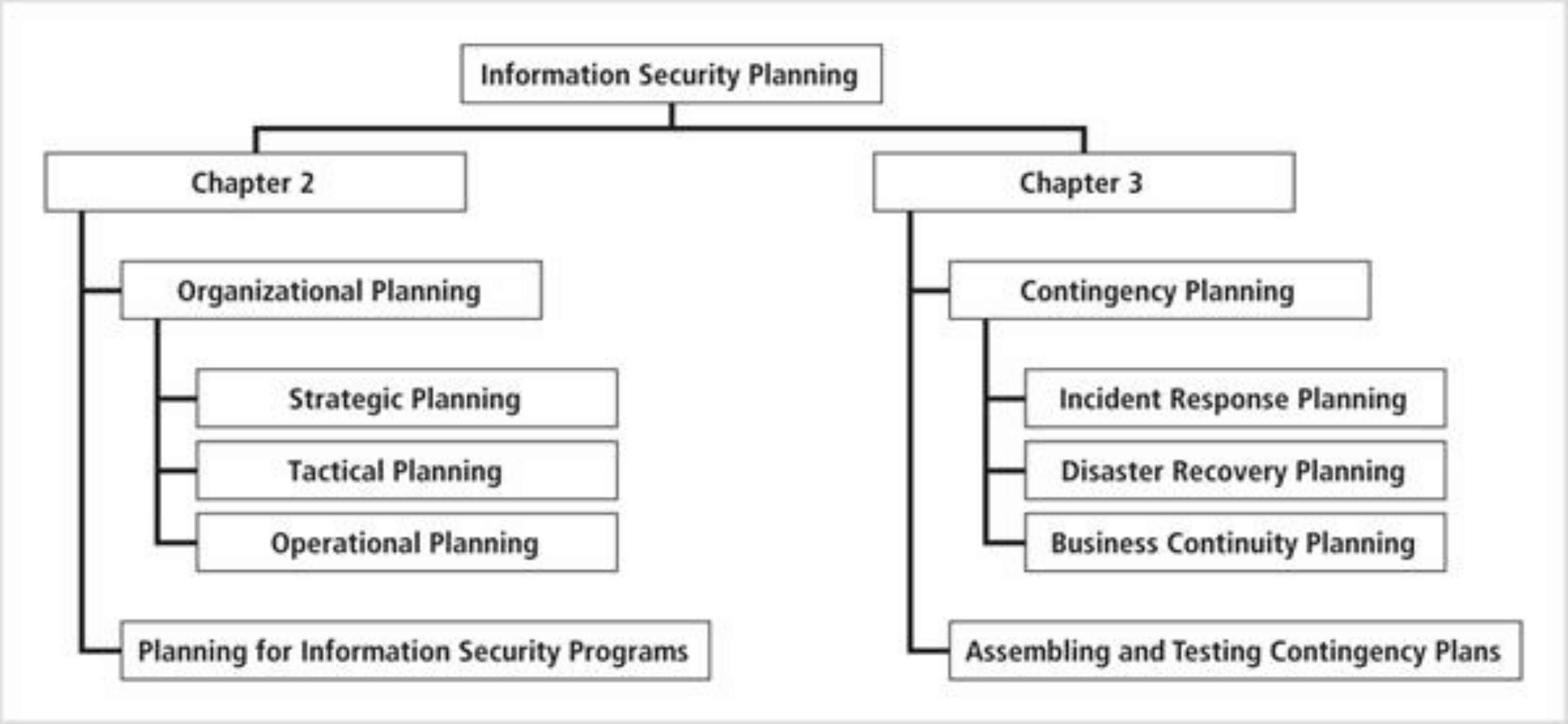
CSIT988
Security, Ethics and Professionalism
Week 3: Planning for Security

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Information Security Planning



- Information Security Planning
  - Chapter 2
    - Organizational Planning
      - Strategic Planning
      - Tactical Planning
      - Operational Planning
    - Planning for Information Security Programs
  - Chapter 3
    - Contingency Planning
      - Incident Response Planning
      - Disaster Recovery Planning
      - Business Continuity Planning
    - Assembling and Testing Contingency Plans

- The process that develops, creates, and implements strategies for the accomplishment of objectives
- Planning is the dominant means of managing resources in modern organizations
- Planning provides direction for the organization's future
- Top-down process:
    - ➢ leadership chooses the direction and initiatives
    - ➢ begins with the general, ends with the specific

The Role of Planning

Planning involves many interrelated groups and organizational processes

- Employees, management, stockholders, outside stakeholders.
- Physical and technological environment, political and legal environment, competitive environment.

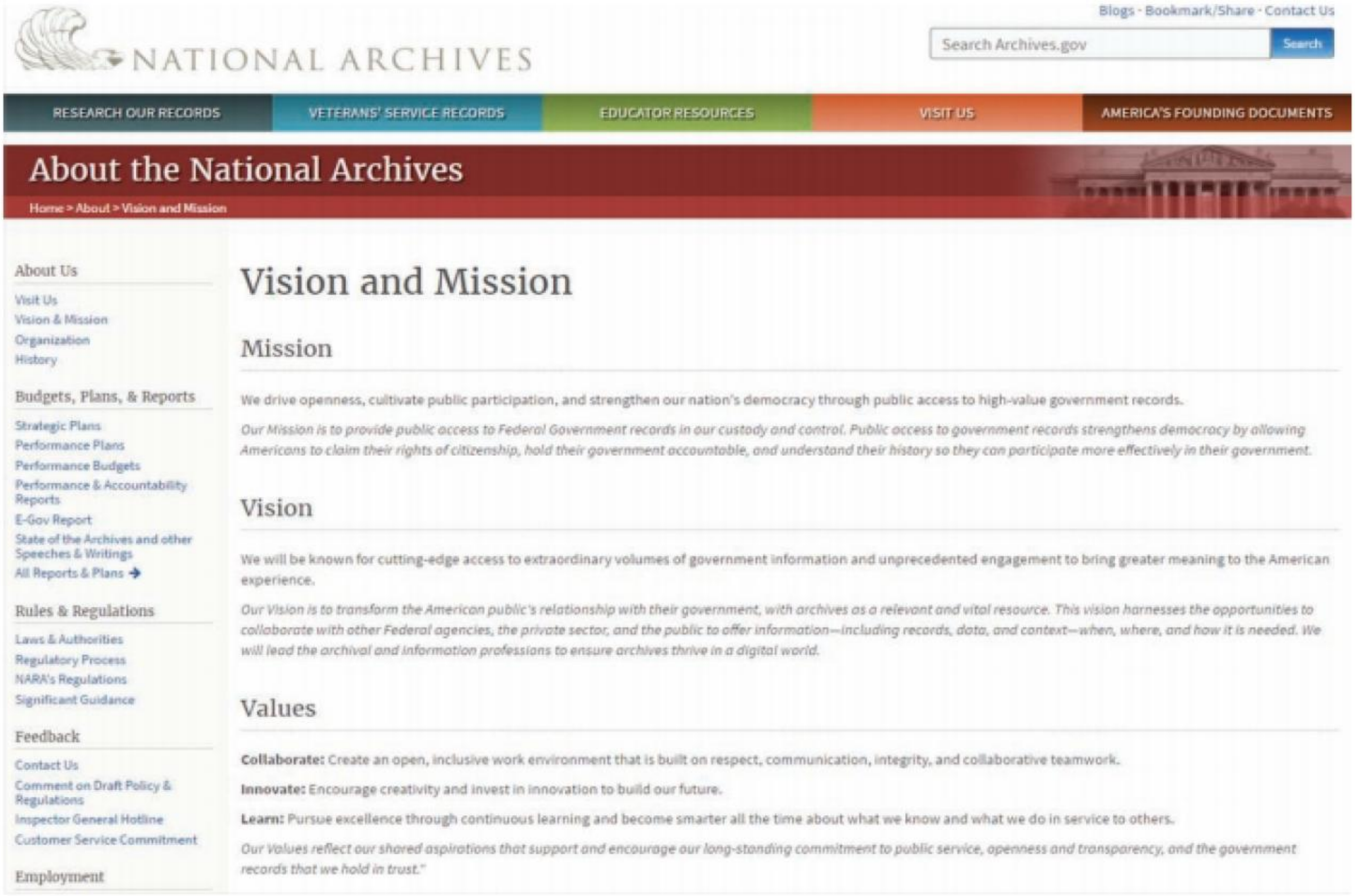
Effective InfoSec planners should understand organizational planning

- Members of the InfoSec community of interest use the same planning processes and methodologies as the other two communities of interest.

Precursors to Planning

To develop and implement effective planning, first create foundational documents

- Values statement
- Vision statement
- Mission statement
- Strategy


Blogs · Bookmark/Share · Contact Us
Search Archives.gov
Search
NATIONAL ARCHIVES
RESEARCH OUR RECORDS
VETERANS' SERVICE RECORDS
EDUCATOR RESOURCES
VISIT US
AMERICA'S FOUNDING DOCUMENTS
About the National Archives
Home > About > Vision and Mission
About Us
Visit Us
Vision & Mission
Organization
History
Budgets, Plans, & Reports
Strategic Plans
Performance Plans
Performance Budgets
Performance & Accountability Reports
E-Gov Report
State of the Archives and other Speeches & Writings
All Reports & Plans
Rules & Regulations
Laws & Authorities
Regulatory Process
NARA's Regulations
Significant Guidance
Feedback
Contact Us
Comment on Draft Policy & Regulations
Inspector General Hotline
Customer Service Commitment
Employment

Vision and Mission

Mission

We drive openness, cultivate public participation, and strengthen our nation's democracy through public access to high-value government records.

Our Mission is to provide public access to Federal Government records in our custody and control. Public access to government records strengthens democracy by allowing Americans to claim their rights of citizenship, hold their government accountable, and understand their history so they can participate more effectively in their government.

Vision

We will be known for cutting-edge access to extraordinary volumes of government information and unprecedented engagement to bring greater meaning to the American experience.

Our Vision is to transform the American public's relationship with their government, with archives as a relevant and vital resource. This vision harnesses the opportunities to collaborate with other Federal agencies, the private sector, and the public to offer information—including records, data, and context—when, where, and how it is needed. We will lead the archival and information professions to ensure archives thrive in a digital world.

Values

Collaborate: Create an open, inclusive work environment that is built on respect, communication, integrity, and collaborative teamwork.

Innovate: Encourage creativity and invest in innovation to build our future.

Learn: Pursue excellence through continuous learning and become smarter all the time about what we know and what we do in service to others.

Our Values reflect our shared aspirations that support and encourage our long-standing commitment to public service, openness and transparency, and the government records that we hold in trust."

Values Statement

- One of the first positions that management must articulate

- Establishes a formal set of organizational principles and qualities, as well as benchmarks for measuring behavior against these published values
    - ➢ Makes organization’s conduct standards clear to employees and the public

NSW Department of Education – Values

Excellence

- We have high expectations and we continually seek to improve ourselves and our work.
- We strive to excel and invite the best ideas from everyone in and outside the department.
- We use and share evidence, research and data to underpin policy and practice.
- We welcome collaboration and learning with others.

Equity

- We ensure that every student has access to high quality public education.
- We respect diversity and the views and contributions of others.
- We treat people fairly.

Accountability

- We take responsibility for decisions and outcomes.
- We allocate and use resources efficiently and effectively.
- We monitor and review performance to drive improvement.

Trust

- We build relationships based on transparency, honesty and mutual respect.
- We support each other.
- We respect others' expertise, experience and points of view, and listen with an open mind.

Integrity

- We act professionally with honesty and consistency.
- We communicate clear expectations.
- We are transparent with information and our decisions.

Service

- We are flexible, innovative, responsive and reliable.
- We provide coordinated and aligned services to enhance teaching and learning.
- We work openly in partnership with parents, communities and organisations.

Vision Statement

- The vision statement expresses what the organization wants to become
- Vision statements should be ambitious
  - ➢ UOW's 2030 Vision (https://www.uow.edu.au/about/2030vision/)

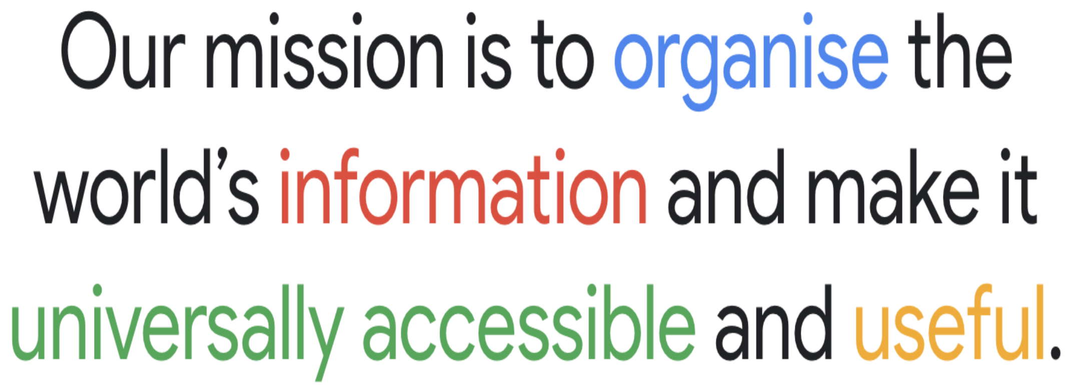
> *"We inspire a better future through education, research and partnership.*
> *We are grounded by our intellectual openness, excellence and dedication, empowerment and academic freedom, mutual respect and diversity, recognition and performance. These are our values.*
> *They have navigated us through our first 40 years and will strengthen us as we create our future."*

  - ➢ NSW Department of Education's Vision

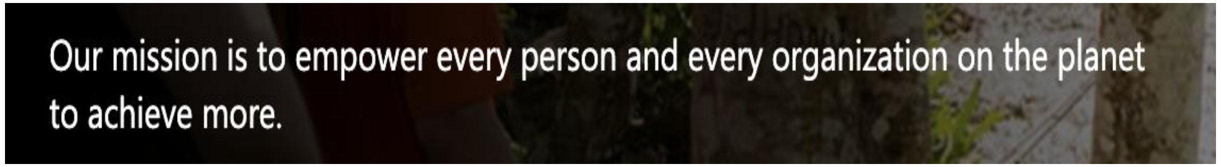
To be Australia's best education system and one of the finest in the world.

Mission Statement

- ➢ Declares the business of the organization and its intended areas of operations
- ➢ A mission statement should be concise, reflect both internal and external operations, and be robust enough to remain valid for a period of four to six years. It must explain what the organization does and for whom.
- ➢ **Examples:** Google and Microsoft



Our mission is to organise the world's information and make it universally accessible and useful.



Our mission is to empower every person and every organization on the planet to achieve more.

Mission, Vision and Values Statement

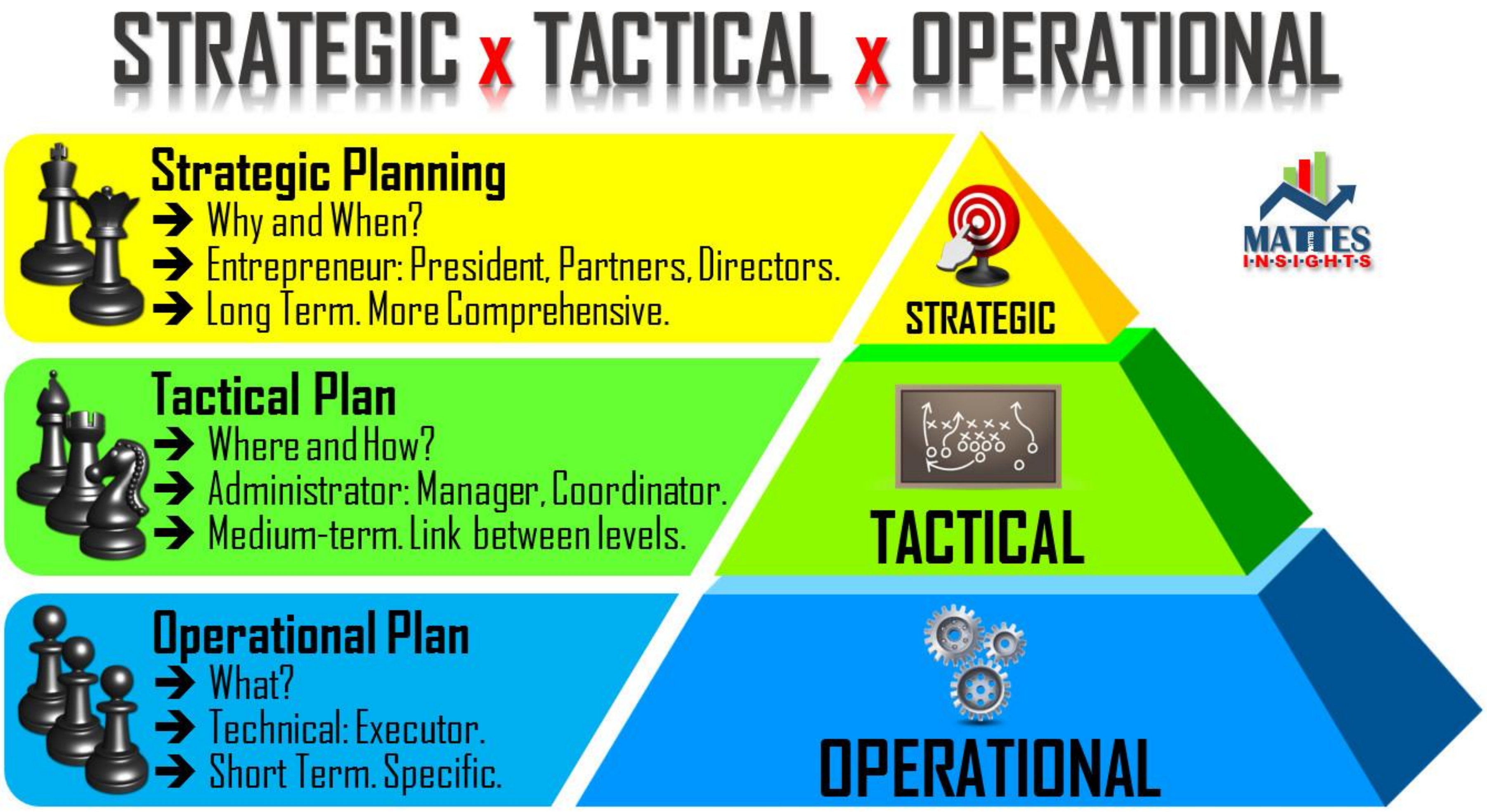
- The mission statement is the follow-up to the vision statement. If the vision statement states where the organization wants to go, the mission statement describes how it wants to get there.

- Taken together, the mission, vision, and values statements provide the philosophical foundation for planning and guide the creation of the strategic plan.

- Strategy is the basis for long-term direction

- Strategic planning guides organizational efforts
  - Focuses resources on clearly defined goals
  - From ***Encyclopædia Britannica*** (https://www.britannica.com/topic/strategic-planning-organization)

  "… disciplined effort to produce decisions and actions that shape and guide an organization's purpose and activities, particularly with regard to the future."



STRATEGIC x TACTICAL x OPERATIONAL

Strategic Planning

- ➔ Why and When?
- ➔ Entrepreneur: President, Partners, Directors.
- ➔ Long Term. More Comprehensive.

Tactical Plan

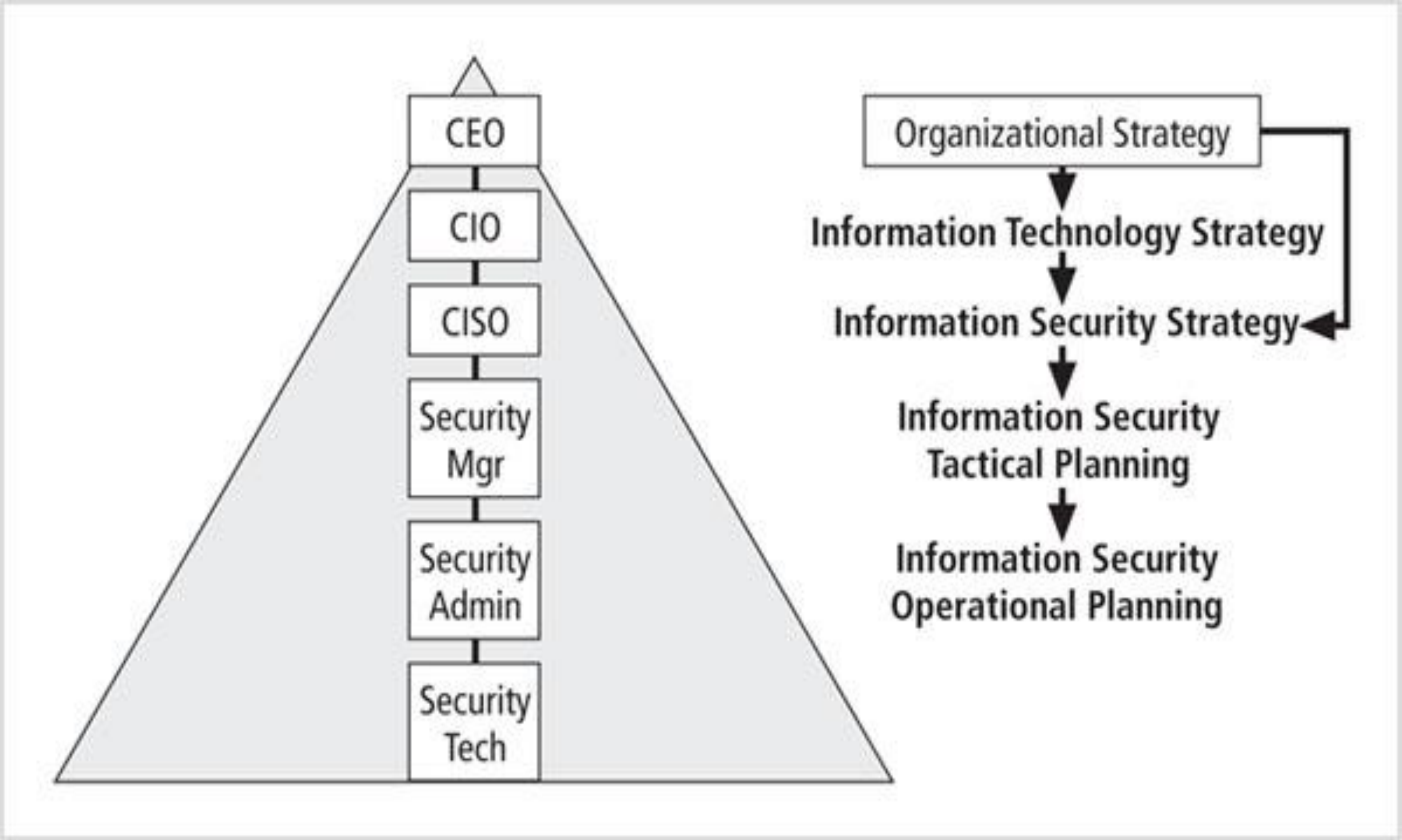
- ➔ Where and How?
- ➔ Administrator: Manager, Coordinator.
- ➔ Medium-term. Link between levels.

Operational Plan

- ➔ What?
- ➔ Technical: Executor.
- ➔ Short Term. Specific.

- Strategic plans formed at the highest levels are translated into more specific strategic plans for intermediate layers of management.
- These plans are then converted into tactical planning for supervisory managers and eventually provide direction for the operational plans

Top-down Strategic Planning


CEO
CIO
CISO
Security Mgr
Security Admin
Security Tech
Organizational Strategy
Information Technology Strategy
Information Security Strategy
Information Security Tactical Planning
Information Security Operational Planning

CEO: Chief Executive Officers
CISO: Chief Information Security Officers

CIO: Chief Information Officers
COO: Chief Operations Officers

Creating a Strategic Plan

- An organization develops a general strategy
  - ➢ Then creates specific strategic plans for major divisions
  - ➢ Each level or division translates those objectives into more specific objectives for the level below

Providing the highest quality health care service in the industry.

Creating a Strategic Plan

- The executive team must define individual managerial responsibilities
- E.g., to respond to the CEO,

CIO

Providing high-level health care information service in support of the highest quality health care service in the industry.

COO

Providing the highest quality medical services.

CISO

Ensuring that quality health care information services are provided securely and in compliance with all local, state, and federal information processing, information security, and privacy statutes, including HIPAA.

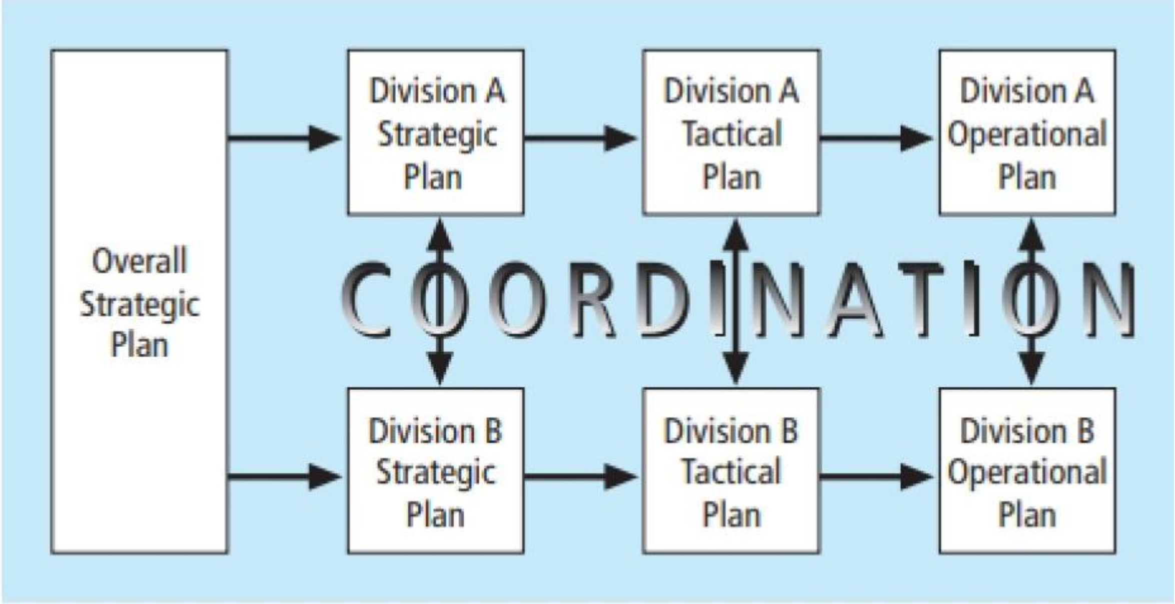
*** HIPAA: Health Insurance Portability and Accountability Act (of the US).**

Planning Levels

- Strategic goals are translated into tasks with specific, measurable, attainable, relevant and time-bound (SMART) objectives.

- Strategic planning then begins a transformation from general to specific objectives. Strategic plans are used to create tactical plans and then operational plans.

S
Specific
M
Measurable
A
Attainable
R
Relevant
T
Time-bound


Overall Strategic Plan
Division A Strategic Plan
Division A Tactical Plan
Division A Operational Plan
COORDINATION
Division B Strategic Plan
Division B Tactical Plan
Division B Operational Plan

Planning Levels

- Shorter focus (1y—5y) than strategic planning
- Breaks applicable strategic goals into a series of incremental objectives, each should be specific and have a delivery date.
- Budgeting, resource allocation, personnel are critical components for tactical plan
- Includes project plans, resource acquisition planning documents, project budgets, project reviews, and regular reports.
- Used to organize, prioritize and acquire resources to support the overall strategic plan.

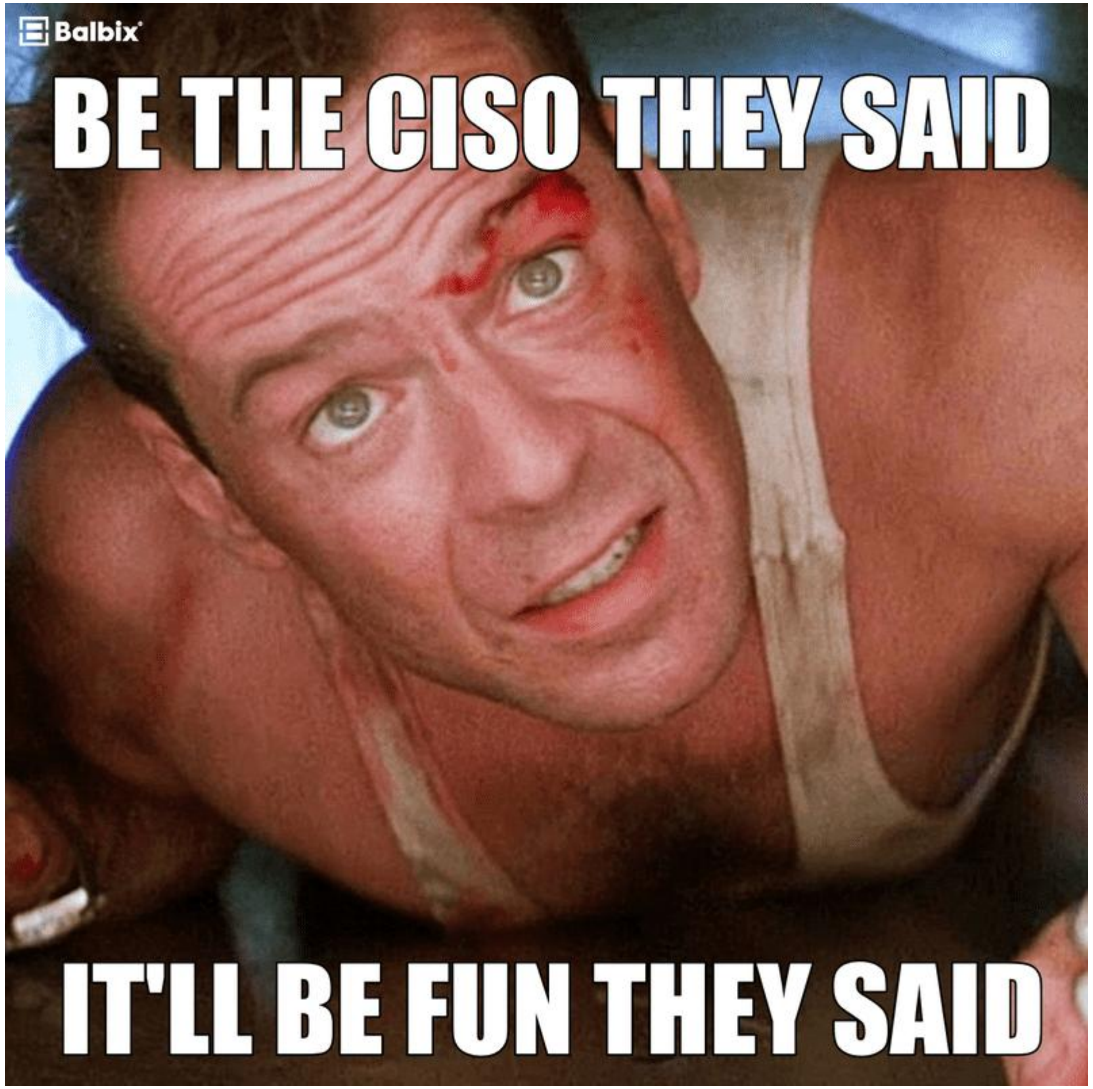
Planning Levels

Operational Planning

- Used by managers and employees to organize the ongoing, day-to-day performance of tasks
- Includes clearly identified coordination activities across department boundaries such as: communications requirements, weekly meetings, summaries, progress reports, and associated tasks.

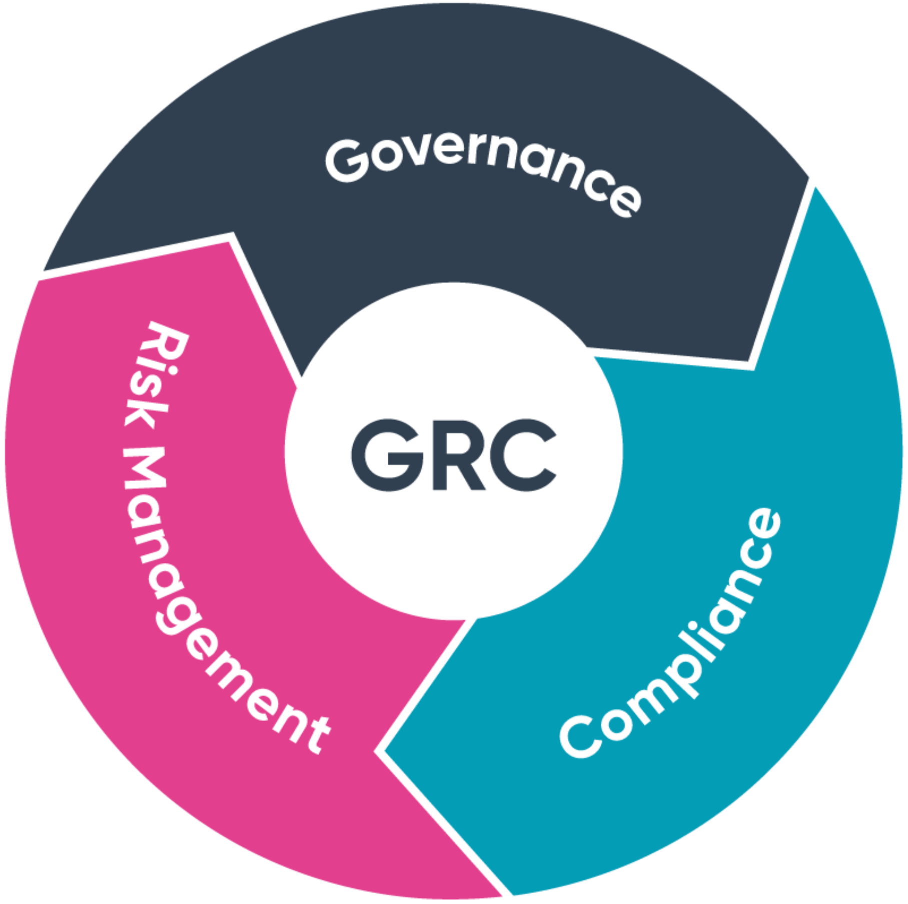
Planning and the CISO

- The first priority of the CISO should be the structure of a strategic plan
- Elements of a strategic plan
  - ➢ Executive summary
  - ➢ Mission and vision statements
  - ➢ Organizational profile and history
  - ➢ Strategic issues and core values
  - ➢ Program goals and objectives
  - ➢ Management/operations goals and objectives
  - ➢ Appendices (optional)



Information Security Governance

- Strategic planning and corporate responsibility are accomplished by using governance, risk management, and compliance (GRC).
- GRC integrate them into one holistic approach for executive-level strategic planning and management.
- Governance of InfoSec is a strategic planning responsibility
  - ➢ Importance has grown in recent years
- InfoSec objectives must be addressed at the highest levels of an organization's management team



Information Security Governance

- **ITGI: InfoSec governance includes**
  - ➢ Providing strategic direction
  - ➢ Establishing objectives
  - ➢ Measuring progress toward those objectives
  - ➢ Verifying that risk management practices are appropriate
  - ➢ Validating that the organization's assets are used properly

ISACA®

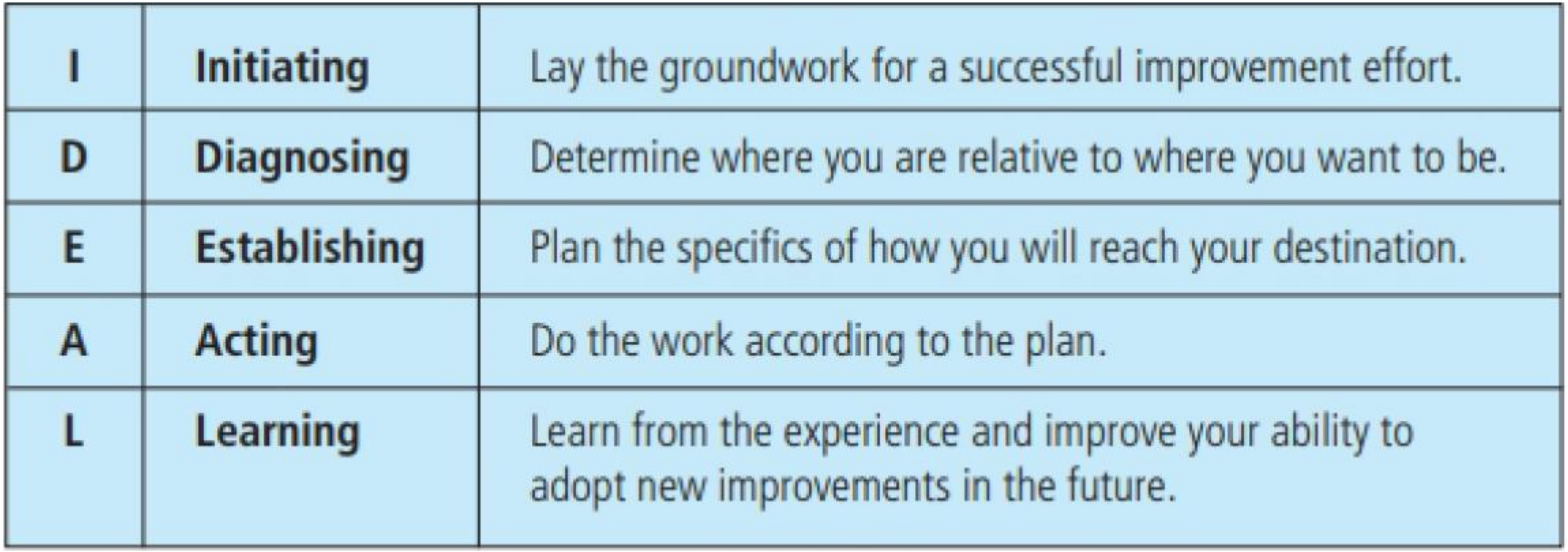
IT GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

Desired Outcomes

- **Outcomes of information security governance**
  - Strategic alignment of information security with business strategy to support organizational objectives
  - Risk management to reduce impacts on information resources
  - Resource management with efficient use of information security knowledge and infrastructure
  - Performance measurement to ensure that objectives are achieved
  - Value delivery by optimizing information security investments in support of organizational objectives

Implementing Information Security Governance

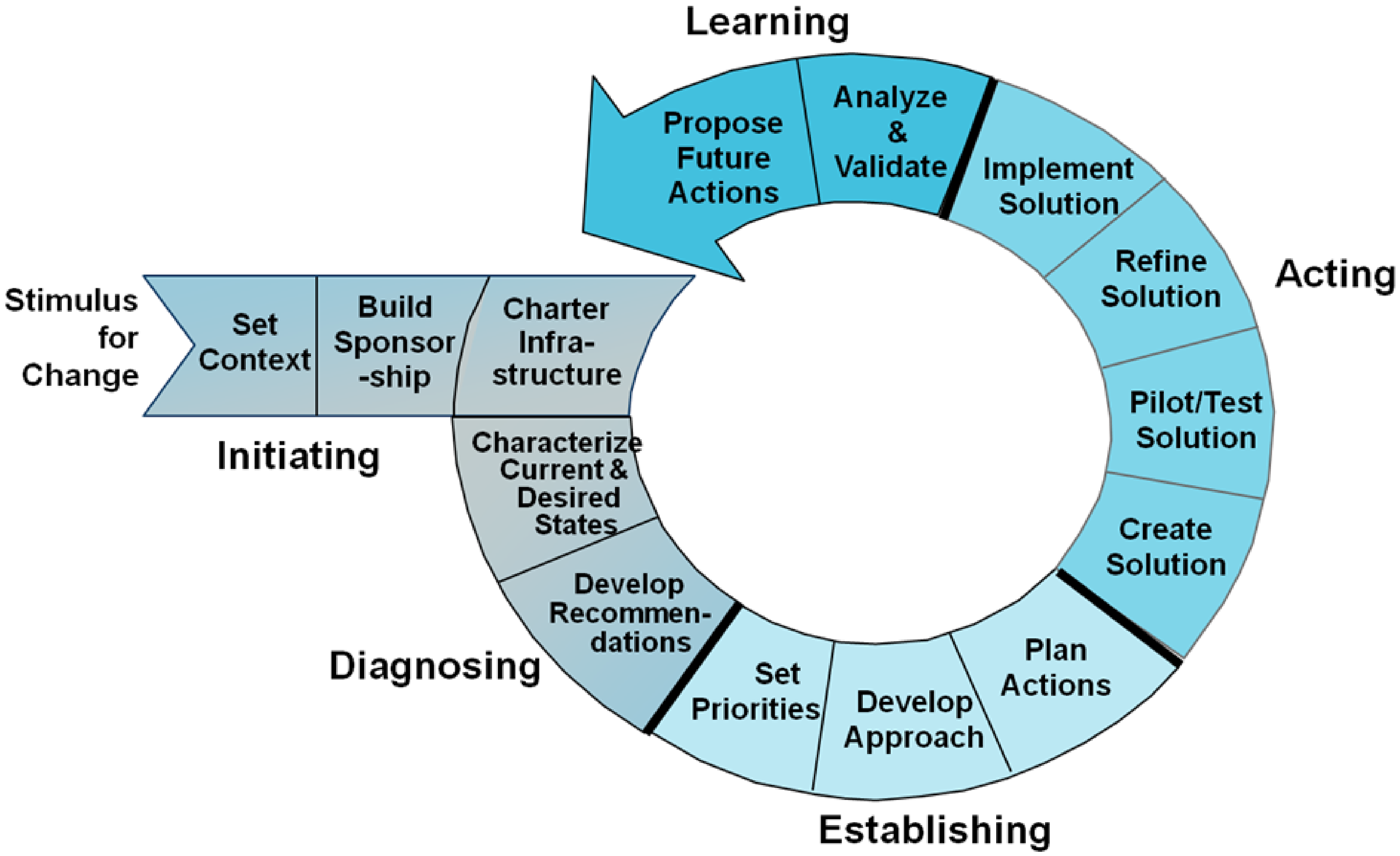


I	Initiating	Lay the groundwork for a successful improvement effort.
D	Diagnosing	Determine where you are relative to where you want to be.
E	Establishing	Plan the specifics of how you will reach your destination.
A	Acting	Do the work according to the plan.
L	Learning	Learn from the experience and improve your ability to adopt new improvements in the future.

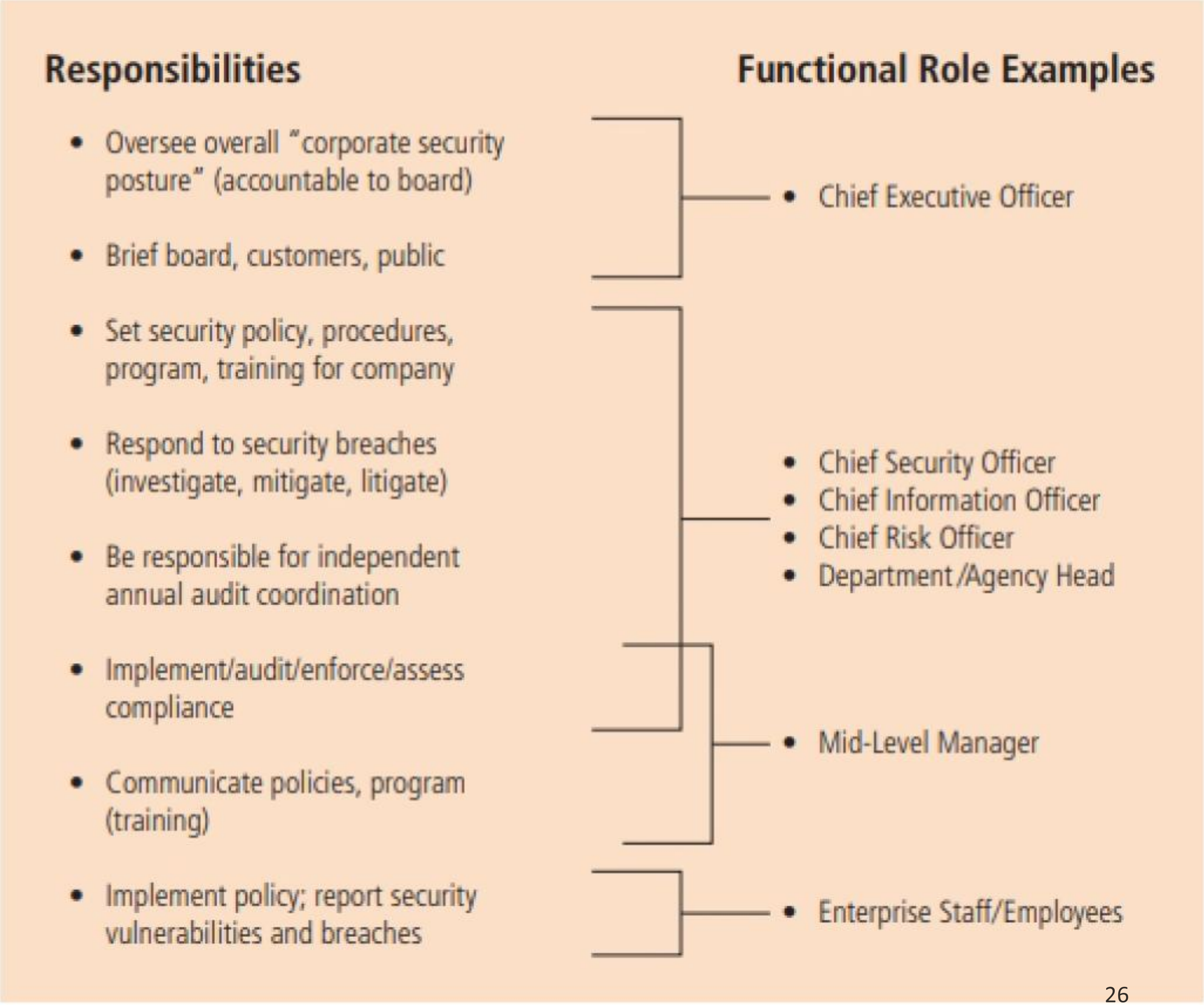
The IDEAL model

by CGTF (Corporate Governance Task Force)

The IDEAL Model



InfoSec Governance Responsibilities



Responsibilities

- Oversee overall "corporate security posture" (accountable to board)
- Brief board, customers, public
- Set security policy, procedures, program, training for company
- Respond to security breaches (investigate, mitigate, litigate)
- Be responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement policy; report security vulnerabilities and breaches

Functional Role Examples

- Chief Executive Officer
- Chief Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department /Agency Head
- Mid-Level Manager
- Enterprise Staff/Employees

Planning For Information Security Implementation

Roles of the CIO and CISO

- Translating overall strategic plan into tactical and operational information security plans
- The CISO plays a more active role in the development of the planning details than does the CIO

CISO Job Description (example)

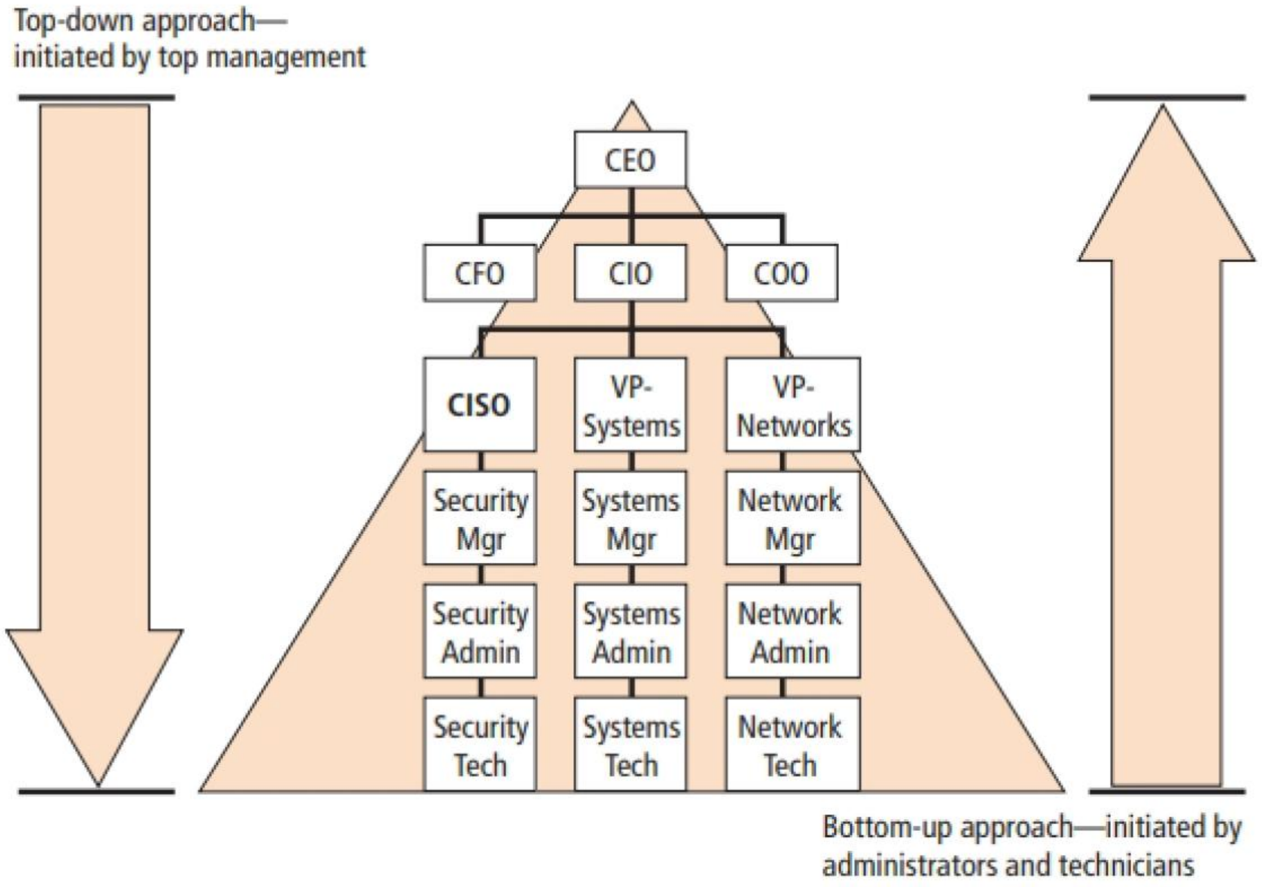
- Creates a strategic information security plan with a vision for the future of information security
- Understands the fundamental business activities and suggests appropriate information security solutions to protect these activities
- Develops action plans, schedules, budgets, and status reports

Planning For Information Security Implementation

Implementation can begin after plan has been translated into IT and InfoSec objectives and tactical and operational plans

Methods of implementation

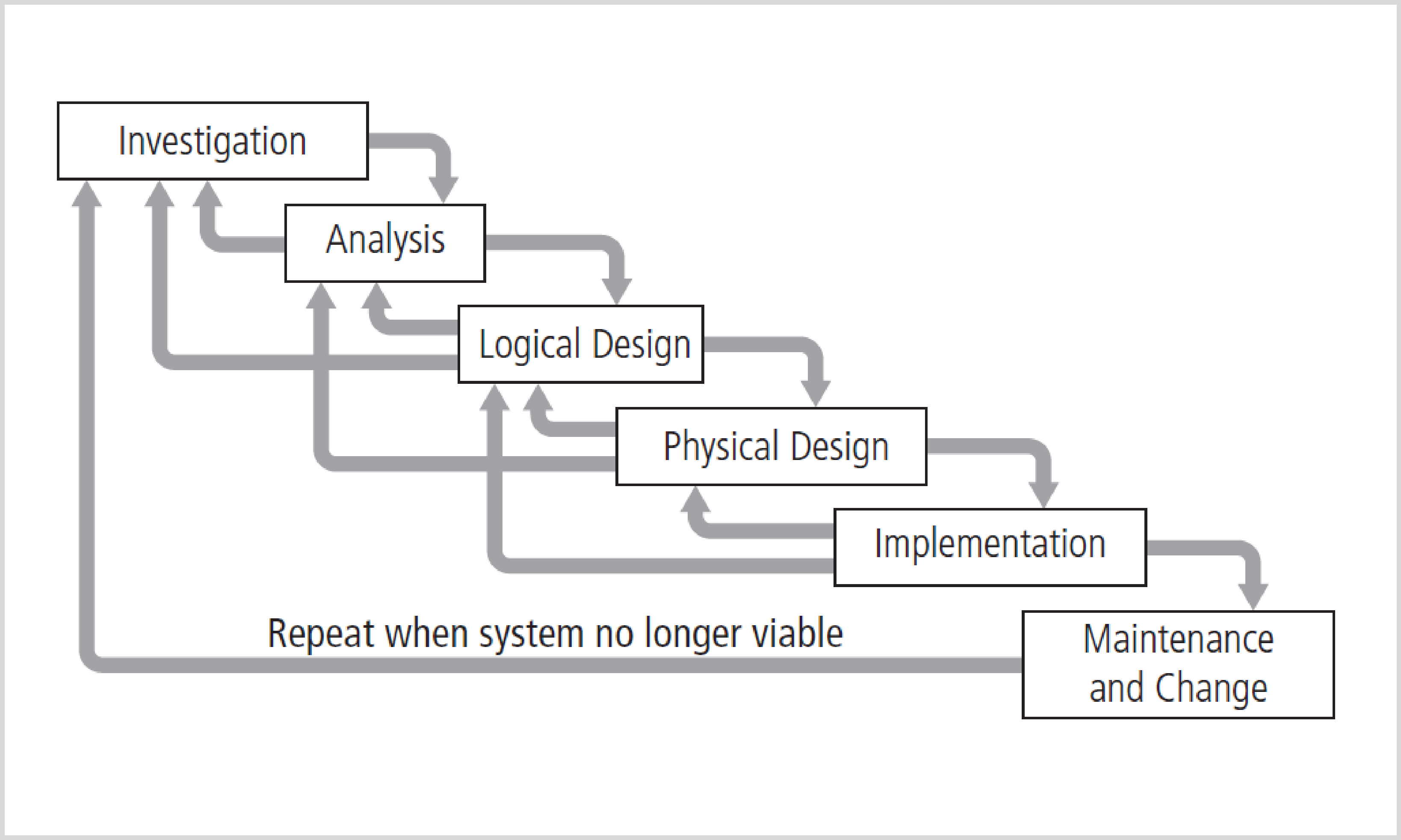
- Bottom-up: use technical expertise of the individual. Lack of coordination
- Top-down: high-level managers provide resources, give direction, issue policies, indicate goals and outcomes, determine responsibilities
- System development life cycle (SDLC)



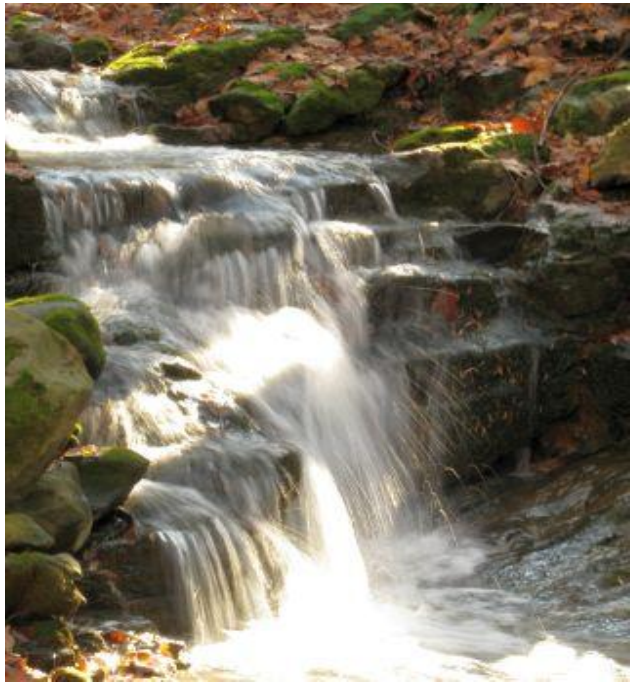
- **SDLC**
  - A methodology for the design and implementation of information systems.
  - SDLC-based projects may be initiated by events or planned.
  - End of each phase: review to determine if the project should be continued, discontinued, outsourced, or postponed.

- **SecSDLC: A variation of SDLC, used to create a comprehensive security posture**
  - Identification of specific threats and the risks they represent
  - Design and implementation of specific controls to counter those threats and manage risks posed to the organization

Security Systems Development Life Cycle



A waterfall model



Investigation in the SecSDLC

- Phase begins with directive from management specifying the process, outcomes, and goals of the project and its budget
- Frequently begins with the affirmation or creation of security policies
- Teams assembled to analyze problems, define scope, specify goals and identify constraints
- Feasibility analysis determines whether the organization has the resources and commitment to conduct a successful security analysis and design

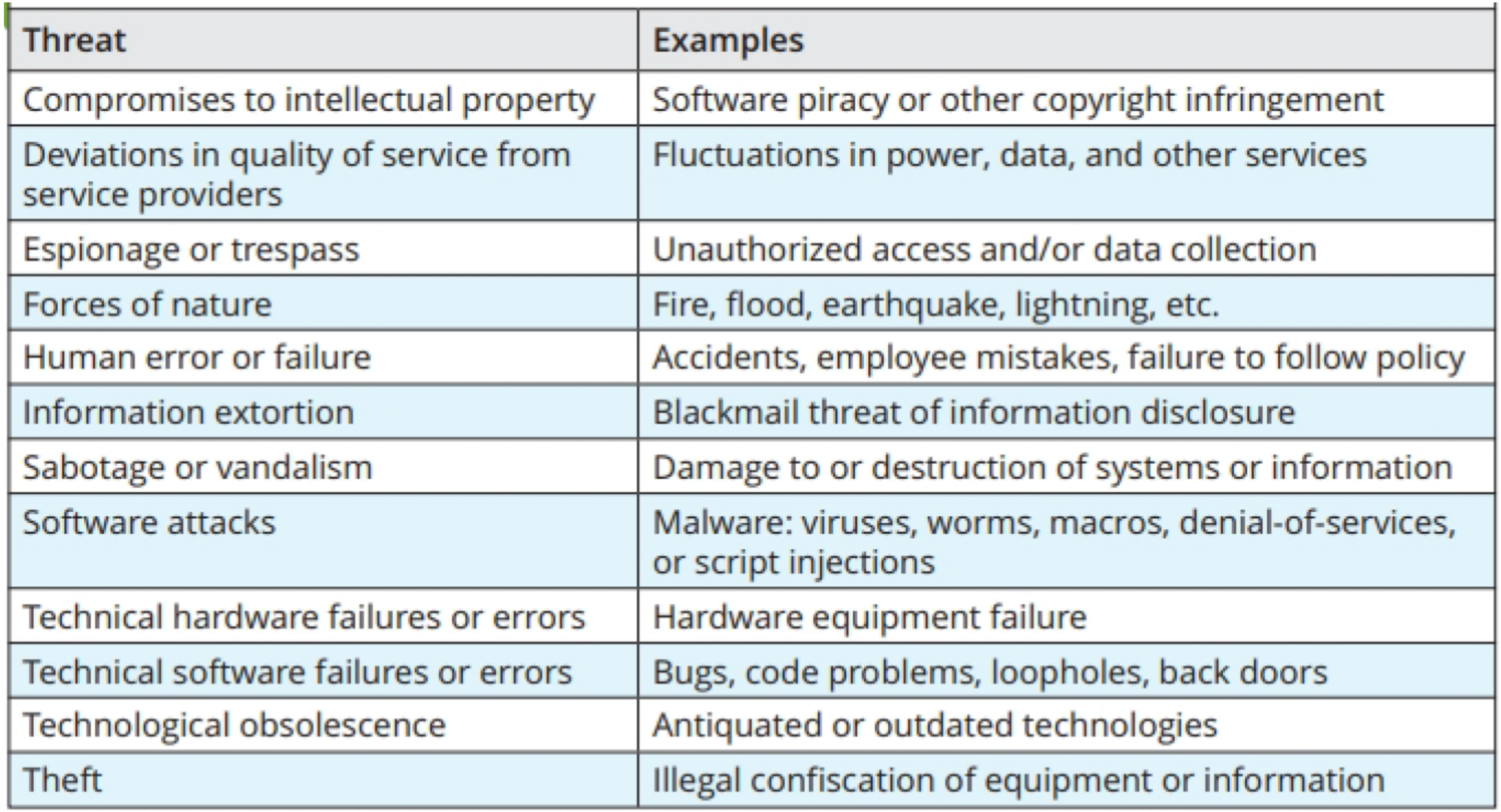
Analysis in the SecSDLC

- Analysis of existing security policies and programs, along with known threats and current controls
- Analysis of legal issues that could affect the design of the security solution
- Risk management begins in this stage: The process of identifying, assessing, and evaluating the levels of risk facing the organization

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." -- ***Sun Tzu (The Art of War)***

Threats to information security

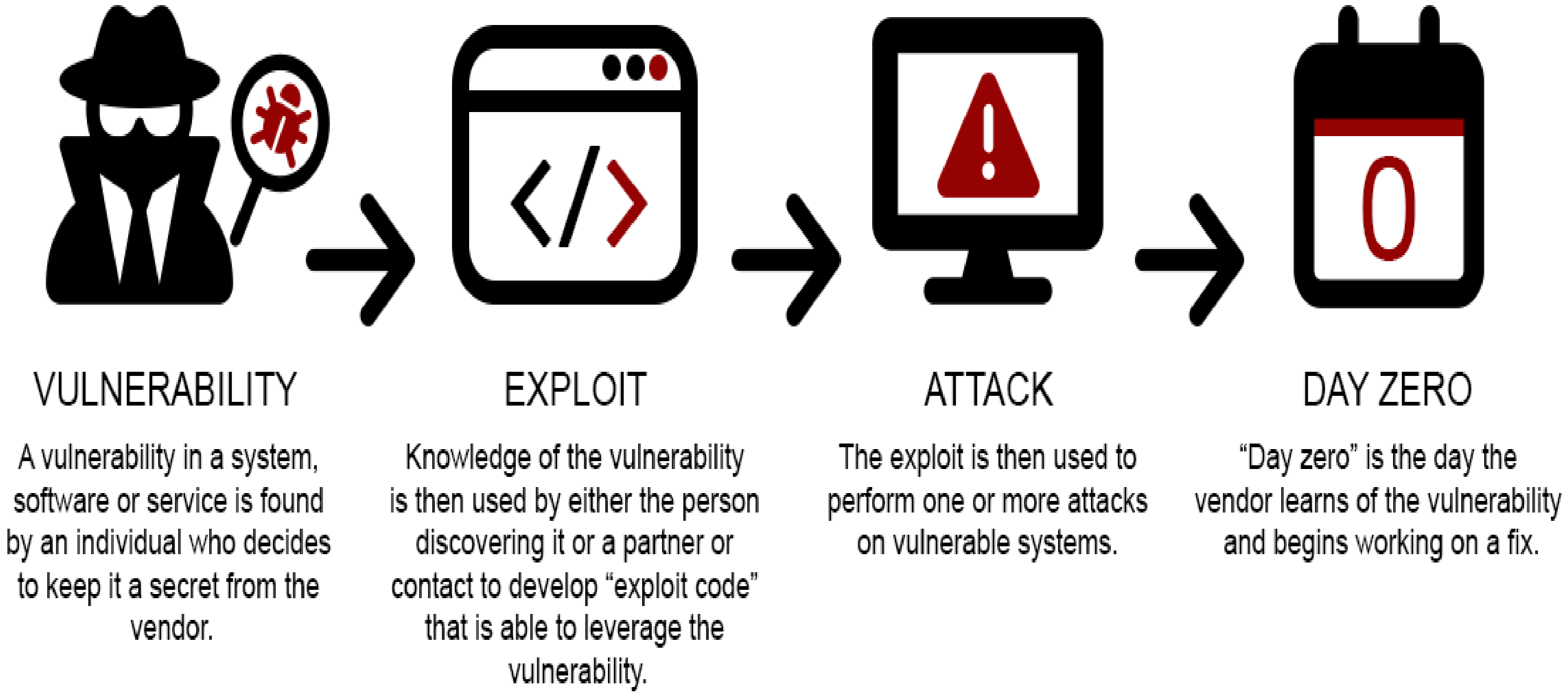
Threat: an object, person, or other entity that represents a constant danger to an asset.



Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, back doors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Source: CACM.

- **Attack:** A deliberate act that exploits a vulnerability to achieve the compromise of a controlled system
- **Vulnerability**: An identified weakness of a controlled system in which necessary controls that are not present or are no longer effective
- **Exploit:** A technique or mechanism used to compromise a system



VULNERABILITY

A vulnerability in a system, software or service is found by an individual who decides to keep it a secret from the vendor.

EXPLOIT

Knowledge of the vulnerability is then used by either the person discovering it or a partner or contact to develop "exploit code" that is able to leverage the vulnerability.

ATTACK

The exploit is then used to perform one or more attacks on vulnerable systems.

DAY ZERO

"Day zero" is the day the vendor learns of the vulnerability and begins working on a fix.

Threats to InfoSec

A **technical attack** may use an exploit to compromise a controlled system.

A **nontechnical attack** may result from natural events or less sophisticated approaches.

Some common technical attacks

Backdoor	Brute force
Buffer overflow	Denial-of-Service (DoS)
Dictionary	DNS cache poisoning
Hoax	Mail bombing

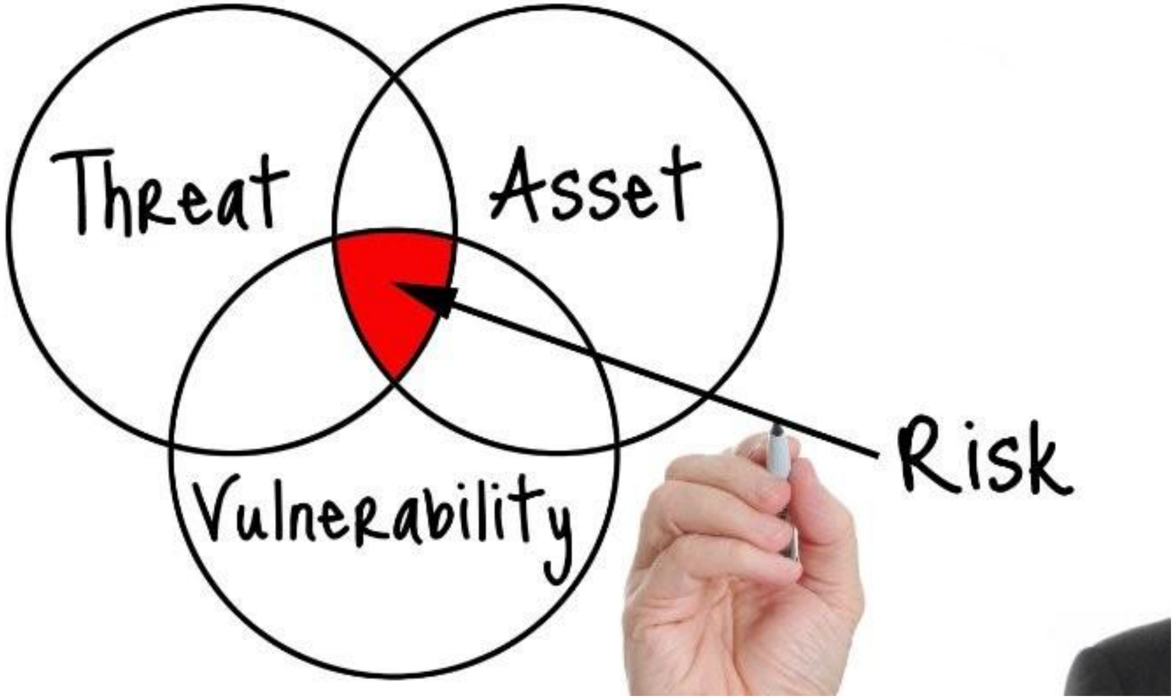
Some common technical attacks (cont.)

Malicious code	Man-in-the-middle
Password crack	Phishing
Sniffer	Social engineering
Spam	Spear phishing
Spoofing	Timing

Threats to InfoSec

- Prioritize the risk posed by each category of threat

- Identify and assess the value of your information assets
  - ➢ Assign a comparative risk rating or score to each specific information asset

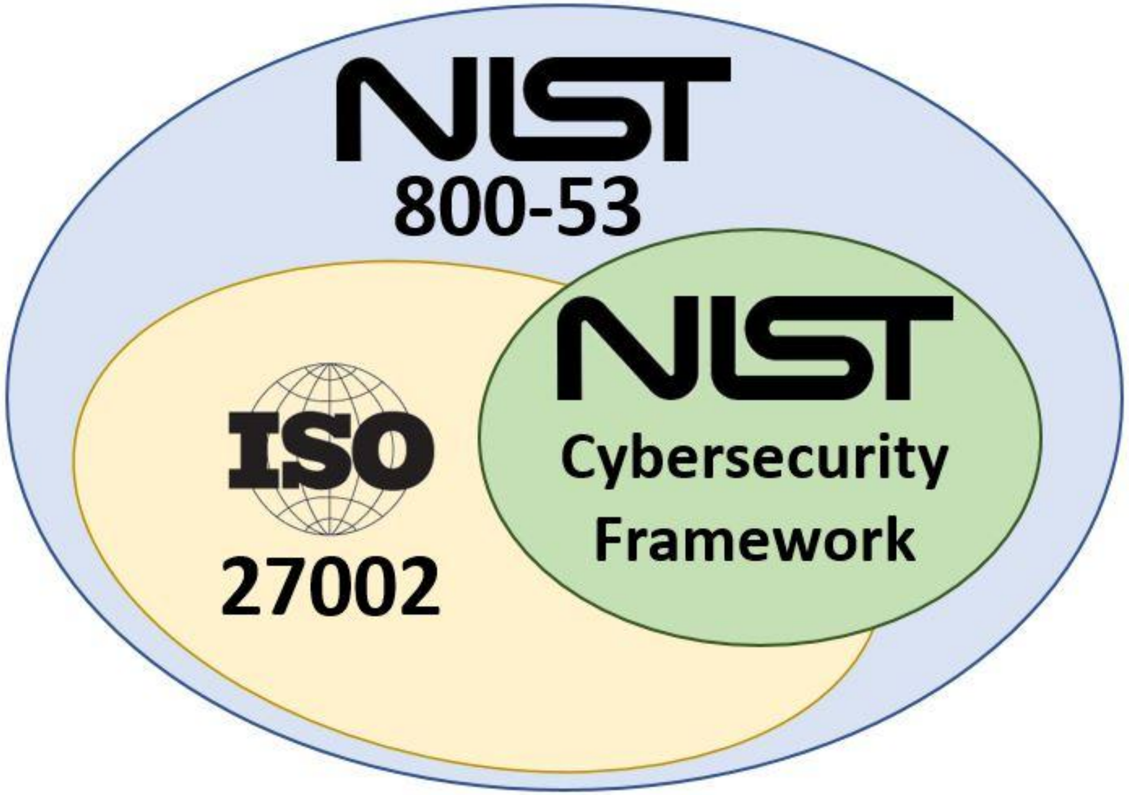


Design in the SecSDLC (logical, physical)

- Create and develop a blueprint for security
- Examine and implement key policies
- Evaluate the technology needed to support the security blueprint
- Generate alternative solutions
- Agree upon a final design

Design in the SecSDLC

- Security models may be used to guide the design process
  - Models provide frameworks for ensuring that all areas of security are addressed
  - Organizations can adapt or adopt a framework to meet their own information security needs



Design in the SecSDLC

- A critical design element of the information security program is the information security policy

- Management must define three types of security policy (NIST SP 800-100)
  - ➢ Enterprise information security policies
  - ➢ Issue-specific security policies
  - ➢ Systems-specific security policies

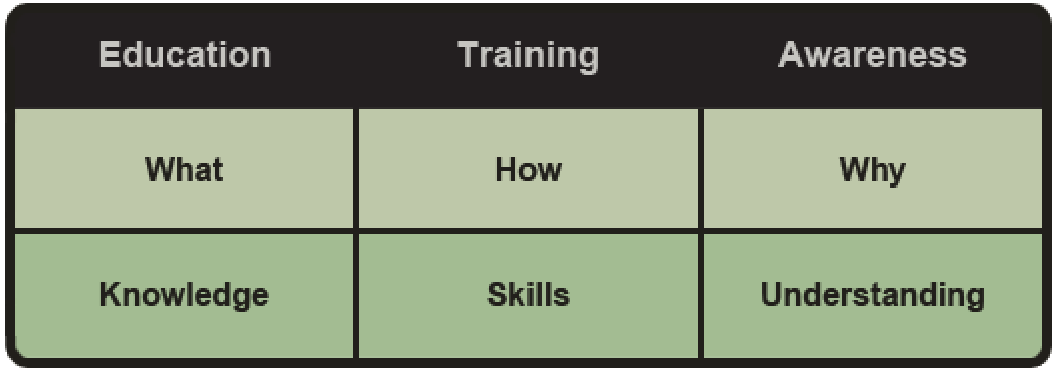
Design in the SecSDLC

- SETA program consists of security education, security training, and security awareness

SETA

SECURITY
EDUCATION
TRAINING
AWARENESS

- The purpose of SETA is to enhance security by
  - ➢ Improving awareness
  - ➢ Developing skills and knowledge
  - ➢ Building in-depth knowledge



Education	Training	Awareness
What	How	Why
Knowledge	Skills	Understanding

Design in the SecSDLC

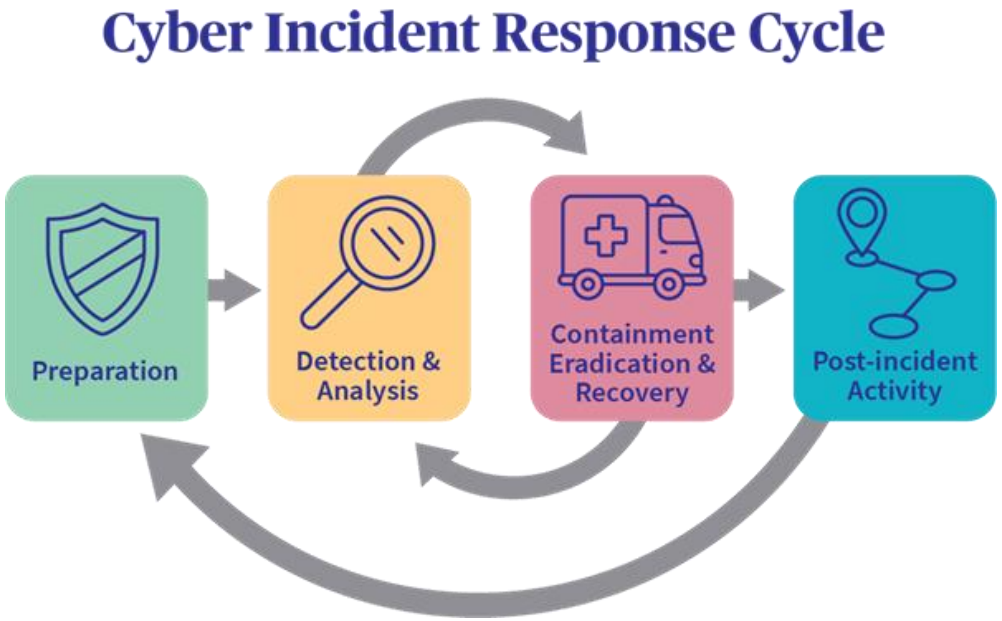
- **Design controls and safeguards:** Used to protect information from attacks by threats
- **Three categories of controls:** managerial, operational and technical

Managerial controls: address the design and implementation of the security planning process, security program management, risk management, and security control reviews

Design in the SecSDLC

Operational controls cover management functions and lower-level planning

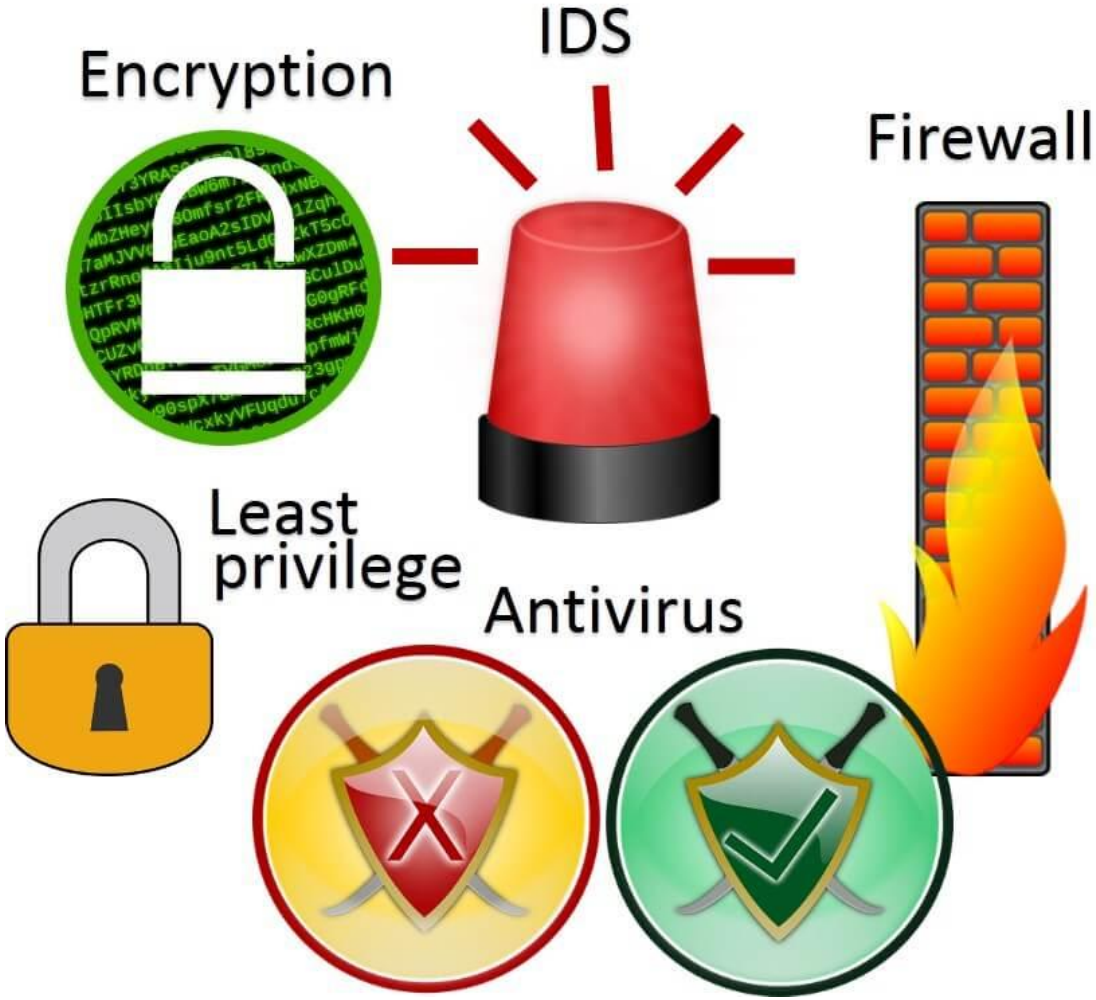
- Disaster recovery
- Incident response planning
- Personnel security
- Physical security
- Protection of production inputs and outputs


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

Design in the SecSDLC

Technical controls

- Address tactical and technical issues related to designing and implementing security in the organization
- Technologies necessary to protect information are examined and selected



Implementation in the SecSDLC

- **SecSDLC implementation phase**
  - ➢ Security solutions are acquired, tested, implemented, and tested again
  - ➢ Personnel issues are evaluated and specific training and education programs are conducted
- **Management of the project plan**
  - ➢ Planning the project
  - ➢ Supervising the tasks and action steps
  - ➢ Wrapping up the project

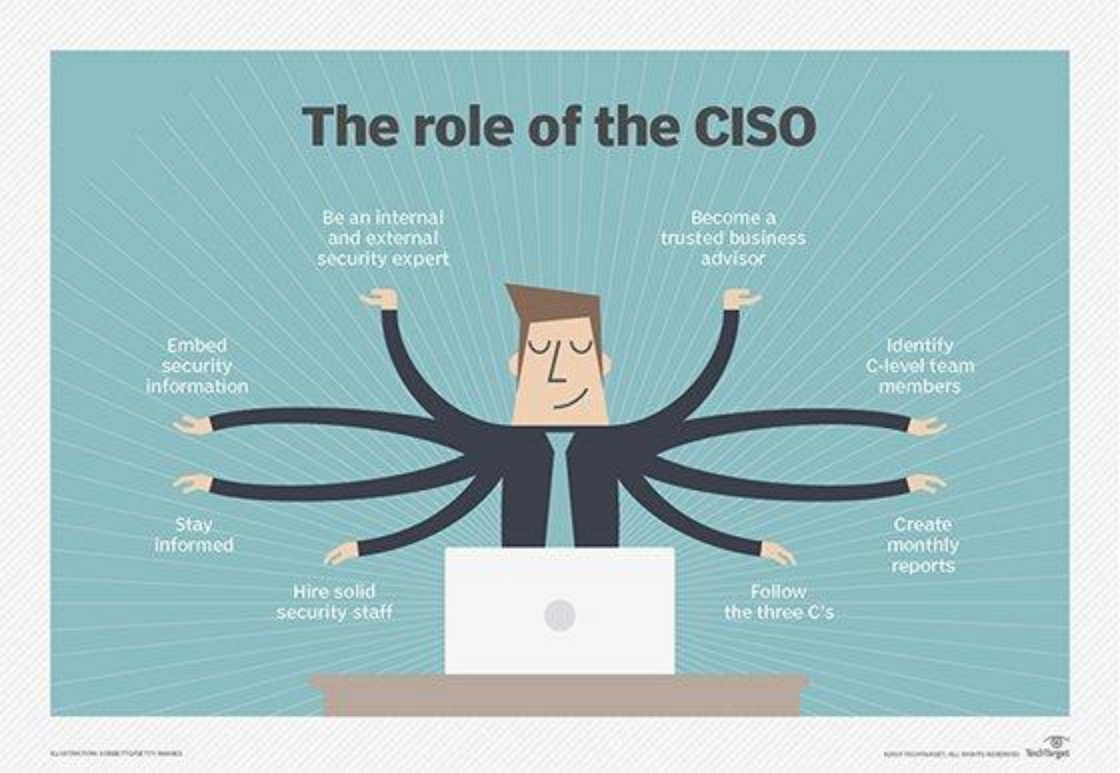
Implementation in the SecSDLC

- **Members of the team**
  - ➢ Champion
  - ➢ Team leader
  - ➢ Security policy developers
  - ➢ Risk assessment specialists
  - ➢ Security professionals
  - ➢ Systems administrators
  - ➢ End users

Implementation in the SecSDLC

Staffing the information security function

- Position and name the security function
- Plan for the staffing of InfoSec function
- Understand the impact of InfoSec across IT
- Integrate InfoSec concepts into the personnel management practices of the organization


The role of the CISO
Be an internal and external security expert
Become a trusted business advisor
Embed security information
Identify C-level team members
Stay informed
Create monthly reports
Hire solid security staff
Follow the three C's
TechTarget

Information security professionals: CIO, CISO, security managers, security technicians, data owners, data custodians, data users

Maintenance and Change in the SecSDLC

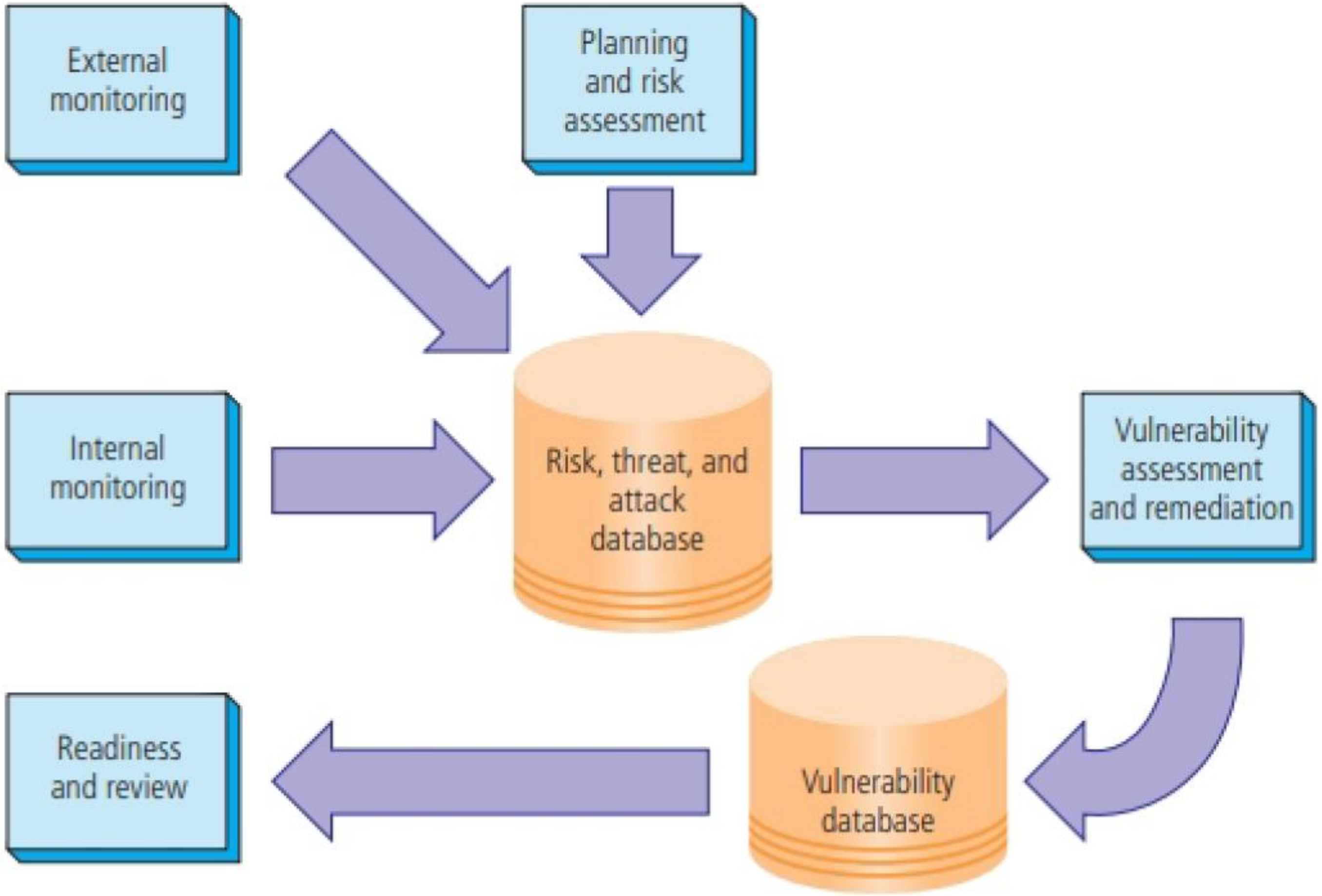
- Once the information security program is implemented, it must be operated, properly managed, and kept up to date by means of established procedures

- If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again

Maintenance and change in the SecSDLC

Aspects of a maintenance model

- External monitoring
- Internal monitoring
- Planning and risk assessment
- Vulnerability assessment and remediation
- Readiness and review


External monitoring
Planning and risk assessment
Internal monitoring
Risk, threat, and attack database
Vulnerability assessment and remediation
Readiness and review
Vulnerability database

A Summary

- Planning is central to the management of any organization.
- Creating values, vision, mission and strategy of the organization.
- Security can begin either as a bottom-up approach or with a top-down approach. InfoSec governance is the process of creating and maintaining the organizational structures that manage the InfoSec function within an enterprise.
- Systems development life cycle (SDLC): a methodology for the design and implementation of an information system in an organization.
- SecSDLC: investigation, analysis, design (logical, physical), implementation, maintenance and change.

Remarks on the Assignments

- **Assignment 1:** 10-min Moodle Quiz at the end of Week 4 Lecture
- **Assignment 2:** details will be provided by next week.
- **Assignment 3:** group creation mechanism on Moodle will be active from 24 March to 24 May 2025.