Pengenalan Keamanan Informasi

Ahmad Almaarif

Pengenalan

- *Information security is a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Inovant (2002)*

- Keamanan informasi adalah sebuah jaminan bahwa ada keseimbangan antara risiko dan kendali pada sebuah informasi. Dengan kata lain, setiap risiko yang mungkin terjadi pada informasi memiliki kendali yang dapat diterapkan untuk mengurangi atau menghilangkan dampak risiko tersebut.

Sejarah singkat terkait keamanan informasi

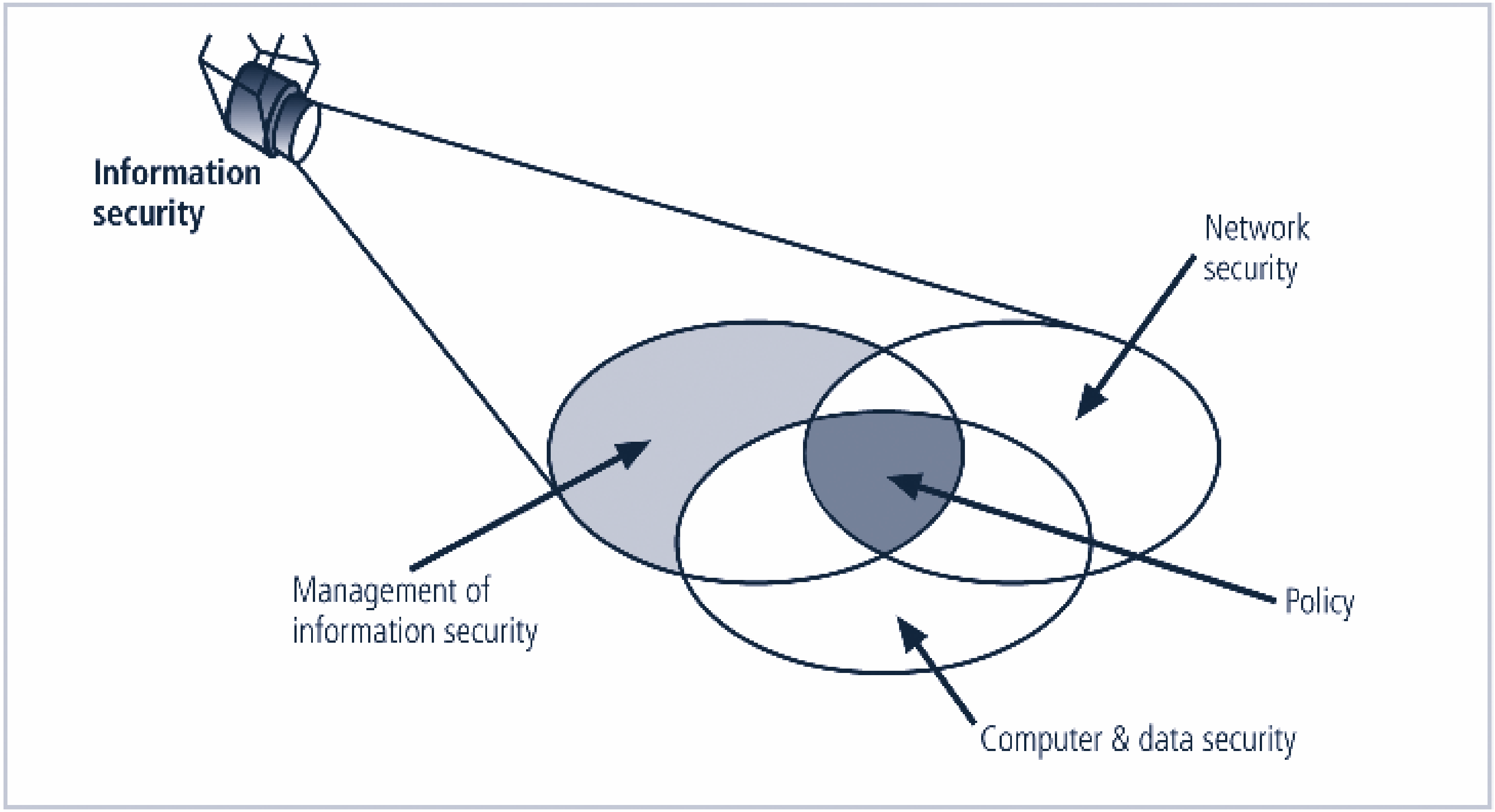
- Persandian dikembangkan pada masa Caesar di Romawi, dikenal dengan nama Caesar Cipher
- Pada era modern, persandian mulai berkembang pada masa Perang Dunia ke II, terkenal dengan mesin sandi yang bernama Enigma
- Berkembang mulanya di dunia militer
- Mulai dikenal luas oleh publik sejak Tim Berners-Lee mengembangkan World Wide Web (WWW)
- Keamanan Informasi berkembang sejalan dengan perkembangan teknologi mainframe, pc, laptop, smartphone, dan Internet of Things (IoT)

What is Security?

- *“The quality or state of being secure—to be free from danger”*
- Kondisi ketika bebas dari ancaman atau bahaya
- Setiap organisasi harus memiliki beberapa lapis tipe keamanan untuk menjamin keamanan organisasi tersebut:
    - Physical security
    - Personal security
    - Operations security
    - Communications security
    - Network security
    - Information security

Apa yang dimaksud dengan *Information Security*?

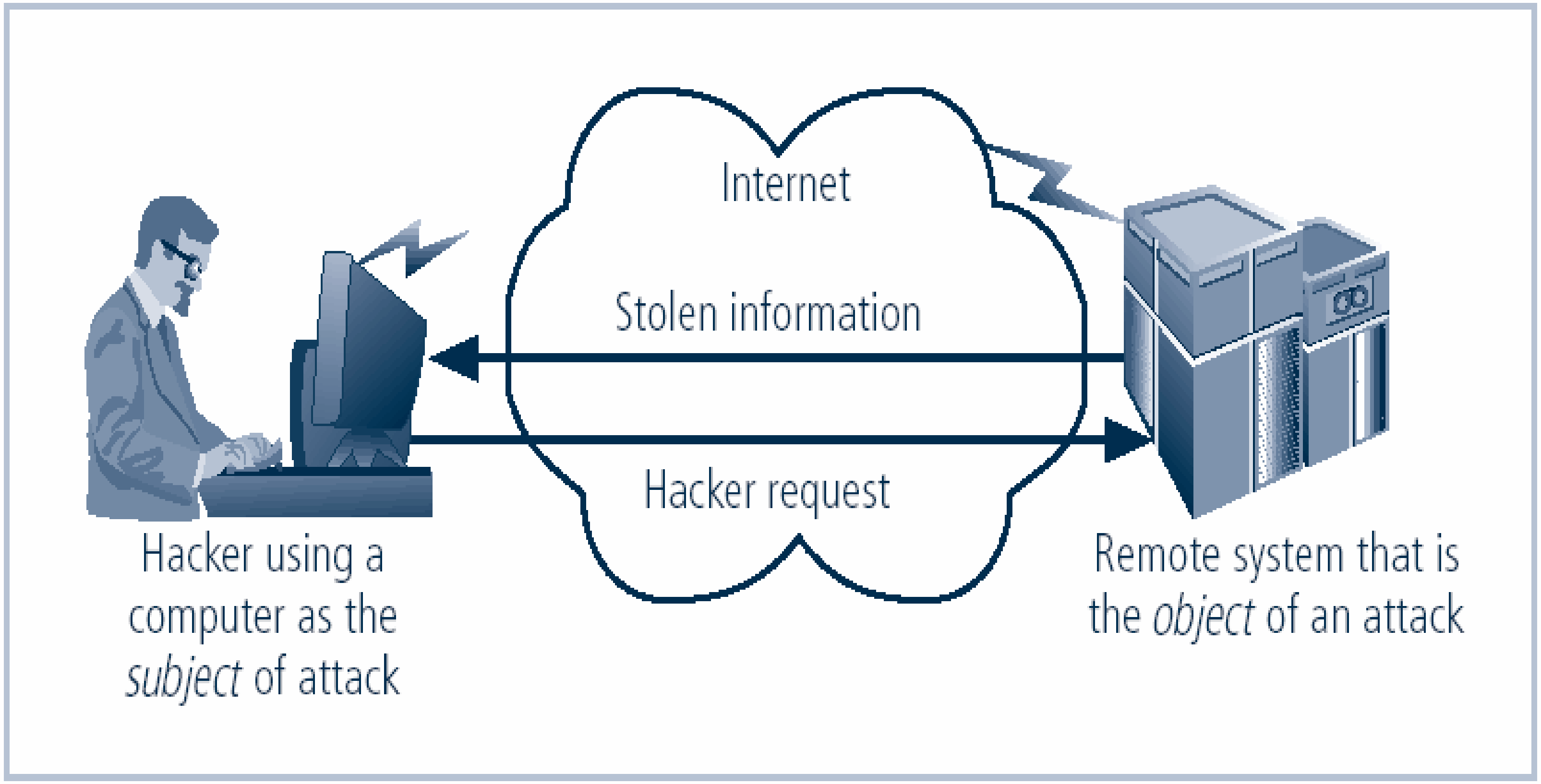
- Perlindungan informasi dan elemen kritikal, termasuk sistem dan hardware yang digunakan untuk pemrosesan, penyimpanan, dan transmisi informasi
- Keamanan informasi sering diilustrasikan dengan Segitiga C.I.A. (C.I.A. *Triangle*) yang merupakan singkatan dari Confidentiality, Integrity dan Availability



Components of Information Security

Komponen Sistem Informasi

- Sistem Informasi adalah serangkaian kumpulan software, hardware, data, people, prosedur, dan jaringan yang diperlukan untuk pemanfaatan informasi sebagai sumber daya organisasi


Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

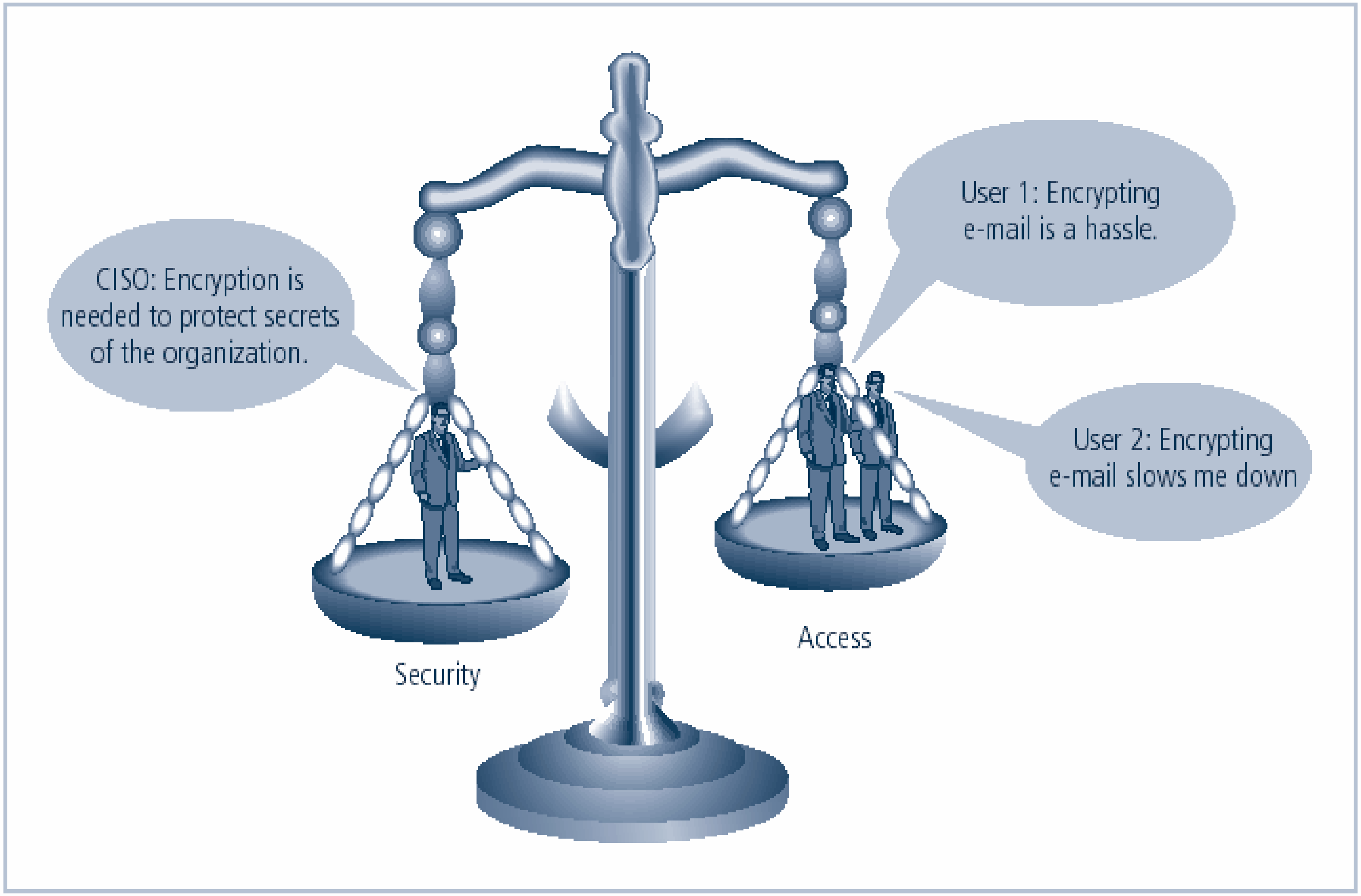
Computer as the Subject and Object of an Attack

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute

- Security should be considered balance between protection and availability

- To achieve balance, level of security must allow reasonable access, yet protect against threats


CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down
Security
Access

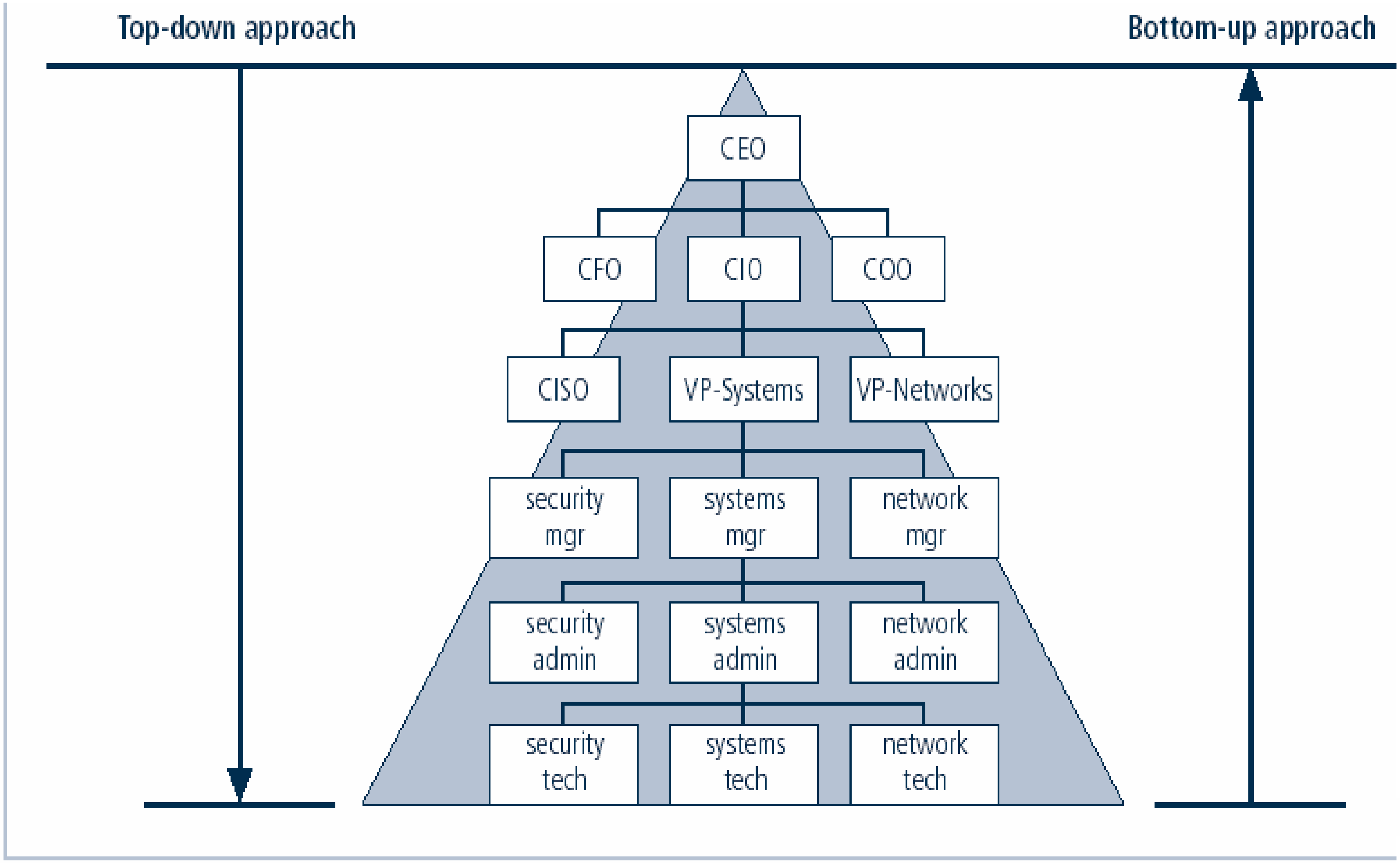
Balancing Information Security and Access

Pendekatan implementasi keamanan informasi: Bottom-Up Approach

- Grassroots effort: administrator sistem berinisiatif untuk meningkatkan keamanan sistem
- Key advantage: keahlian teknis sistem administrator
- Jarang berhasil, tidak memiliki dukungan:
  - Participant support
  - Organizational staying power

Pendekatan implementasi keamanan informasi : Top-Down Approach

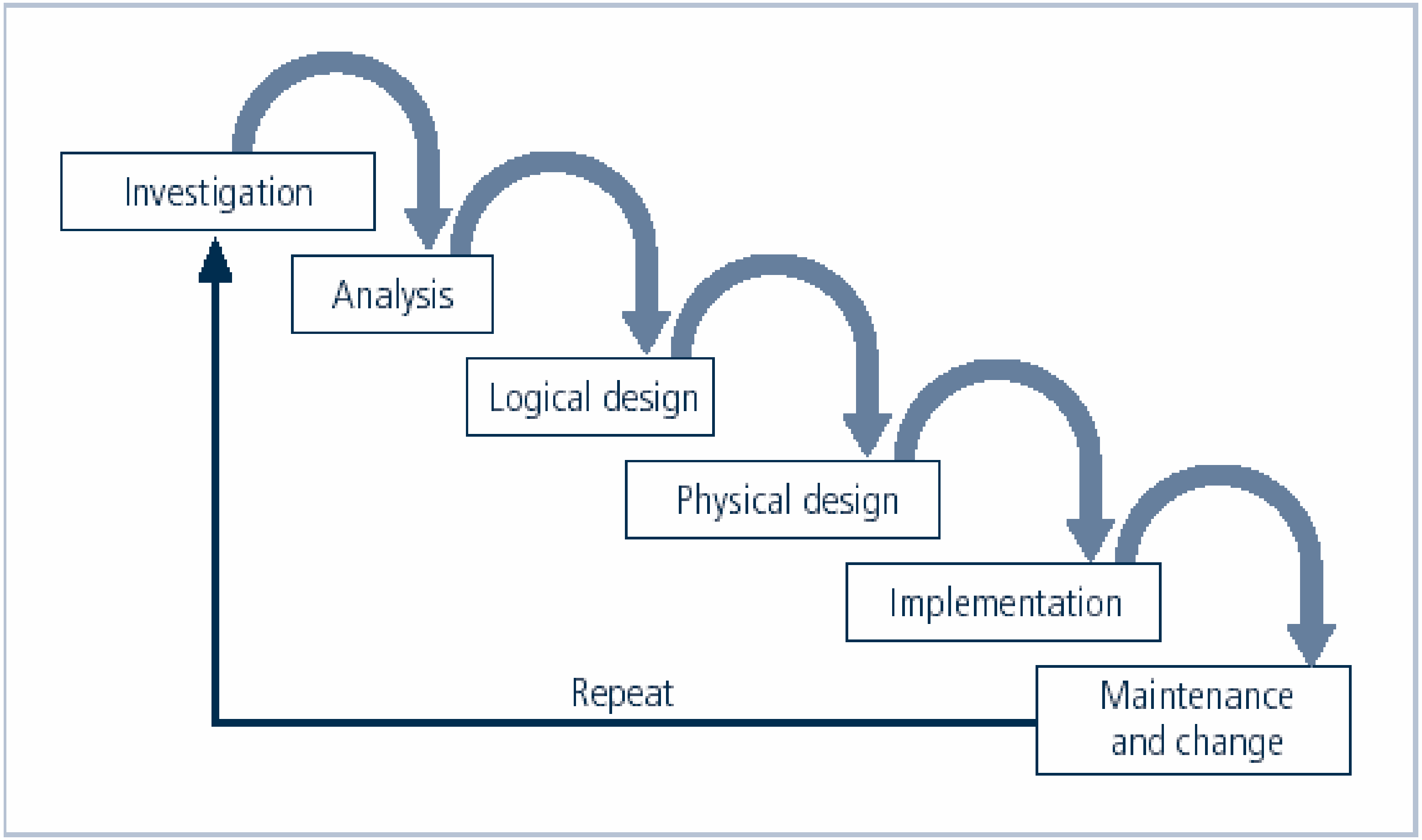
- Diinisiasi oleh upper management
  - Issue policy, procedures and processes
  - Dictate goals and expected outcomes of project
  - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle



Approaches to Information Security Implementation

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
- SSDLC 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

VTRC (Vulnerability, Threat, Risk and Control)

- Vulnerability : Kelemahan atau celah yang terdapat pada sistem atau organisasi dan terkait dengan keamanan informasi
- Threat : Ancaman yang dapat muncul terhadap sumber daya informasi maupun informasi itu sendiri; biasanya menyerang celah atau kelemahan yang ada
- Risk : Risiko yang muncul jika terjadi ancaman
- Control : Tindakan pengendalian risiko jika terjadi ancaman

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