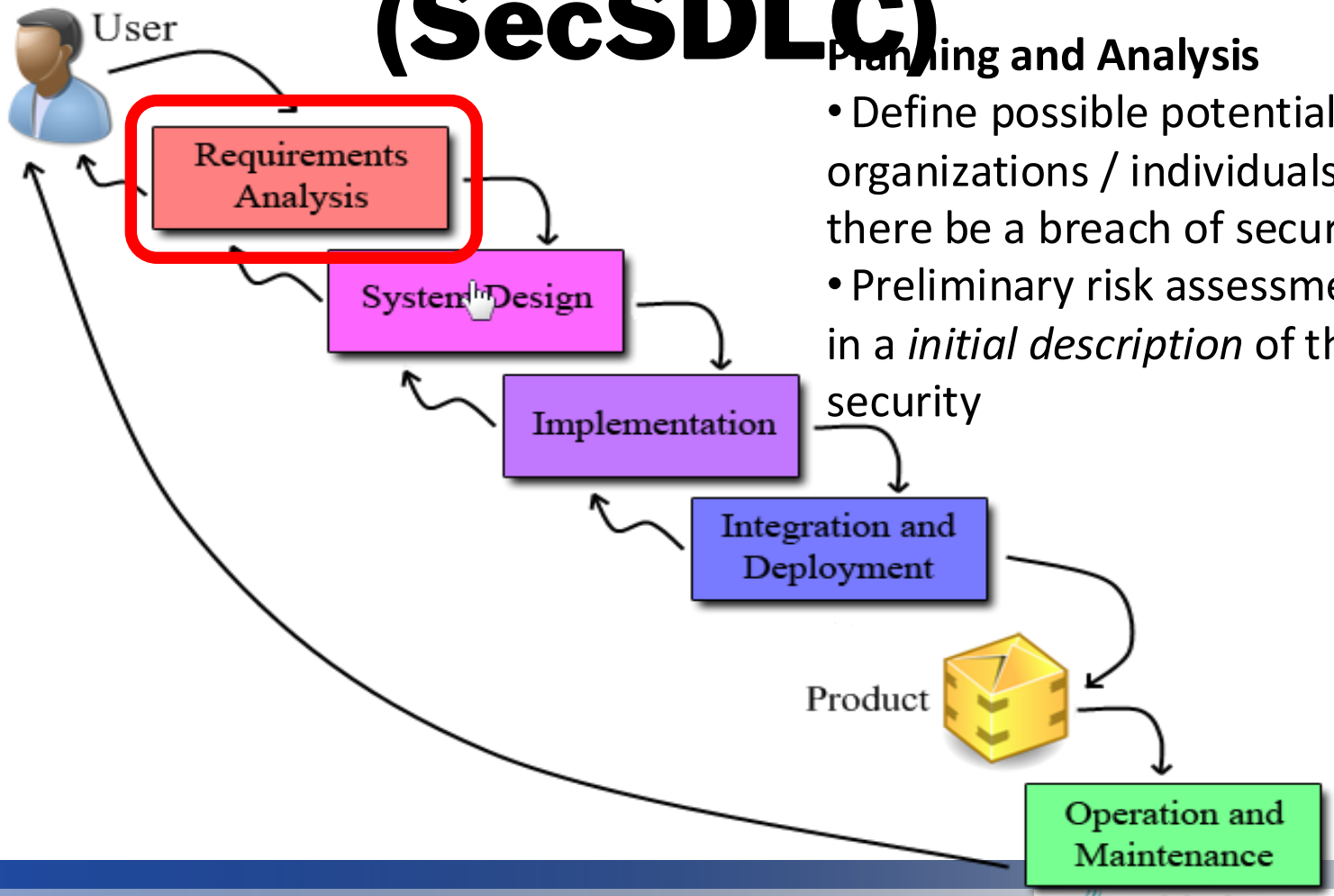
Security System Development Life Cycle (SecSDLC)

- Each phases in SecSDLC should consider the security of the system being assembled as well as the information it uses
- Each implementation done is secure and does not harm the C.I. A of the organization's information assets

Security System Development Life Cycle (SecSDLC)



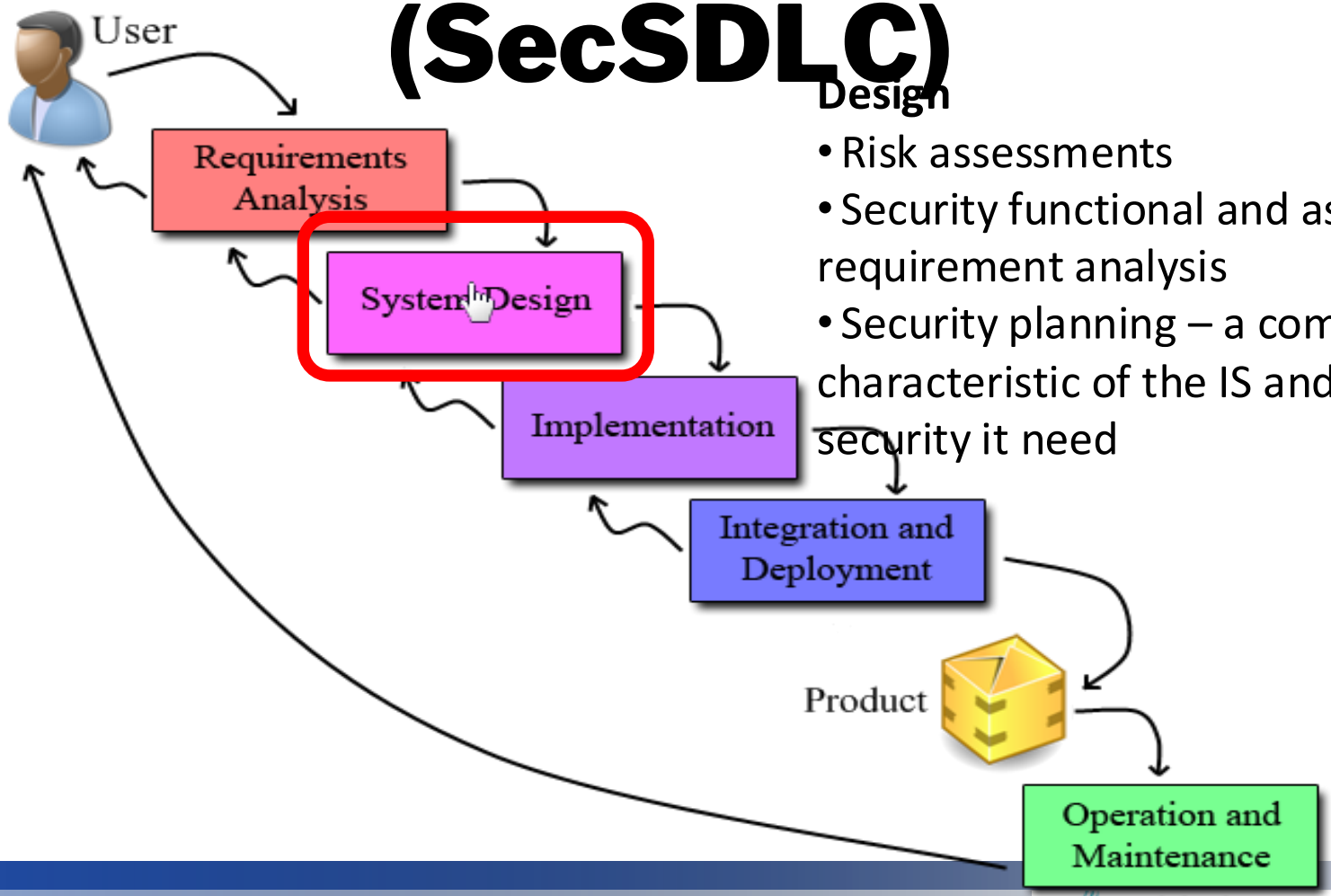
Security System Development Life Cycle (SecSDLC)



Planning and Analysis

- Define possible potential impact on organizations / individuals should there be a breach of security
- Preliminary risk assessment – result in a *initial description* of the basic security

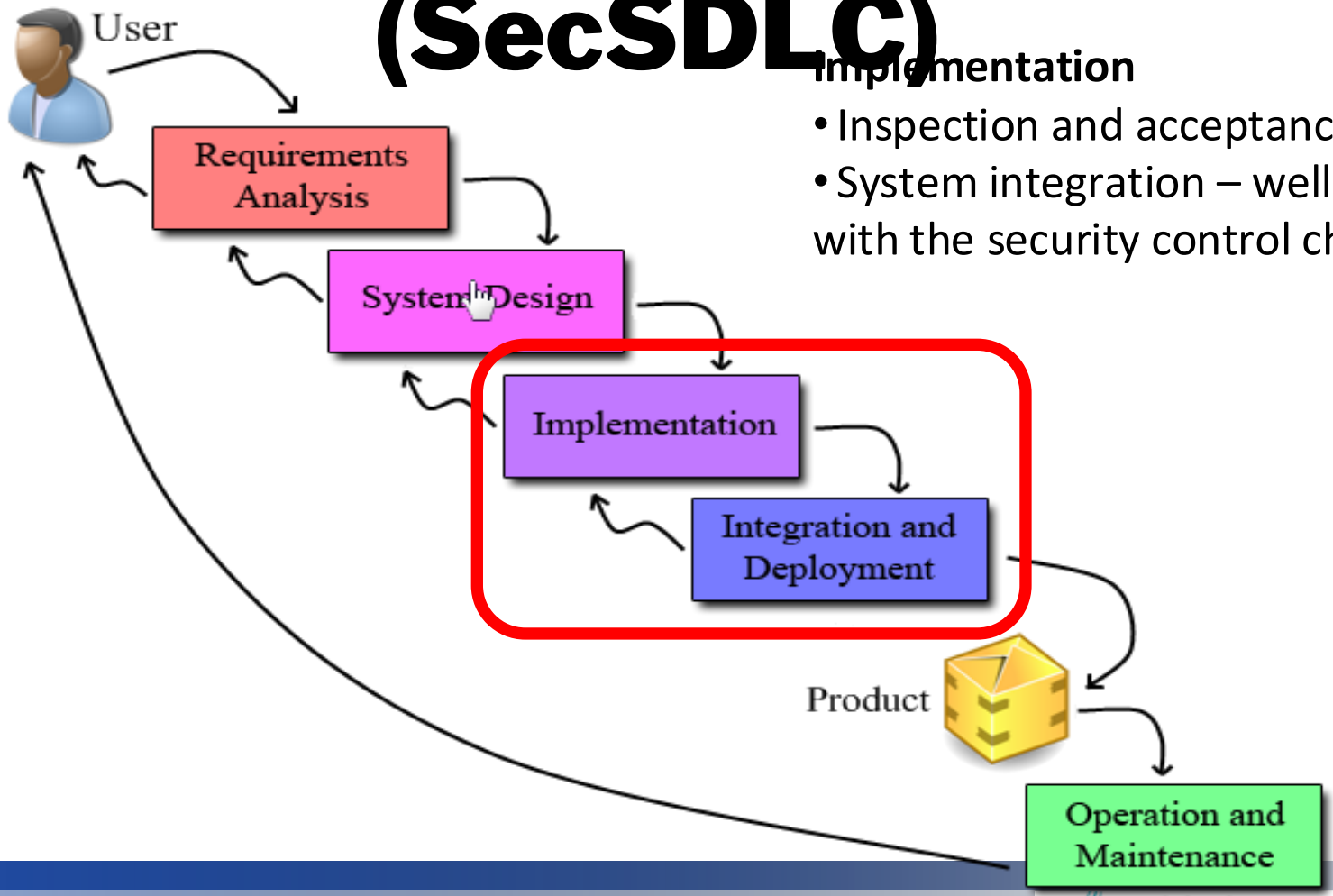
Security System Development Life Cycle (SecSDLC)



Design

- Risk assessments
- Security functional and assurance requirement analysis
- Security planning – a complete characteristic of the IS and the security it need

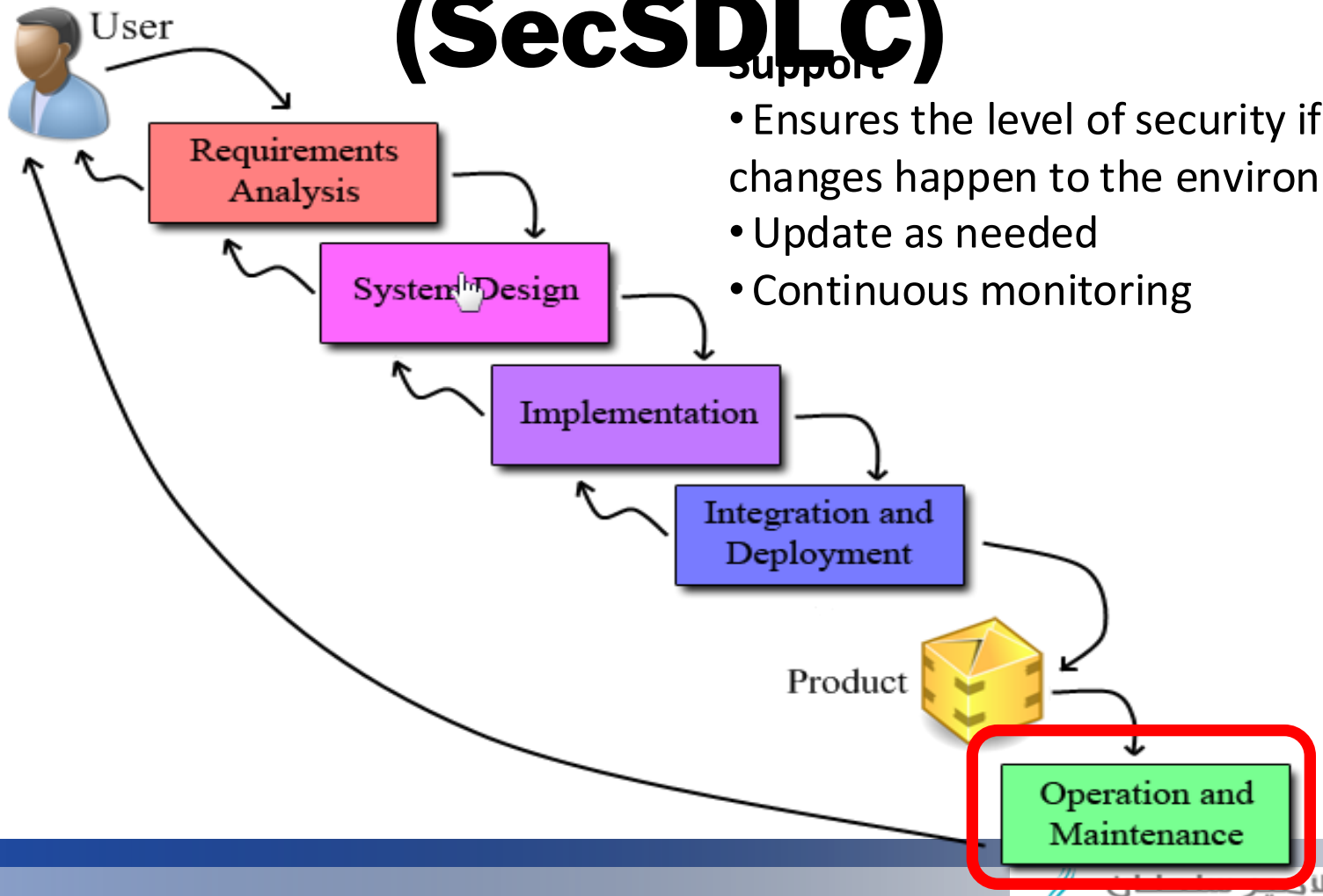
Security System Development Life Cycle (SecSDLC)



Implementation

- Inspection and acceptance
- System integration – well bounded with the security control chosen

Security System Development Life Cycle (SecSDLC)



Support

- Ensures the level of security if any changes happen to the environment
- Update as needed
- Continuous monitoring

SDLC vs. SecSDLC

- SecSDLC is basically following the exact phases as what the formal SDLC is doing
- In addition, SecSDLC identifies specific threats that possibly could happen to the IS and creates specific controls to counter those threats
- A well-observe and planning IS could be demonstrated if all possible threats been taken care off


QUESTIONS