SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)

Approvedy by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE	UNIT V	TOPIC	Semester
23CAE717 Cloud Computing	**Security in the Cloud**	Security Architecture	II Semester / I MCA

Software Development Life Cycle

Agile

Lean

Waterfall

Iterative

Spiral

DevOps

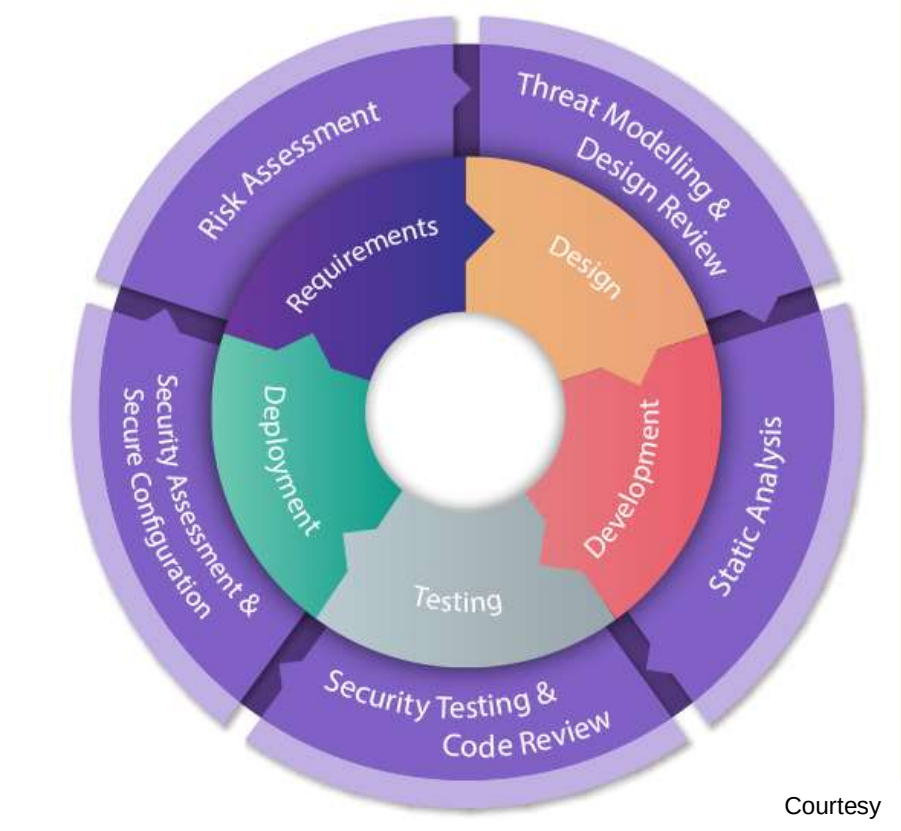
Motivation

- In the past, it was common practice to perform security-related activities only as part of testing
- Software development process that helps developers build more secure software and address security compliance requirements while reducing development cost
- It ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the development effort

SecSDLC

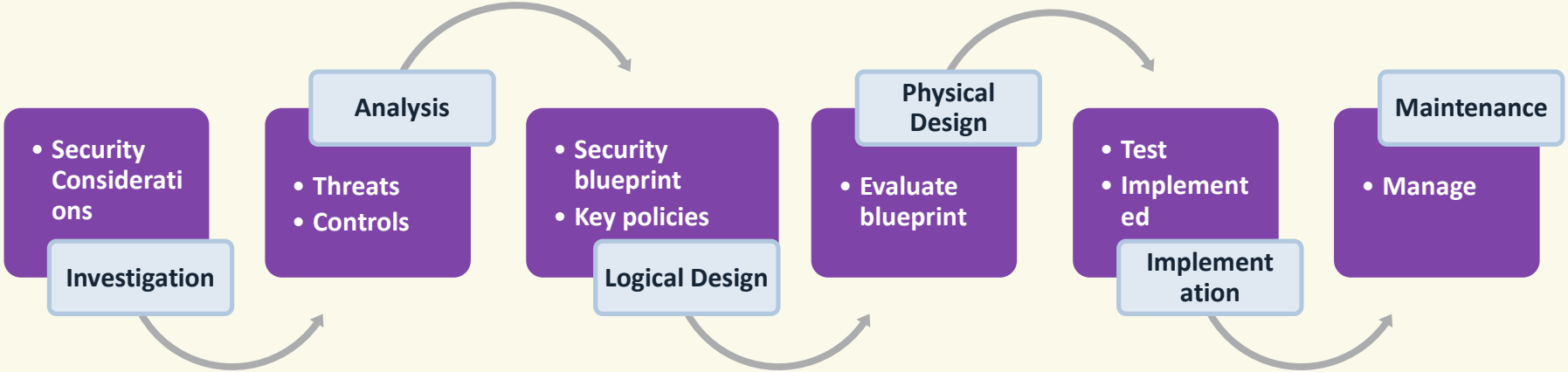
- identifying specific threats and the risks that pose to a system, and
- the necessary deployment of security controls to prevent, remove, and manage the risks involved
- It ensures that a new system or application has acceptable security controls and requirements

Security Architecture



Courtesy snyk

SecSDLC System



SecSDLC System

1. • Define project processes and goals, document them in the program security policy
2. • Analyze existing security policies, programs, threats and controls
   • examine legal issues, and perform risk analysis
3. • Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project
4. • Select technologies to support blueprint, develop a solution, design physical security measures to support technological solutions, and review and approve plans.
5. • Buy / develop security solutions.
   • At he end of this phase, present a tested package to management for approval
6. • Constantly monitor, test, modify, update, and repair to respond to changing threats

Motivation

- Advantages
  - Security is a continuous concern
  - Awareness of security concerns by stakeholders
  - Early detection of flaws in the system
  - Cost reduction as the part of early detection
  - Overall reduction of intrinsic business risks

Guidelines

- Application code is written in a consistent manner that can be audited and enhanced
- Core application services are provided in a common, structured, and repeatable manner
- Framework modules are thoroughly tested for security issues before implementation
- Training and communications should also be developed to raise awareness of process enhancements

Security Architecture

- Framework to be established with consideration of
  - processes
  - operational procedures
  - technology specifications
  - people and organizational management and
  - security program compliance and reporting
- A design and implementation program should be integrated with the formal system development life cycle

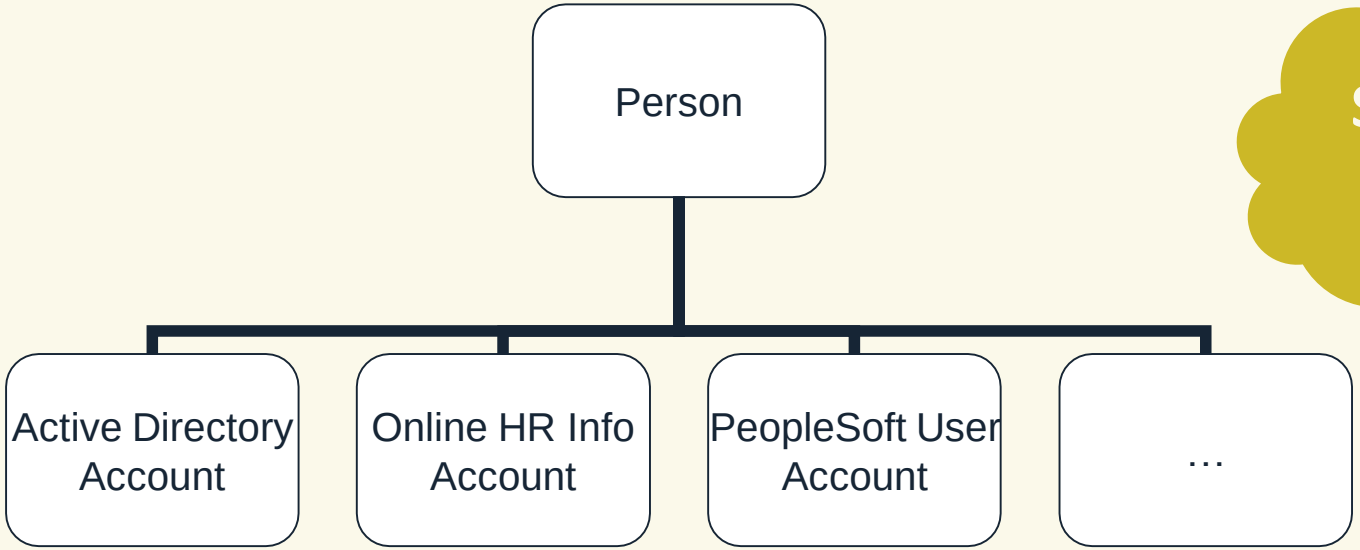
Security Architecture

- provide the following services across all technology layers
  - Authentication
  - Authorization
  - Availability
  - Confidentiality
  - Integrity
  - Accountability
  - Privacy

Security Monitoring

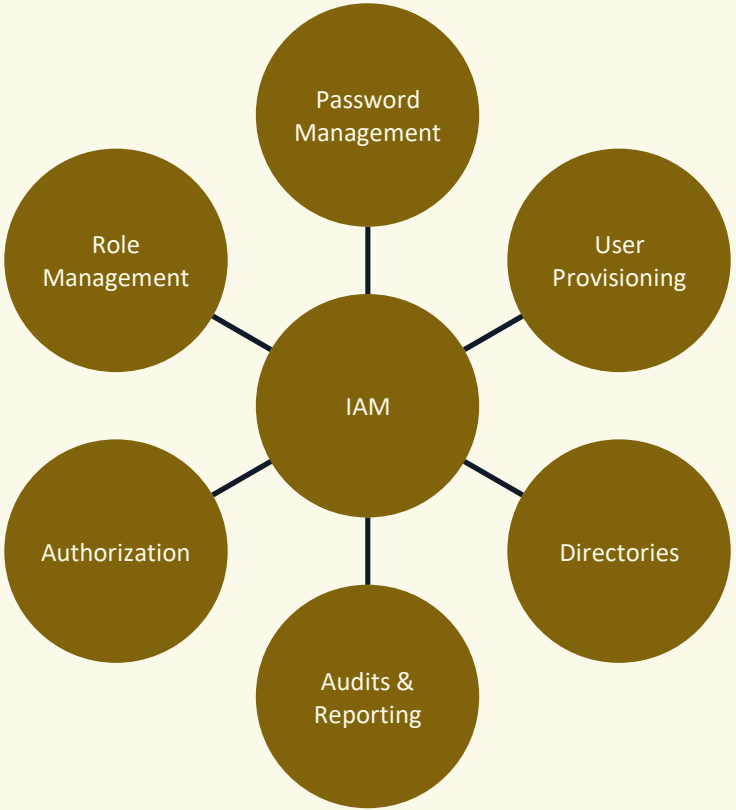
- Centralized security information management systems
- integrate with network and other systems monitoring processes like (e.g., security information management, security event management, security information and event management, and security operations centers
- security threats and issues in application and data layers

Identity and Access Management (IAM)



- Networks use multiple identity systems
- Users get confused with all of these Ids
- Management and audit has difficulty keeping track of all these Ids

Identity and Access Management (IAM)



References

- Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012
- James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
- Kumar Saurabh, “Cloud Computing – insights into New-Era Infrastructure”, Wiley India,2011.
- Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
- John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 201