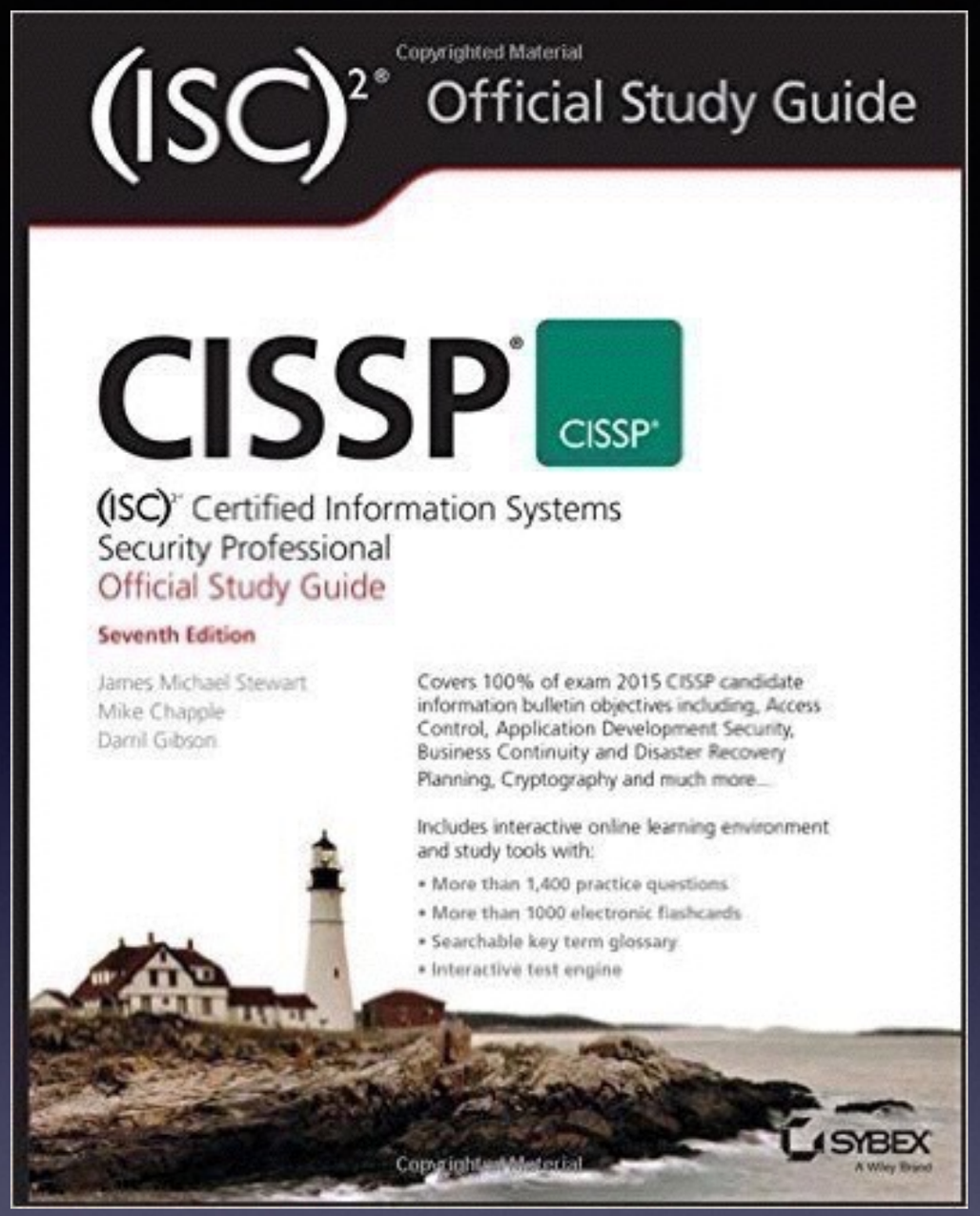
CNIT 125: Information Security Professional (CISSP Preparation)

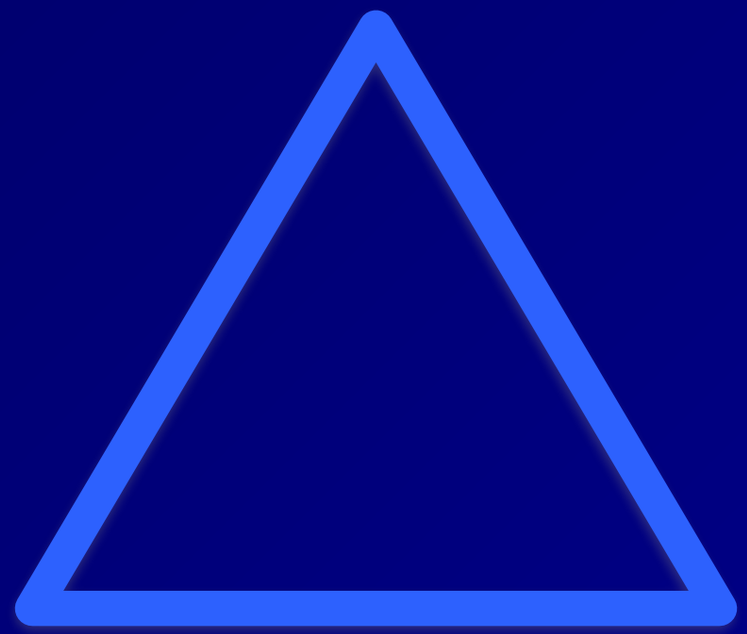


Ch 1. Security Governance Through Principles and Policies

The CIA Triad

Core Information Security Tenets

Confidentiality



Integrity **Availability**

Controls

- Security controls are evaluated on how well they address the code tenets
- A complete security solution should adequately address each of these tenets
- Vulnerabilities and risks are also evaluated on the threat they pose against one or more of the CIA Triad principles

Confidentiality

- Assurance that data, objects, or resources are restricted from unauthorized subjects
- Data must be protected in **storage**, in **process**, and in **transit**
- Attacks include sniffing network traffic, social engineering, eavesdropping, and more
- Unauthorized disclosure often results from human error

Other Confidentiality Concepts

- **Sensitivity**
  - Quality of information which could cause harm if disclosed
- **Discretion**
  - An operator's act or decision to control disclosure to minimize harm
- **Criticality**
  - The level to which information is mission-critical; highly critical information is essential to the operation or function of an organization

Other Confidentiality Concepts

- **Concealment**
  - Hiding or preventing disclosure; a means of cover, obfuscation, or distraction
- **Secrecy**
  - Keeping something secret; preventing disclosure
- **Privacy**
  - Keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace

Other Confidentiality Concepts

- **Seclusion**
  - Storing something in an out-of-the-way location
- **Isolation**
  - Keeping something separated from others

Integrity

- Assures that data has not been modified, tampered with, or corrupted
- **Three perspectives**
  - Prevent **unauthorized** subjects from making modifications
  - Prevent authorized subjects from making unauthorized modifications, such as **mistakes**
  - Maintaining **consistency** of objects so data is correct and maintains its proper relationships with child, peer, or parent objects

Integrity Controls and Countermeasures

- Access controls
- Authentication
- Intrusion Detection Systems
- Activity logging
- Maintaining and validating object integrity
- Encryption
- Hashing

Integrity Attacks

- Viruses
- Logic bombs
- Unauthorized access
- Errors in coding
- Malicious modification
- System back doors

Other Integrity Concepts

- Accuracy
- Truthfulness
- Authenticity
- Validity
- Nonrepudiation
- Accountability
- Responsibility
- Completeness
- Comprehensiveness

Non-Repudiation

- Prevents entities from denying that they took an action
- Examples: signing a home loan, making a credit card purchase
- Techniques
  - Digital signatures
  - Audit logs

Availability

- Data and services are available when needed by authorized subjects
  - Remove SPOF (Single Point of Failure)
  - Prevent Denial of Service attacks

Threats to Availability

- Device failure
- Software errors
- Environmental issues (heat, static, flooding, power loss, etc.)
- Denial of Service attacks
- Human errors (deleting important files, under allocating resources, mislabeling objects)

Availability Controls

- Intermediary delivery systems design (routers, proxies, etc.)
- Access controls
- Monitoring performance and traffic
- Redundant systems
- Backups
- Business Continuity Planning
- Fault-tolerant systems

Balancing CIA

- You can never have perfect security
- Increasing one item lowers others
- Increasing confidentiality generally lowers availability
  - Example: long ,complex passwords that are easily forgotten

AAA Services

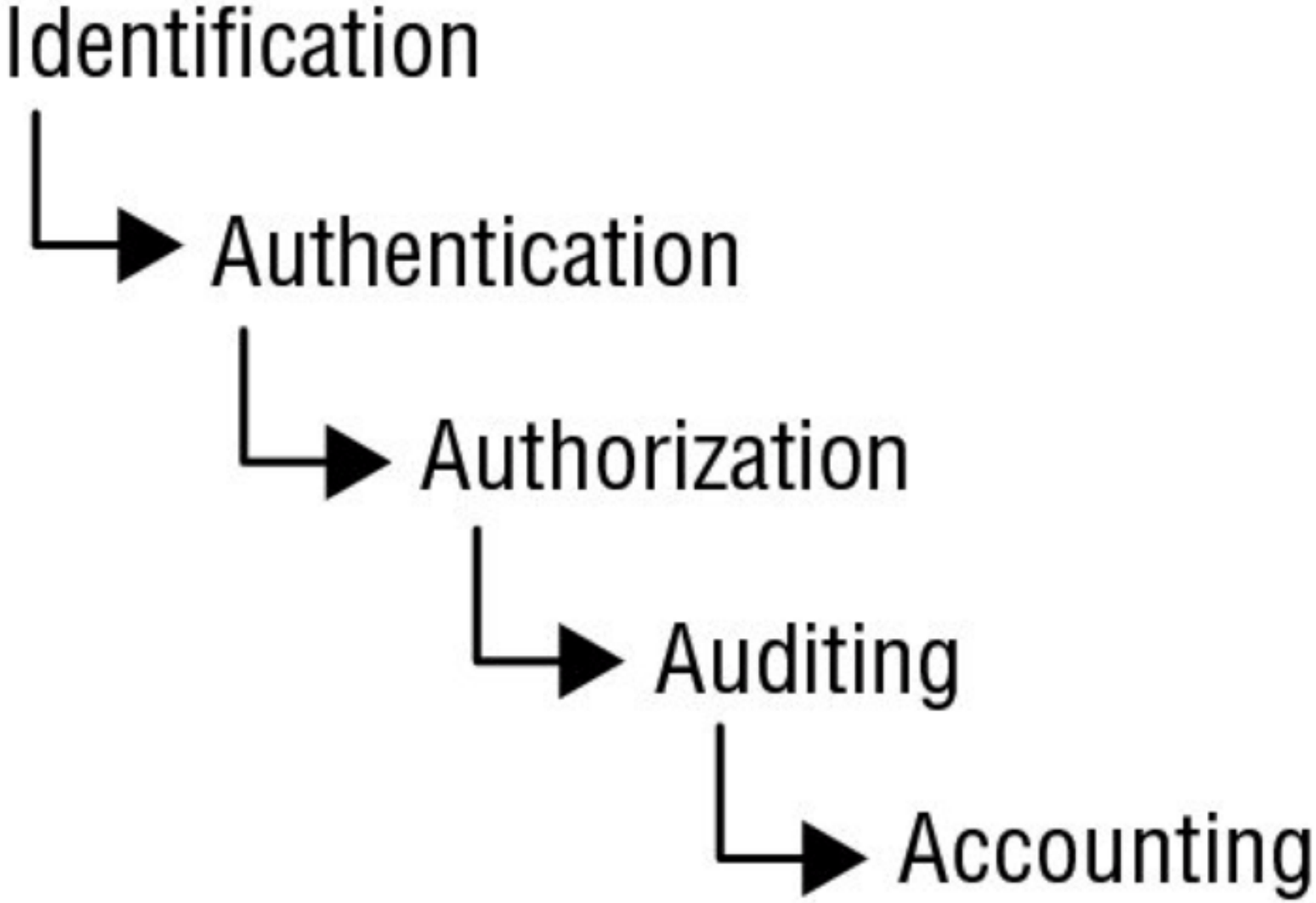


Figure 1.2 The five elements of AAA services

Five Elements

- **Identification** claiming to be someone
- **Authentication** proving that you are that person
- **Authorization** allows you to access resources
- **Auditing** records a log of what you do
- **Accounting** reviews log files and holds subjects accountable for their actions

AAA Services

- **Authentication**
- **Authorization**
- **Accounting**

Nonrepudiation

- The subject of an activity cannot deny that the event occurred
- Established using digital certificates, session identifiers, transaction logs, etc.

Protection Mechanisms

- Layering
- Abstraction
- Data Hiding
- Encryption

Layering

- Also called **Defense in Depth**
- Multiple defenses in series
- If one fails, another may succeed

Abstraction

- Group similar elements together
- Assign security controls, restrictions, or permissions to the groups
- Such as Administrators, Sales, Help Desk, Managers

Data Hiding

- Placing data in a logical storage compartment that is not seen by the subject
- Ex:
  - Keeping a database inaccessible to unauthorized users
  - Restricting a subject at a low classification level from accessing data at a higher classification level

Encryption

- Hiding the meaning of a communication from unintended recipients

Security Governance Principles

- The collection of practices
  - Supporting, defining and directing
  - The security efforts of an organization
- Goal is to maintain business processes while striving towards growth and resiliency
- Some aspects are imposed on organizations
  - Regulatory compliance
  - Industry guidelines
  - License requirements

Security Governance Principles

- Must be assessed and verified
- Security is not just an IT issue
  - Affects every aspect of an organization

Alignment of Security Function to Strategy, Goals, Mission, and Objectives

- Base security planning on a **business case**
  - A documented argument to define a need
  - Justifies the expense

Top-Down Approach

- Upper management initiates and defines security policy
- Recommended
- **Bottom-Up Approach**
  - IT staff makes security decisions without input from senior management
  - Rarely used and problematic
- Security plans are useless without approval from senior management

CSO (Chief Security Officer)

- Security management is a responsibility of upper management, not IT staff
- InfoSec team should be led by a CSO
- CSO reports directly to senior management
- CSO and InfoSec team are outside the typical hierarchical structure

Strategic, Tactical, and Operational Plans

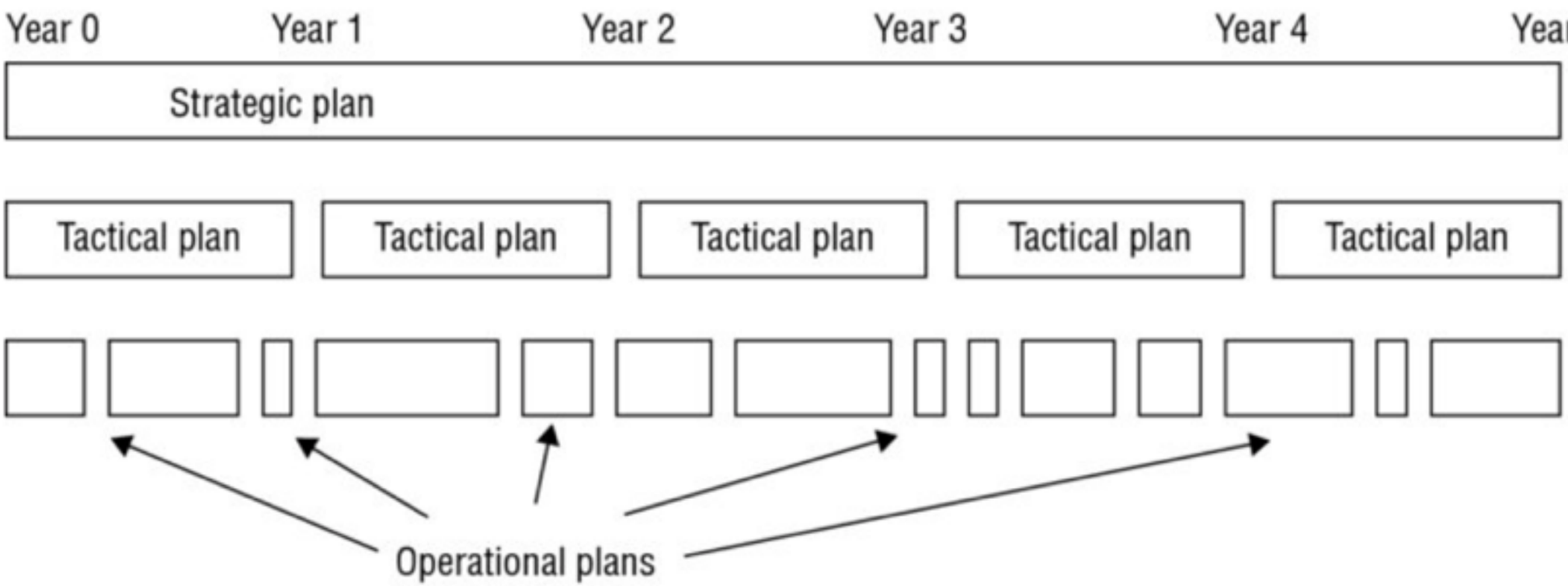


Figure 1.3 Strategic, tactical, and operational plan timeline comparison

Strategic, Tactical, and Operational Plans

- Strategic Plan
  - Long term (about five years)
  - Goals and visions for the future
  - Risk assessment
- Tactical Plan
  - Useful for about a year
  - Ex: projects, acquisitions, hiring, budget, maintenance, support, system development

Strategic, Tactical, and Operational Plans

- Operational Plan
  - Short term (month or quarter)
  - Highly detailed
  - Ex: resource allotments, budgetary requirements, staffing assignments, scheduling, step-by-step or implementation procedures

Change Control/Management

- Planning, testing, logging, auditing, and monitoring of activities related to security controls and mechanisms
- Goal: ensure that a change does not reduce or compromise security
- Must include **rollback** plan
  - How to reverse a change to recover a previous secured state

Change Control/Management

- Required fir ITSEC classifications of B2, B3, and A1
  - Information Technology Security Evaluation and Criteria

Change Control Process

- Implement change in a monitored and orderly manner
- Formalized testing process to very expected results
- Rollback plan
- Users are informed of change before it occurs
- Effects of change are systematically analyzed
- Negative impact of change is minimized
- Changes are reviewed and approved by CAB (Change Approval Board)

Data Classification

- Some data needs more security than others
- Criteria:
  - Usefulness, timeliness, value, age, data disclosure damage assessment, national security implications
  - Authorized access, restrictions, maintenance, monitoring, and storage

To Implement a Classification Scheme

1. Identity custodian
2. Specify evaluation criteria
3. Classify and label each resource
4. Document exceptions
5. Select security controls
6. Specify declassification procedures
7. Create awareness program to instruct all personnel

Classification Levels

- Government / Military
  - Top Secret
  - Secret
  - Confidential
  - Unclassified
- Business / Private Sector
  - Confidential or Private
  - Sensitive
  - Public

Security Roles and Responsibilities

- Senior Manager
  - Ultimately responsible for the security of an organization
  - Must sign off on all activities
- Security Professional
  - Writes security policy and implements it
  - Follows directives from senior management
- Data Owner
  - Responsible for classifying information

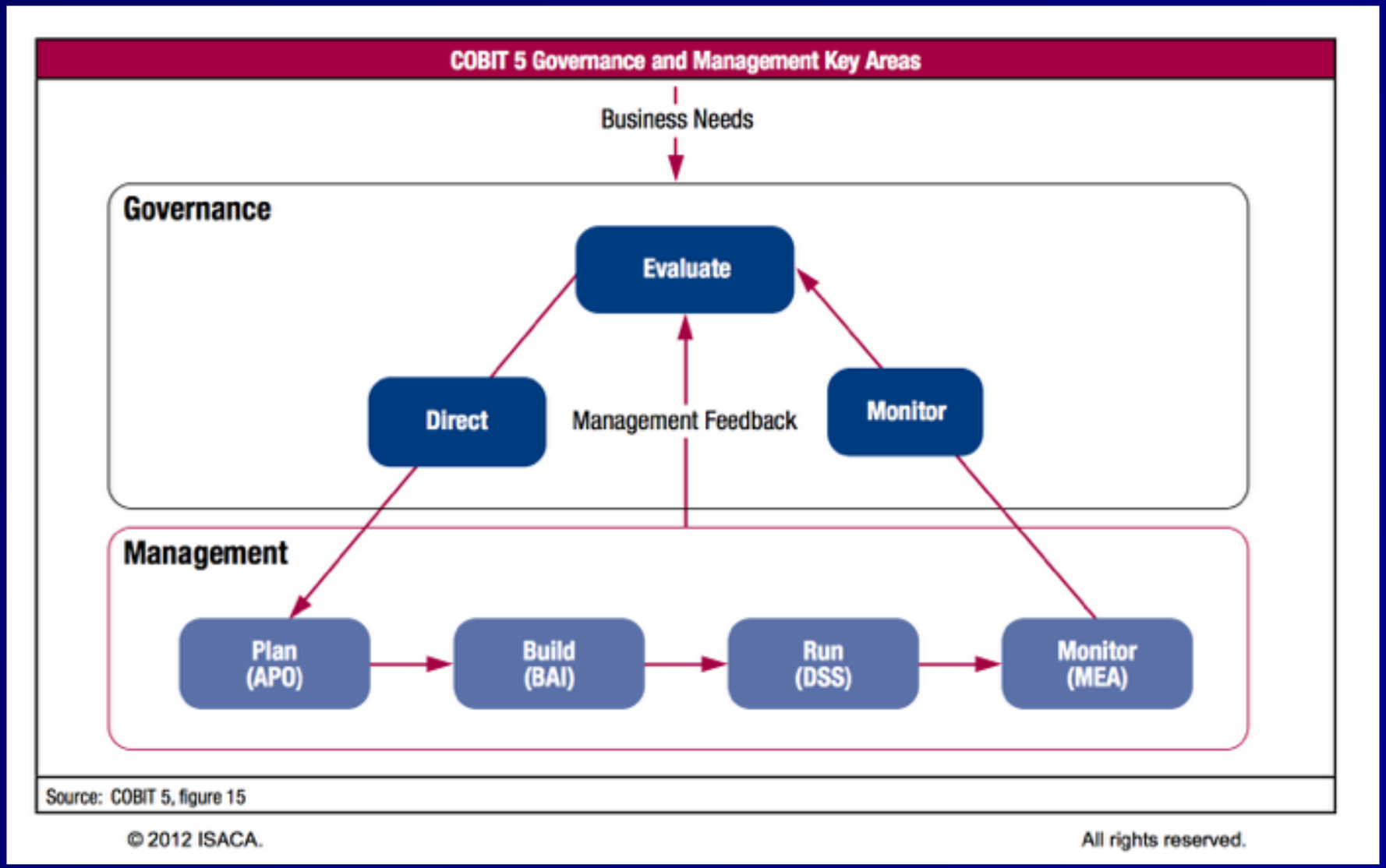
Security Roles and Responsibilities

- Data Custodian
  - Implements protections defined by security policy
  - Ex: Making and testing backups, managing data storage based on classification
- User
  - Anyone with access to the secured system
- Auditor
  - Produces compliance and effectiveness reports for the senior manager

Control Objectives for Information and Related Technology (COBIT)

- A set of IT best practices
- from ISACA (Information Systems Audit and Control Association)
- Five key principles
  1. Meeting stakeholder needs
  2. Covering the enterprise end-to-end
  3. Applying a single, integrated framework
  4. Enabling a holistic approach
  5. Separating governance from management

COBIT 5



- Link Ch 1a

Due Care and Due Diligence

- Due Care *(thought)*
  - Using reasonable care to protect the interests of an organization
  - Ex: Developing a security structure
    - Security policy, standards, baselines, guidelines, and procedures
- Due Diligence *(action)*
  - Practicing the activities that maintain due care
  - Applying the security structure onto IT infrastructure
  - Link Ch 1b

Security Structure Components

- Policies
- Standards
- Guidelines
- Procedures

Security Policies

- Overview or generalization of security needs
- A strategic plan for implementing security
  - Assigns responsibilities
  - Specifies audit and compliance requirements
  - Outlines enforcement processes
  - Defines acceptable risk levels
- Used as proof that senior management has exercised due care
- Always compulsory

Types of Security Policies

- Organizational
  - Issues relevant to every aspect of an organization
- Issue-specific
  - Such as a specific network service
- System-specific
  - Such as a firewall policy

Categories of Security Policies

- Regulatory
  - Compliance with industry or legal standards
- Advisory
  - Discusses acceptable activities and consequences of violations
  - Most policies are advisory
- Informative
  - Provides background information

Standards

- Compulsory requirements for homogenous use of software, technology, and security controls
- Course of action to implement technology and procedures uniformly thought an organization
- Tactical documents

Baselines

- Minimum level of security that every system must meet
- Often refer to an industry or government standard, like
  - Trusted Computer System Evaluation Criteria (TCSEC)
  - NIST (National Institute of Standards and Technology)

Guidelines

- Recommendation on how to meet standards and baselines
- Flexible; can be customized
- Not compulsory

Security Procedures

- Detailed step-by-step instructions
- System- and software-specific
- Must be updated as hardware and software evolve

Threat Modeling

- Identifies potential harm
- Probability of occurrence
- Priority of concern
- Means to reduce the threat

Proactive Threat Modeling

- During early stages of systems development
- During early design and specifications establishment
- Predicts threats and designs in defenses
  - Ex: Microsoft's Security Development Lifecycle

Reactive Threat Modeling

- Takes place after a product has been created and deployed
- Adversarial approach
  - Ethical hacking
  - Penetration testing
  - Source code review
  - Fuzz testing
- Leads to updates and patches

Identifying Threats

- Focused on Assets
  - Control access to assets
- Focused on Attackers
  - Consider goals of known attackers
- Focused on Software
  - Custom software
  - Ex: fancy Web pages

Microsoft STRIDE Threat Categorization

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Diagramming Potential Attacks

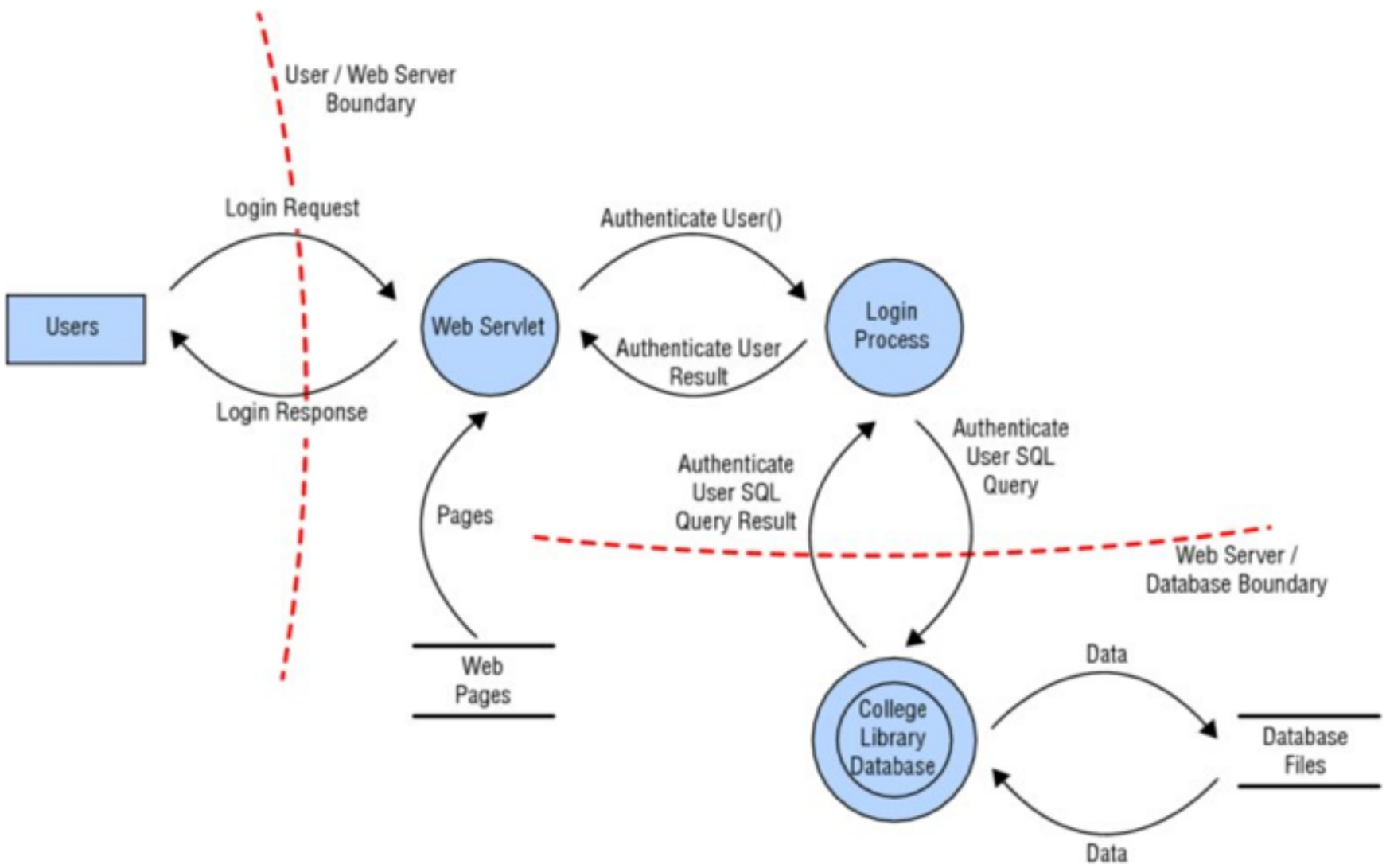


Figure 1.7 An example of diagramming to reveal threat concerns

Reduction Analysis (Decomposition)

- Divide system into smaller containers and find:
  - Trust Boundaries
  - Data Flow Paths
  - Input Points
  - Privileges Operations
  - Details about Security Stance and Approach

Prioritization and Response

- Document threats: means, target, consequences
- Rank threats
  - Probability x Damage
  - High / Medium / Low
  - DREAD model (Link Ch 1c)
    - Damage potential, Reproducibility, Exploitability, Affected users, Discoverability

Security Risk and Acquisitions

- Purchasing items without considering security leads to long-term risks
- Selecting purchases that are more secure is often more cost-effective
  - Consider **Total Cost of Ownership**
- Also applies to outsourcing contracts, suppliers, consultants, etc.
- Ongoing security monitoring, management, and assessment may be required

Evaluating a Third Party

- On-Site Assessment
- Document Exchange and Review
- Process / Policy Review