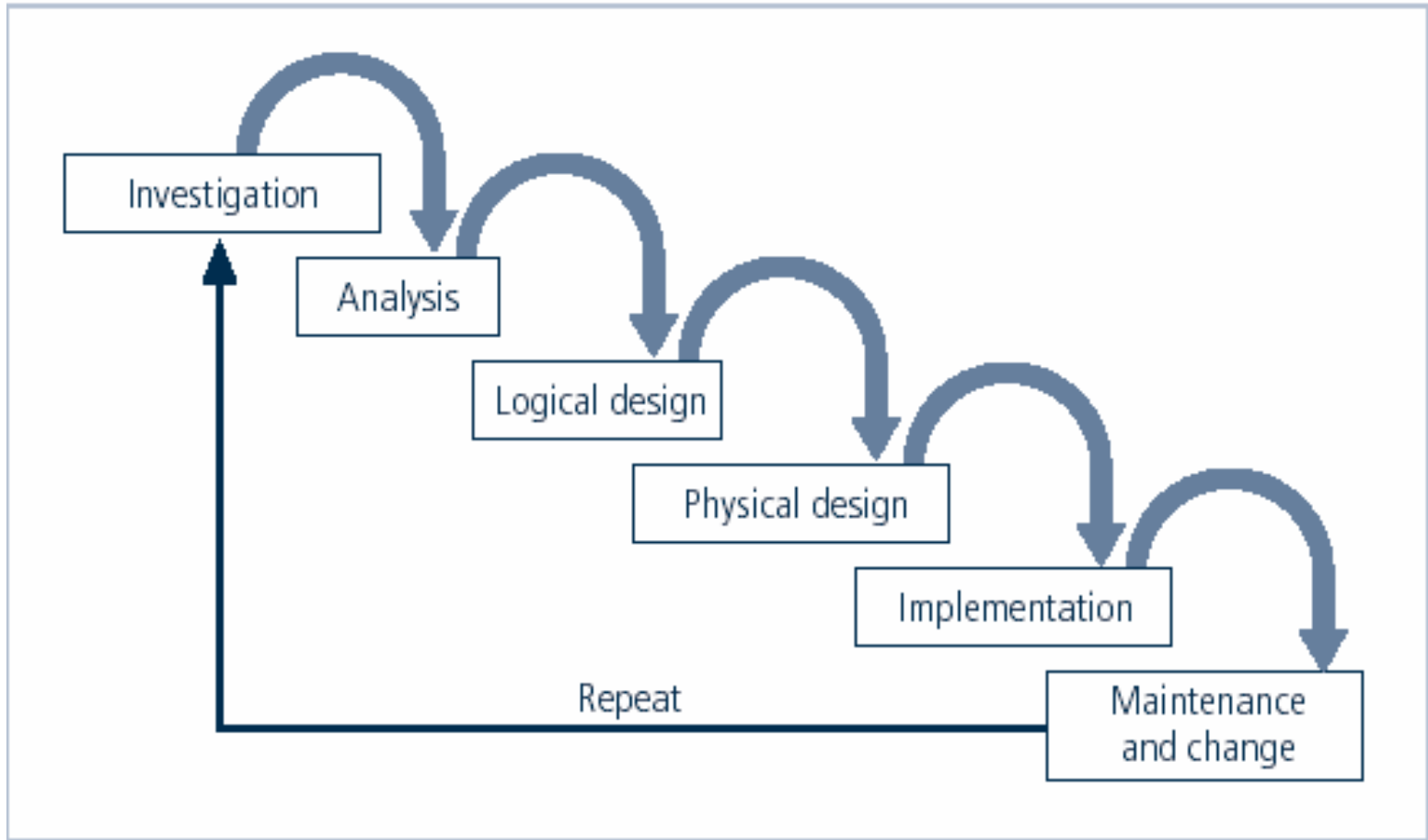


Approaches to Information Security Implementation: Top-Down Approach

- Initiated by upper management
 - Issue policy, procedures and processes
 - Dictate goals and expected outcomes of project
 - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle

The Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
 - ensures a rigorous process
 - avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases



SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints and scope of project are specified
- Preliminary cost-benefit analysis is developed
- At the end, feasibility analysis is performed to assesses economic, technical, and behavioral feasibilities of the process

Analysis

- Consists of assessments of the organization, status of current systems, and capability to support proposed systems
- Analysts determine what new system is expected to do and how it will interact with existing systems
- Ends with documentation of findings and update of feasibility analysis

Logical Design

- Main factor is business need; applications capable of providing needed services are selected
- Data support and structures capable of providing the needed inputs are identified
- Technologies to implement physical solution are determined
- Feasibility analysis performed at the end

Physical Design

- Technologies to support the alternatives identified and evaluated in the logical design are selected
- Components evaluated on make-or-buy decision
- Feasibility analysis performed; entire solution presented to end-user representatives for approval

Implementation

- Needed software created; components ordered, received, assembled, and tested
- Users trained and documentation created
- Feasibility analysis prepared; users presented with system for performance review and acceptance test

Maintenance and Change

- Consists of tasks necessary to support and modify system for remainder of its useful life
- Life cycle continues until the process begins again from the investigation phase
- When current system can no longer support the organization's mission, a new project is implemented

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

- Identifies process, outcomes, goals, and constraints of the project
- Begins with enterprise information security policy
- Organizational feasibility analysis is performed

Analysis

- Documents from investigation phase are studied
- Analyzes existing security policies or programs, along with documented current threats and associated controls
- Includes analysis of relevant legal issues that could impact design of the security solution
- The risk management task begins

Logical Design

- Creates and develops blueprints for information security
- Incident response actions planned:
 - Continuity planning
 - Incident response
 - Disaster recovery
- Feasibility analysis to determine whether project should continue or be outsourced

Physical Design

- Needed security technology is evaluated, alternatives generated, and final design selected
- At end of phase, feasibility study determines readiness of organization for project

Implementation

- Security solutions are acquired, tested, implemented, and tested again
- Personnel issues evaluated; specific training and education programs conducted
- Entire tested package is presented to management for final approval

Maintenance and Change

- Perhaps the most important phase, given the ever-changing threat environment
- Often, reparation and restoration of information is a constant duel with an unseen adversary
- Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve

Security Professionals and the Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

Senior Management

- Chief Information Officer (CIO)
 - Senior technology officer
 - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
 - Primarily responsible for assessment, management, and implementation of IS in the organization
 - Usually reports directly to the CIO

Information Security Project Team

- A number of individuals who are experienced in one or more facets of technical and non-technical areas:
 - Champion
 - Team leader
 - Security policy developers
 - Risk assessment specialists
 - Security professionals
 - Systems administrators
 - End users

Data Ownership

- Data Owner: responsible for the security and use of a particular set of information
- Data Custodian: responsible for storage, maintenance, and protection of information
- Data Users: end users who work with information to perform their daily jobs supporting the mission of the organization

Communities Of Interest

- Group of individuals united by similar interest/values in an organization
 - Information Security Management and Professionals
 - Information Technology Management and Professionals
 - Organizational Management and Professionals

Key Terms

- Access
- Asset
- Attack
- Control, Safeguard or Countermeasure
- Exploit
- Exposure
- Hacking
- Object
- Risk
- Security Blueprint
- Security Model
- Security Posture or Security Profile
- Subject
- Threats
- Threat Agent
- Vulnerability

Summary

- Information security is a “well-informed sense of assurance that the information risks and controls are in balance.”
- Computer security began immediately after first mainframes were developed
- Successful organizations have multiple layers of security in place: physical, personal, operations, communications, network, and information.

Summary

- Security should be considered a balance between protection and availability
- Information security must be managed similar to any major system implemented in an organization using a methodology like SecSDLC