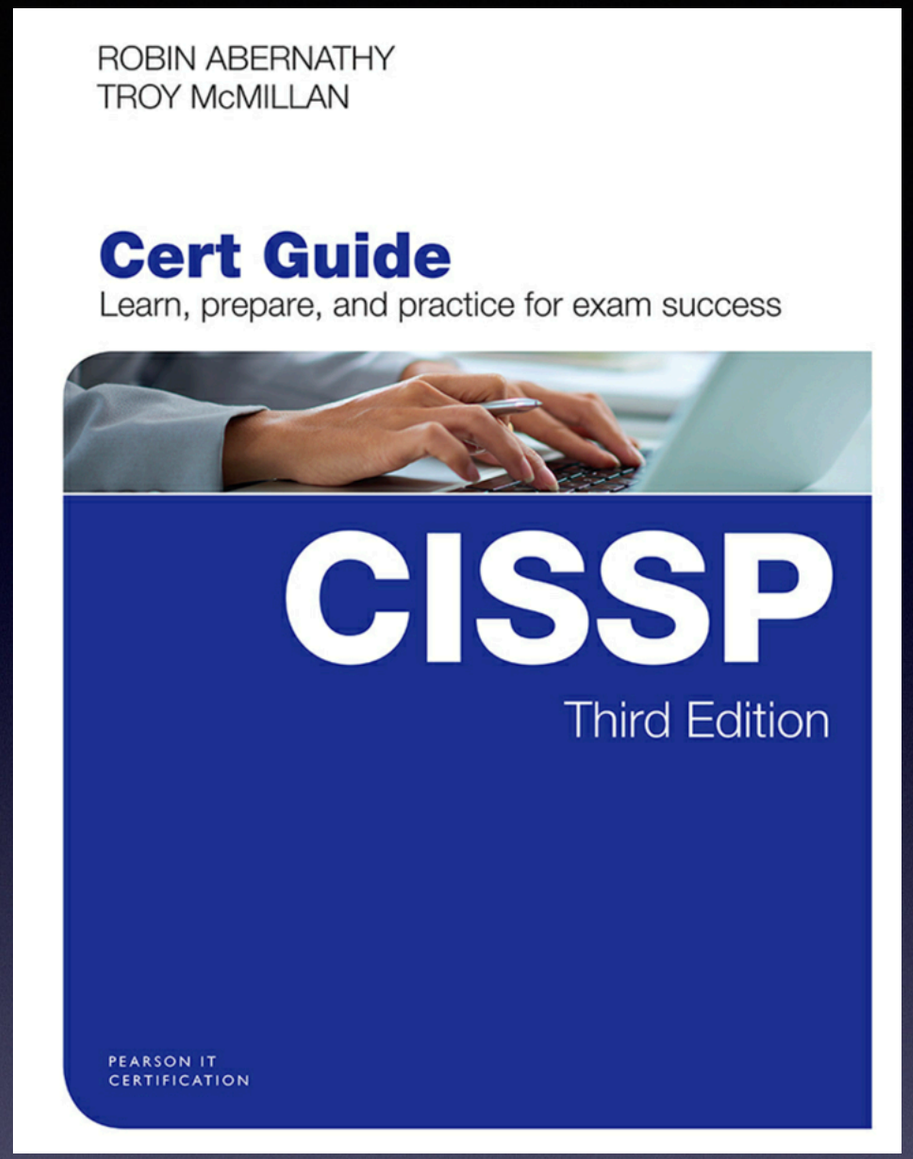
# CNIT 125: Information Security Professional (CISSP Preparation)




Updated 1-24-22

# Ch 1. Security and Risk Management (Part 1)

# Topics in Part 1

- Security Terms
- Security Governance Principles
  - Ends at "Security Control Frameworks"

# Topics in Part 2

- Security Control Frameworks
- Compliance
- Legal and Regulatory Issues
  - Important Laws and Regulations
- Professional Ethics
- Security Documentation
- Business Continuity Personnel Security Policies and Procedures
- Risk Management Concepts
  - Risk Assessment/Analysis
  - Control Categories and Types
- Threat Modeling

# Security Terms

# The CIA Triad

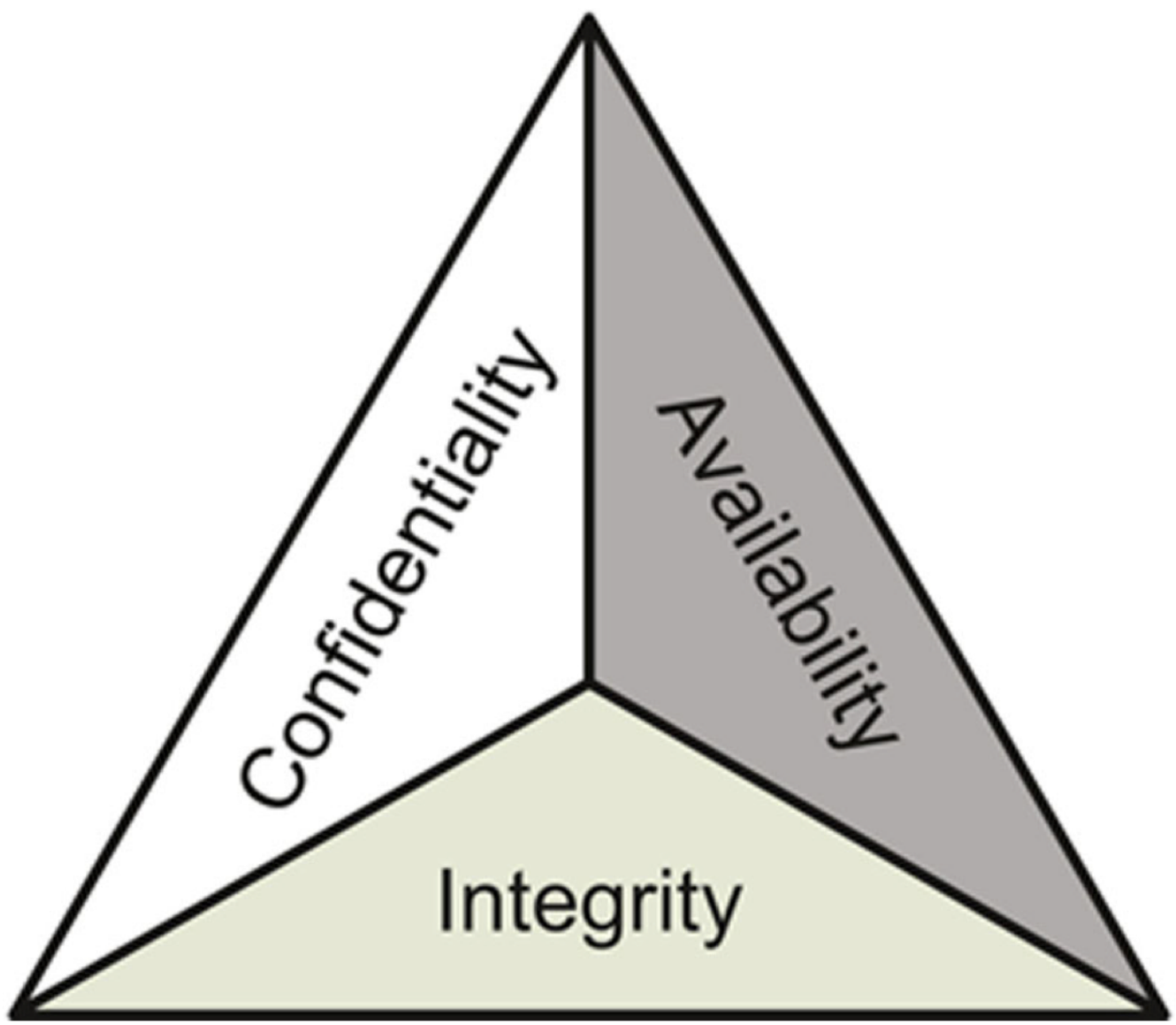



**FIGURE 2.1** **The CIA Triad**

# The CIA Triad

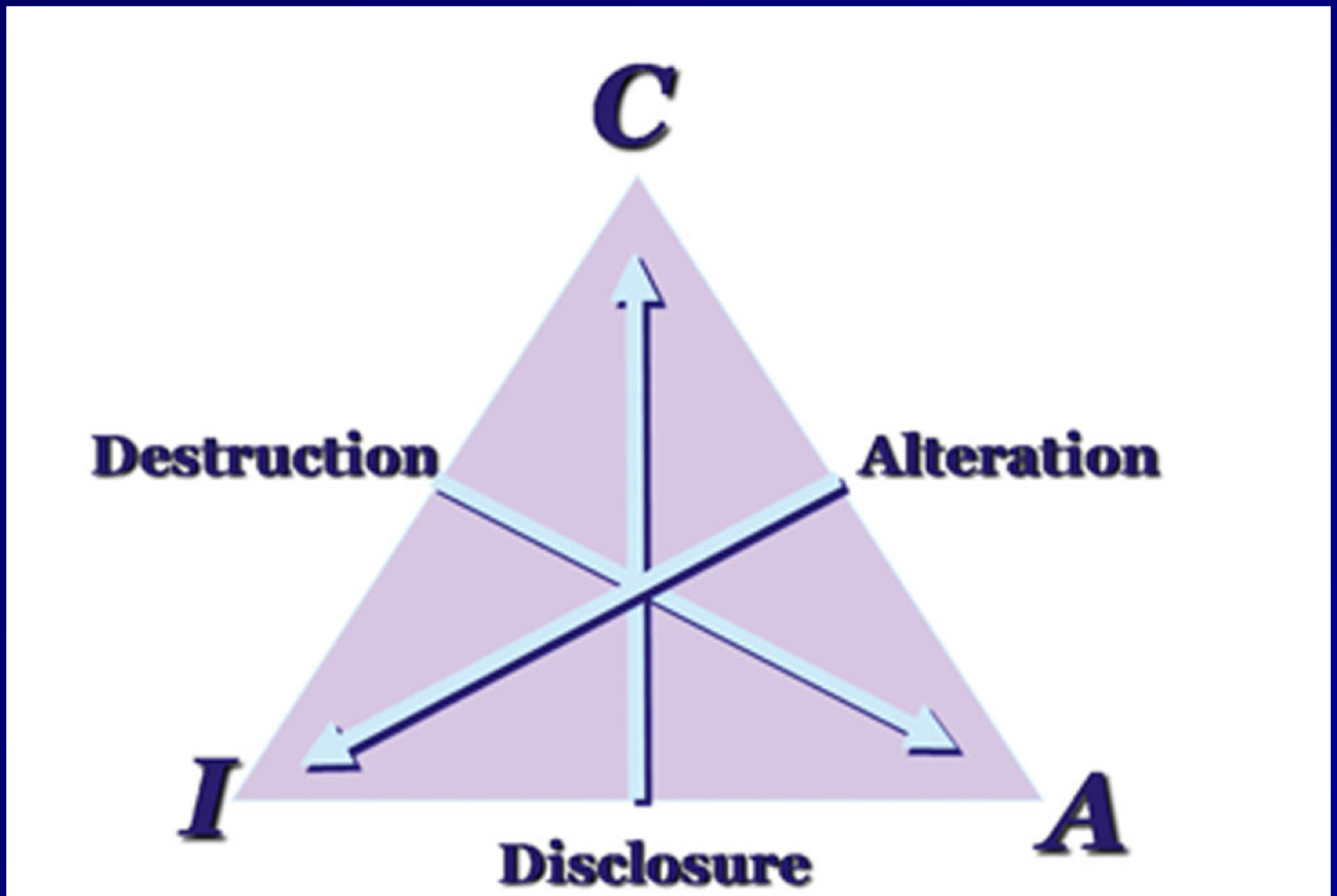



FIGURE 2.2 Disclosure, Alteration and Destruction

# Confidentiality

- Keeps data secret
  - Prevents unauthorized read access
  - An attack: theft of **Personally Identifiable Information (PII)** such as credit card information
- Health Insurance Portability and Accountability Act (HIPAA)
  - Requires medical providers to keep patient information private

# Confidentiality

- Data should only be available to users who have
  - **Clearance**
  - **Formal access approval**
  - **Need to know**

# 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

# 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

# Auditing and Accounting

- Auditing
  - Measurable technical assessment of a system or application
- Accounting
  - Logging access and use of information resources

# 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**

# Example of Accounting

March 31, 2009

## Octomom's hospital records accessed, 15 workers fired

*Updated Tuesday, March 31, 2009 at 5:27 p.m. EST*

A Los Angeles-area hospital recently fired 15 workers for accessing the medical records of octuplet mother Nadia Suleman without permission, a spokesman confirmed to SCMagazineUS.com Tuesday.

- **Link Ch 2a**


1a

# Non-Repudiation

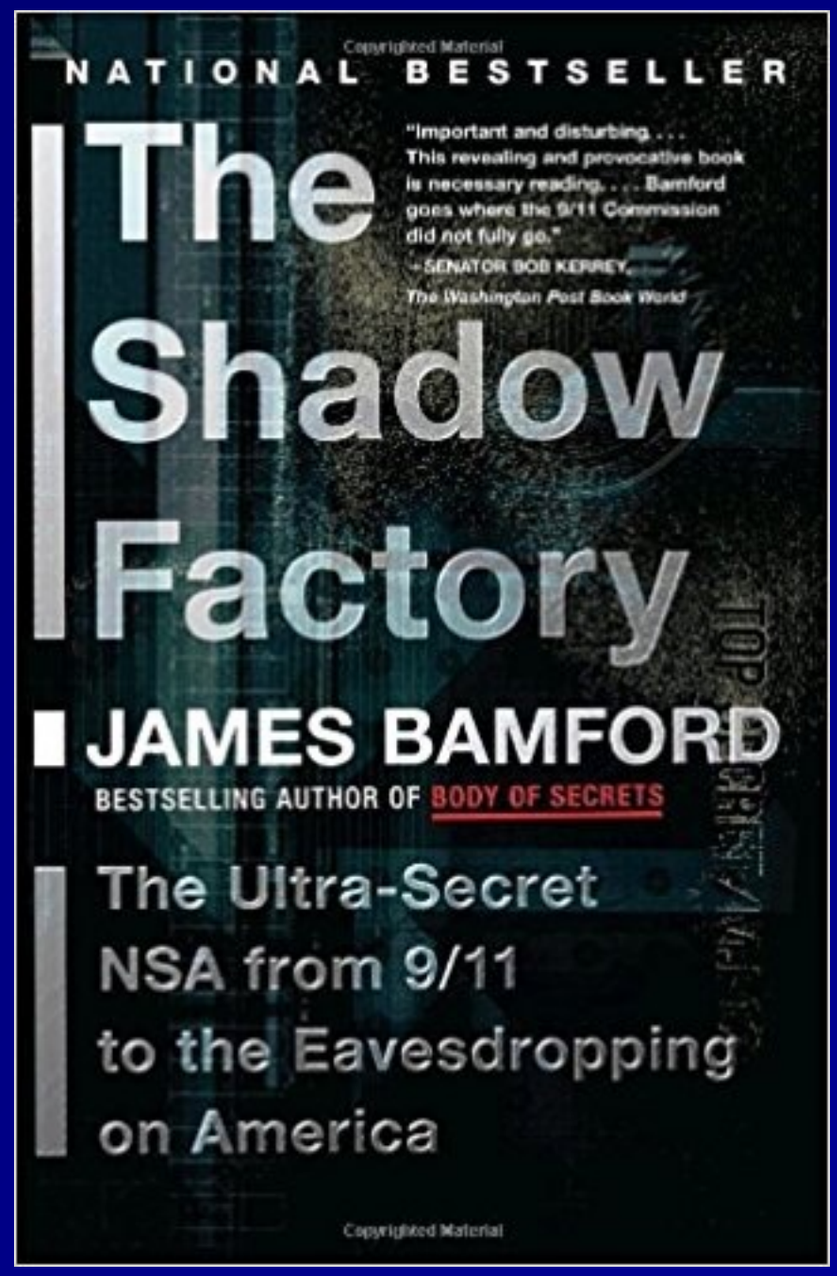
- Prevents entities from denying that they took an action
- Examples: signing a home loan, making a credit card purchase
- Techniques
  - Digital signatures
  - Audit logs

# Least Privilege and Need to Know

- Least privilege
  - Users have the minimum authorization to do their jobs
- Need to know
  - More granular than least privilege
  - Users must have a need to access that particular information before accessing it

# Example: Need to Know

- In the 1990's US intelligence agencies did not share information with one another
  - "Information Silos"
- Failed to predict the 9/11 attacks, arguably for this reason
  - Links Ch 2b, 2c



# Example: Need to Know

- The silos were removed
- So Bradley Manning (now Chelsea), gave 750,000 classified or sensitive documents to Wikileaks
- Links Ch 2d, 2e, 2f

# Subjects and Objects

- **Subject** is an active entity
  - Such as a person accessing data
  - Or a computer program
- **Object** is a passive entity
  - Such as paper records or data files

# Subjects and Objects

- Internet Explorer
  - A **Subject** when running in memory
  - Accessing data
- iexplore.exe
  - An **object** when not running
  - A file sitting on a disk

# Defense in Depth

- Multiple defenses in series
- If one fails, another may succeed
- Example:
  - Palo Alto firewall protects whole LAN
  - Windows firewall runs on each workstation

# Due Care and Due Diligence

- Due Care
  - Doing what a reasonable person would do
  - The "prudent man" rule
  - Informal
- Due Diligence
  - Management of due care
  - Follows a process
  - A step beyond due care

# Gross Negligence

- The opposite of due care
- If you suffer loss of PII
  - Legal consequences will depend on whether you can demonstrate due care or not

# 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


1b

# Security Governance Principles

# 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

# 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

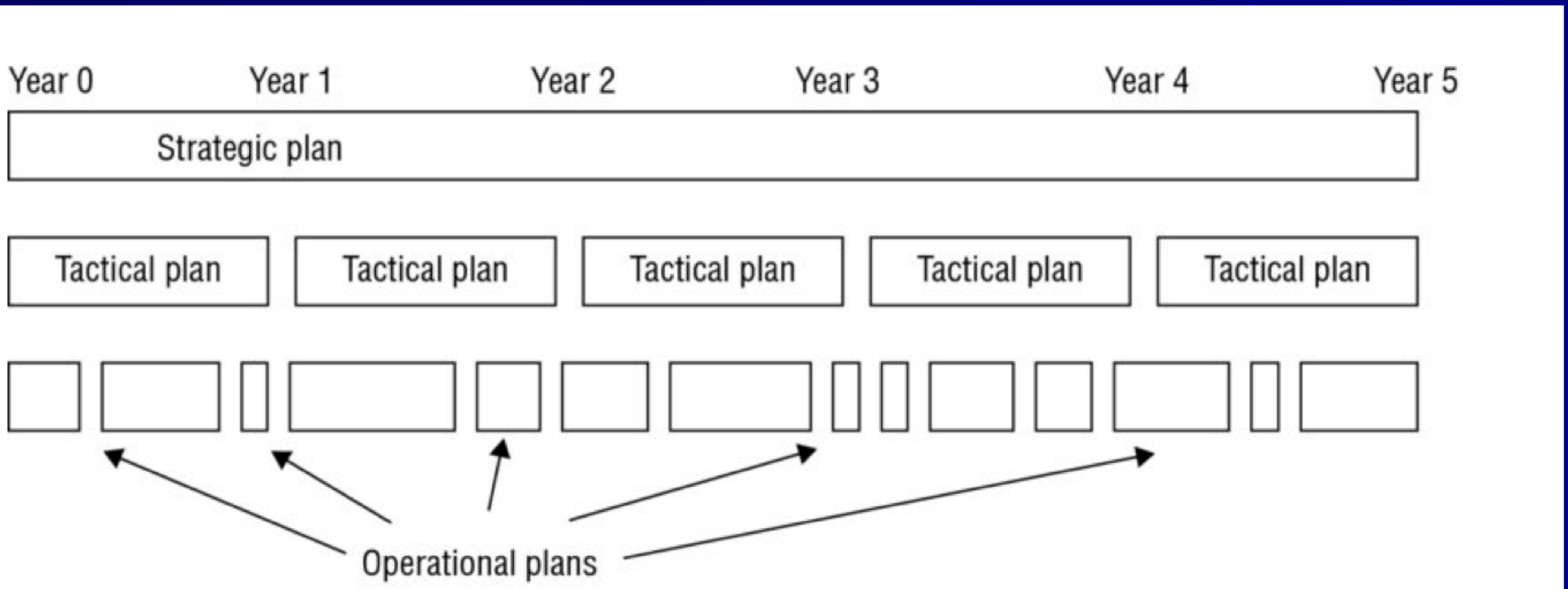



**Figure 1.3** Strategic, tactical, and operational plan timeline comparison

# 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 for 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 verify 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

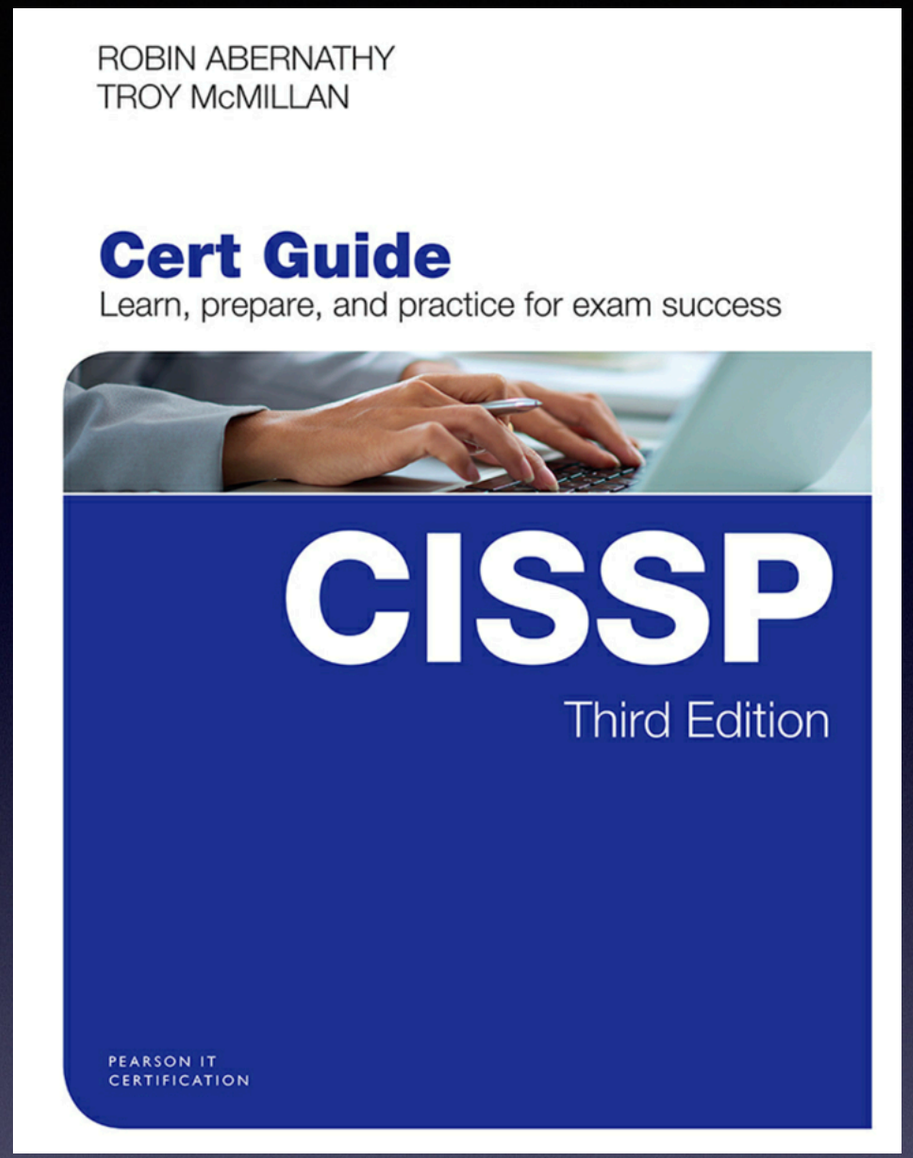
- Senior Manager
  - Ultimately responsible for the security of an organization
  - Must sign off on all activities
- Security Professional
  - Writes security policy and implements it
  - Follows directives from senior management
- Data Owner
  - Responsible for classifying information

# 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


1c

# CNIT 125: Information Security Professional (CISSP Preparation)




# Ch 1. Security and Risk Management (Part 2)

# Security Control Frameworks

- ISO/IEC 27000 Series
- Zachman Framework
- TOGAF
- DoDAF
- MODAF
- SABSA
- COBIT
- NIST 800 Series

- HITRUST CSF
- CIS Critical Security Controls
- COSO
- OCTAVE
- ITIL
- Six Sigma
- CMMI
- CRAMM
- Top-down versus bottom-up approach
- Security program life cycle

# ISO/IEC 27000 Series

- International Organization for Standardization (ISO)
  - With the International Electrotechnical Commission
- A lengthy list of standards for developing and maintaining an Information Security Management System (ISMS)

- **27000:2018—Published overview of ISMSs and vocabulary**
- **27001:2013—Published ISMS requirements**
- **27002:2013—Published code of practice for information security controls**
- **27003:2017—Published guidance on the requirements for an ISMS**
- **27004:2016—Published ISMS monitoring, measurement, analysis, and evaluation guidelines**
- **27005:2011—Published information security risk management guidelines**

- **27042:2015—Published digital evidence analysis and interpretation guidelines**
- **27043:2015—Published incident investigation principles and processes**
- **27050-1:2016—Published electronic discovery (eDiscovery) overview and concepts**
- **27050-3:2017—Published code of practice for electronic discovery**
- **27799:2016—Published information security in health organizations guidelines**

# Zachman Framework

- Two-dimensional classification system
- Based on six communication questions
  - What, Where, When, Why, Who, How
- Intersecting with perspectives
  - Executive, Business Management, Architect, Engineer, Technician, Enterprise
- Not security oriented
- Helps to relay information in language useful to personnel

# The Open Group Architecture Framework (TOGAF)

- Another enterprise architecture framework
- Helps organizations design, plan, implement, and govern
  - An enterprise information architecture
- Four domains:
  - Technology, Applications, Data, Business

# Dept of Defense Architecture Framework (DoDAF)

- Organizes a set of products under eight views
  - All Viewpoint (AV)
  - Capability Viewpoint (CV)
  - Data and Information Viewpoint (DIV)
  - Operation Viewpoint (OV)
  - Project Viewpoint (PV)
  - Services Viewpoint (SvcV)
  - Standards Viewpoint (STDV)
  - Systems Viewpoint (SV)

# British Ministry of Defense Architecture Framework (MODAF)

- Divides information into seven viewpoints
  - Strategic Viewpoint (StV)
  - Operational Viewpoint (OV)
  - Service-Oriented Viewpoint (SOV)
  - Systems Viewpoint (SC)
  - Acquisition Viewpoint (AcV)
  - Technical Viewpoint (TV)
  - All Viewpoint (AV)

# Sherwood Applied Business Security Architecture (SABSA)

| | ASSETS (What) | MOTIVATION (Why) | PROCESS (How) | PEOPLE (Who) | LOCATION (Where) | TIME (When) |
|---|---|---|---|---|---|---|
| **CONTEXTUAL ARCHITECTURE** | Business Decisions | Business Risk | Business Processes | Business Governance | Business Geography | Business Time Dependence |
| | Taxonomy of Business Assets, including Goals & Objectives | Opportunities & Threats Inventory | Inventory of Operational Processes | Organisational Structure & the Extended Enterprise | Inventory of Buildings, Sites, Territories, Jurisdictions, etc. | Time dependencies of business objectives |
| **CONCEPTUAL ARCHITECTURE** | Business Knowledge & Risk Strategy | Risk Management Objectives | Strategies for Process Assurance | Roles & Responsibilities | Domain Framework | Time Management Framework |
| | Business Attributes Profile | Enablement & Control Objectives; Policy Architecture | Process Mapping Framework; Architectural Strategies for ICT | Owners, Custodians and Users; Service Providers & Customers | Security Domain Concepts & Framework | Through-Life Risk Management Framework |
| **LOGICAL ARCHITECTURE** | Information Assets | Risk Management Policies | Process Maps & Services | Entity & Trust Framework | Domain Maps | Calendar & Timetable |
| | Inventory of Information Assets | Domain Policies | Information Flows; Functional Transformations; Service Oriented Architecture | Entity Schema; Trust Models; Privilege Profiles | Domain Definitions; Inter-domain associations & interactions | Start Times, Lifetimes & Deadlines |
| **PHYSICAL ARCHITECTURE** | Data Assets | Risk Management Practices | Process Mechanisms | Human Interface | ICT Infrastructure | Management Schedule |
| | Data Dictionary & Data Inventory | Risk Management Rules & Procedures | Applications; Middleware; Systems; Security Mechanisms | User Interface to ICT Systems; Access Control Systems | Host Platforms, Layout & Networks | Timing & Sequencing of Processes and Sessions |
| **COMPONENT ARCHITECTURE** | ICT Components | Risk Management Tools & Standards | Process Tools & Standards | Personnel Man'ment Tools & Standards | Locator Tools & Standards | Step Timing & Sequencing Tools |
| | ICT Products, including Data Repositories and Processors | Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools | Tools and Protocols for Process Delivery | Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists | Nodes, Addresses and other Locators | Time Schedules; Clocks, Timers & Interrupts |
| **SERVICE MANAGEMENT ARCHITECTURE** | Service Delivery Management | Operational Risk Management | Process Delivery Management | Personnel Management | Management of Environment | Time Management |
| | Assurance of Operational Continuity & Excellence | Risk Assessment; Risk Monitoring & Reporting; Risk Treatment | Management & Support of Systems, Applications & Services | Account Provisioning; User Support Management | Management of Buildings, Sites, Platforms & Networks | Management of Calendar and Timetable |

# 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

**These five principles drive control objectives categorized into seven enablers:**

- **Principles, policies, and frameworks**
- **Processes**
- **Organizational structures**
- **Culture, ethics, and behavior**
- **Information**
- **Services, infrastructure, and applications**
- **People, skills, and competencies**

# National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series

- Describe US Federal Gov't computer security policies, procedures, and guidelines

- **SP 800-12 Rev. 1:** Introduces information security principles.
- **SP 800-16 Rev. 1:** Describes information technology/cybersecurity role-based training for federal departments, agencies, and organizations.
- **SP 800-18 Rev. 1:** Provides guidelines for developing security plans for federal information systems.

- **SP 800-175A and B:** Provide guidelines for using cryptographic standards in the federal government.
- **SP 800-181:** Describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework).
- **SP 800-183:** Describes the Internet of Things (IoT).

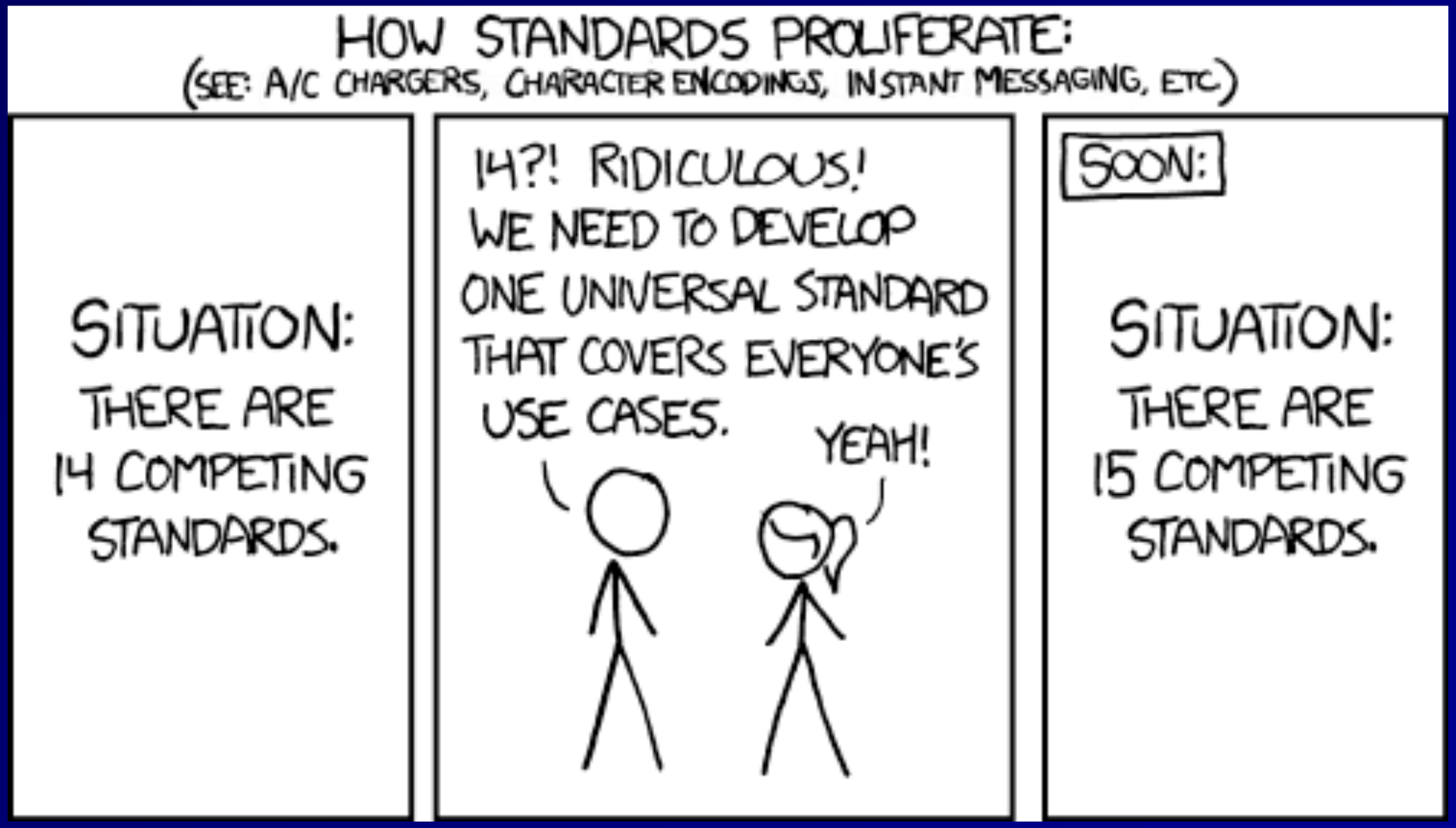
https://www.govtech.com/security/1B-Department-of-Defense-Audit-Stresses-Cybersecurity-Failings.html

# $1B Department of Defense Audit Stresses Cybersecurity Failings

*The roughly year-long assessment, which began in December 2017, highlighted issues with inventory accuracy and complying with cybersecurity discipline, and prompted nearly $560 million in remediation and system fixes.*

**BY CAITLIN M. KENNEY, STARS AND STRIPES** / NOVEMBER 20, 2018

Shanahan said the audit, which began in December 2017, revealed many issues including inventory accuracy and complying with cybersecurity discipline. The audit itself cost $413 million. But in addition, the Pentagon has spent $406 million on audit remediation and $153 million on financial system fixes.


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

# HITRUST CSF

- Privately held US company
- Works with healthcare, technology, and information security leaders
- Establishes Common Security Framework (CSF)
  - To address requirements of multiple regulations and standards
- Primarily used in healthcare industry

**This framework has 14 control categories:**

**0.0: Information Security Management Program**

**1.0: Access Control**

**2.0: Human Resources Security**

**3.0: Risk Management**

**4.0: Security Policy**

**5.0: Organization of Information Security**

**6.0: Compliance**

**7.0: Asset Management**

**8.0: Physical and Environmental Security**

**9.0: Communications and Operations Management**

**10.0: Information Systems Acquisition, Development, and Maintenance**

**11.0: Information Security Incident Management**

**12.0: Business Continuity Management**

**13.0: Privacy Practices**

# CIS Critical Security Controls

- From Center for Internet Security
- The first 5 controls eliminate most vulns

1. **Inventory and control of hardware assets**
2. **Inventory and control of software assets**
3. **Continuous vulnerability management**
4. **Controlled use of administrative privileges**
5. **Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers**

6. Maintenance, monitoring, and analysis of audit logs
7. Email and web browser protections
8. Malware defenses
9. Limitation and control of network ports, protocols, and services
10. Data recovery capabilities
11. Secure configurations for network devices, such as firewalls, routers, and switches

**12. Boundary defense**

**13. Data protection**

**14. Controlled access based on the need to know**

**15. Wireless access control**

**16. Account monitoring and control**

**17. Implement a security awareness training program**

**18. Application software security**

**19. Incident response and management**

**20. Penetration tests and red team exercises**

# Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework

- Five interrelated components:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring activities
- COBIT is the IT governance framework derived from COSO, which is for corporate governance

# Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

- Developed at Carnegie Mellon
- An organization implements small teams that work together to address security needs
- Most recent version is OCTAVE Allegro

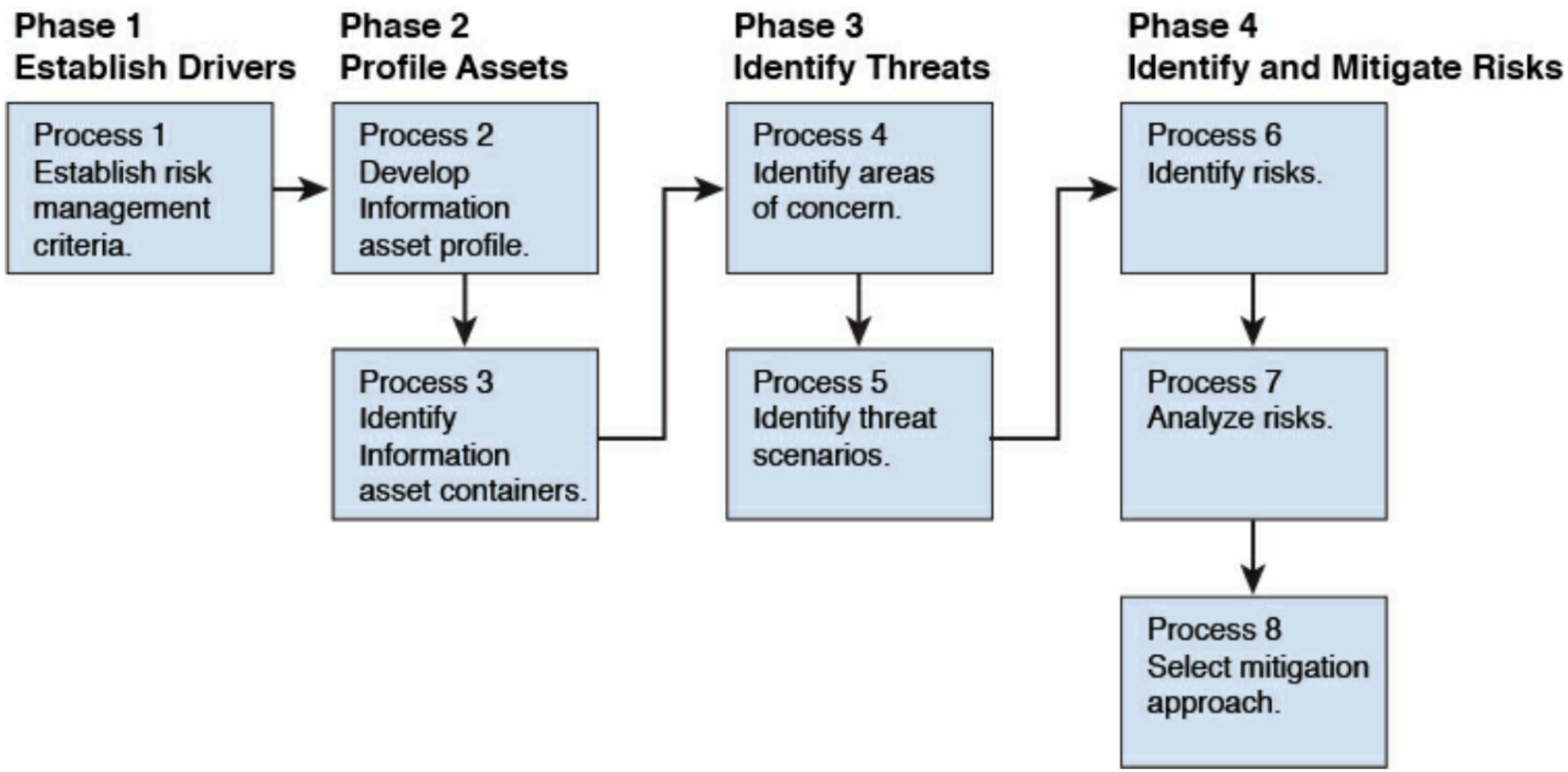



**Figure 1-2 OCTAVE Allegro Phases and Processes**

# Information Technology Infrastructure Library (ITIL)

- Process management standard
- Developed by the Office of Management and Budget
  - In OMB Circular A-130
- Five core publications
  - ITIL Service Strategy
  - ITIL Service Design
  - ITIL Service Transition
  - ITIL Service Operation
  - ITIL continual Service Improvement

# ITIL

- Has a security component
- Primarily concerned with managing service-level agreements (SLAs)
  - Between an IT organization or department
  - And its customers
- Independent review of security controls should be performed every three years

## Table 1-2 ITIL v3 Core Publications and Processes

| ITIL Service Strategy | ITIL Service Design | ITIL Service Transition | ITIL Service Operation | ITIL Continual Service Improvement |
|---|---|---|---|---|
| Strategy Management | Design Coordination | Transition Planning and Support | Event Management | Continual Service Improvement |
| Service Portfolio Management | Service Catalogue | Change Management | Incident Management | |
| Financial Management for IT Services | Service Level Management | Service Asset and Configuration Management | Request Fulfillment | |
| Demand Management | Availability Management | Release and Deployment Management | Problem Management | |
| Business Relationship Management | Capacity Management | Service Validation and Testing | Access Management | |
| | IT Service Continuity Management | Change Evaluation | | |
| | Information Security Management System | Knowledge Management | | |
| | Supplier Management | | | |

# Six Sigma

- Process improvement standard

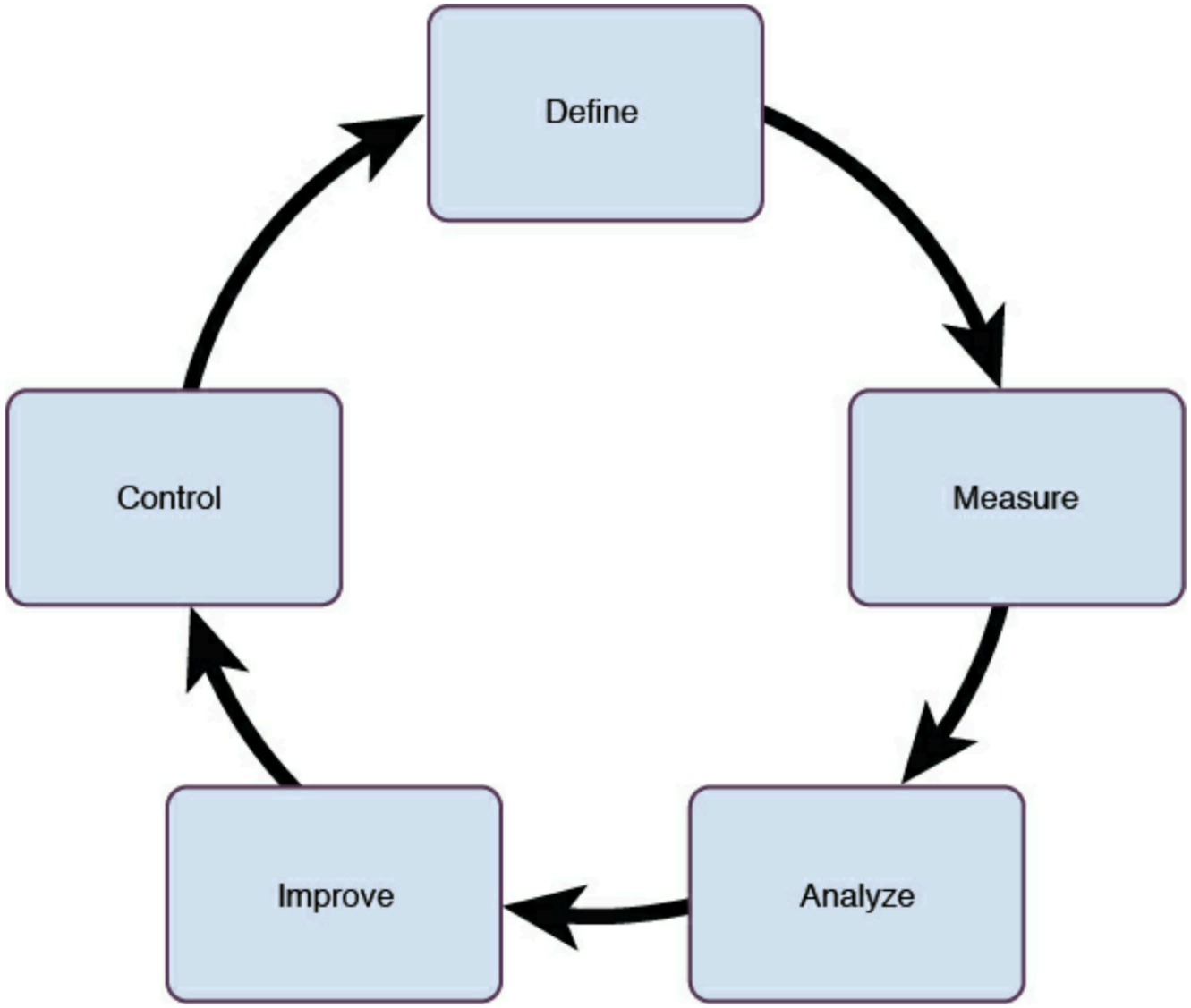



**Figure 1-3** Six Sigma DMAIC

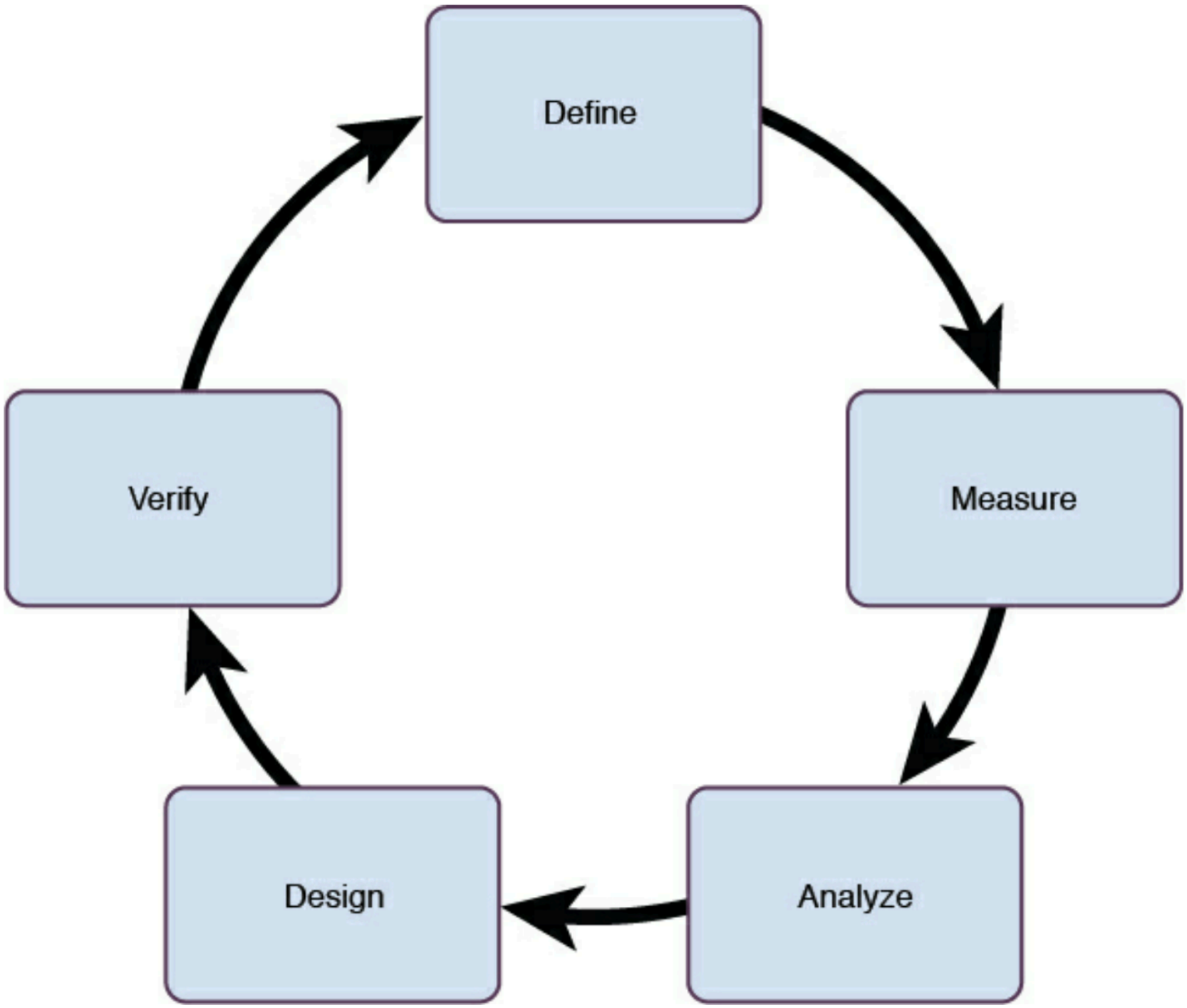



**Figure 1-4** Six Sigma DMADV

# Capability Maturity Model Integration (CMMI)

- Process improvement approach
- Three areas of interest
  - Product and service development
    - CMMI for development
  - Service establishment and management
    - CMMI for services
  - Product service and acquisition
    - CMMI for acquisitions

# CMMI Maturity Levels

- Level 1 Initial
- Level 2 Managed
- Level 3 Defined
- Level 4 Quantitatively Managed
- Level 5 Optimizing

# CCTA Risk Analysis and Management Method (CRAMM)

- Risk analysis and management tool
- Developed by the UK Gov't's Central Computer and Telecommunications Agency (CCTA)
- CRAMM review has three steps

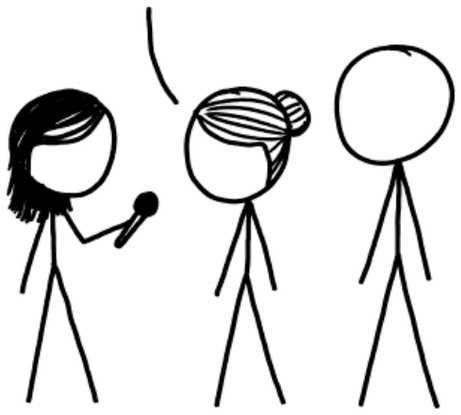
**1. Identify and value assets.**

**2. Identify threats and vulnerabilities and calculate risks.**

**3. Identify and prioritize countermeasures.**

ASKING AIRCRAFT DESIGNERS ABOUT AIRPLANE SAFETY:

NOTHING IS EVER FOOLPROOF, BUT MODERN AIRLINERS ARE INCREDIBLY RESILIENT. FLYING IS THE SAFEST WAY TO TRAVEL.

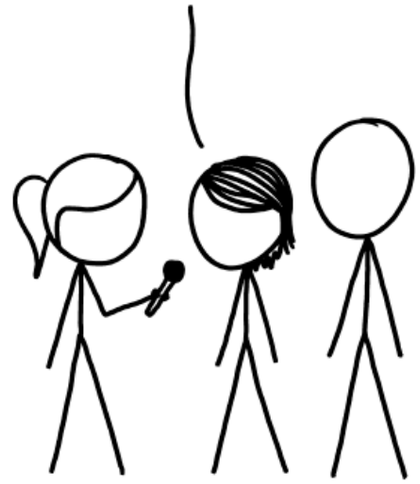


ASKING BUILDING ENGINEERS ABOUT ELEVATOR SAFETY:

ELEVATORS ARE PROTECTED BY MULTIPLE TRIED-AND-TESTED FAILSAFE MECHANISMS. THEY'RE NEARLY INCAPABLE OF FALLING.

ASKING SOFTWARE ENGINEERS ABOUT COMPUTERIZED VOTING:

THAT'S *TERRIFYING.*



WAIT, REALLY?

DON'T TRUST VOTING SOFTWARE AND DON'T LISTEN TO ANYONE WHO TELLS YOU IT'S SAFE.

WHY?

I DON'T QUITE KNOW HOW TO PUT THIS, BUT OUR ENTIRE FIELD IS BAD AT WHAT WE DO, AND IF YOU RELY ON US, EVERYONE WILL DIE.

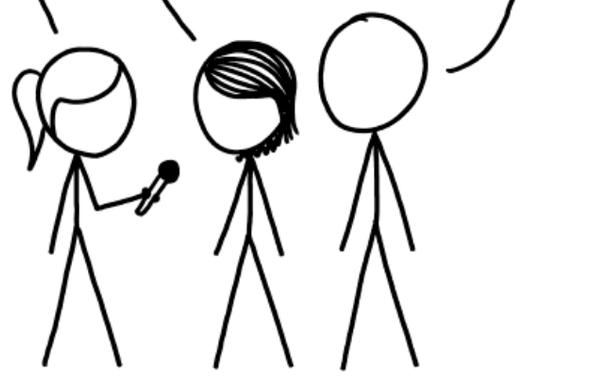
THEY SAY THEY'VE FIXED IT WITH SOMETHING CALLED "BLOCKCHAIN."

AAAAA!!!

WHATEVER THEY SOLD YOU, DON'T TOUCH IT.

BURY IT IN THE DESERT.

WEAR GLOVES.



# 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


1d

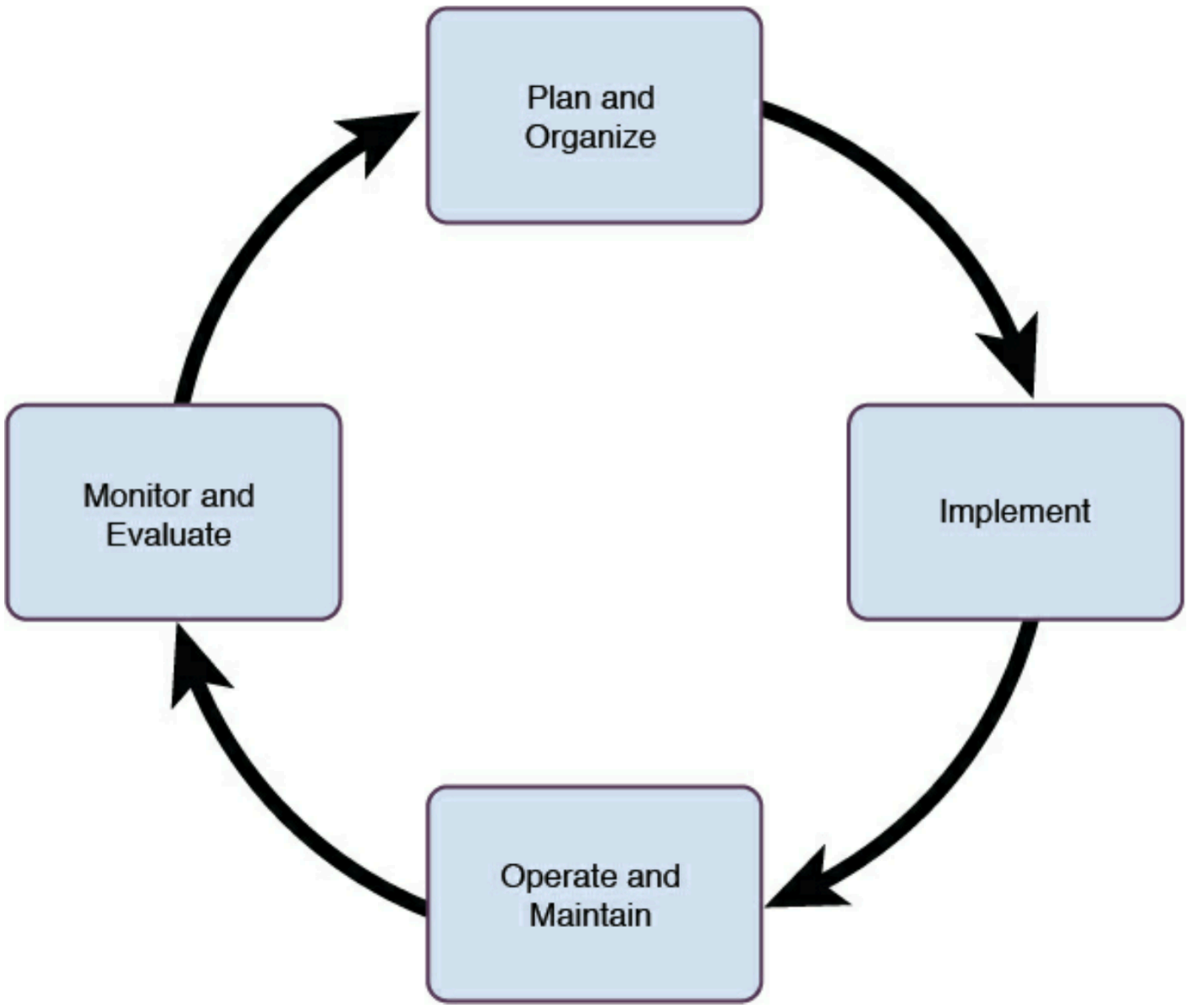
## Security Program Life Cycle

**Any security program has a continuous life cycle and should be assessed and improved constantly. The security program life cycle includes the following steps:**

1. **Plan and Organize:** Includes performing risk assessment, establishing management and steering committee, evaluating business drivers, and obtaining management approval.
2. **Implement:** Includes identifying and managing assets, managing risk, managing identity and access control, training on security and awareness, implementing solutions, assigning roles, and establishing goals.
3. **Operate and Maintain:** Includes performing audits, carrying out tasks, and managing SLAs.
4. **Monitor and Evaluate:** Includes reviewing auditing and logs, evaluating security goals, and developing improvement plans for integration into the Plan and Organize step (step 1).

**Figure 1-5 shows a diagram of the security program life cycle.**

Key Topic



# Compliance

# Compliance

- Alignment with standards, guidelines, regulations, and/or legislation
- Usually industry-specific
  - PCI-DSS (Payment Card Industry Data Security Standard) for merchants who accept credit card payments
  - HIPAA (Health Insurance Portability and Accountability Act) for healthcare

# Governance, Risk Management, and Compliance (GRC)

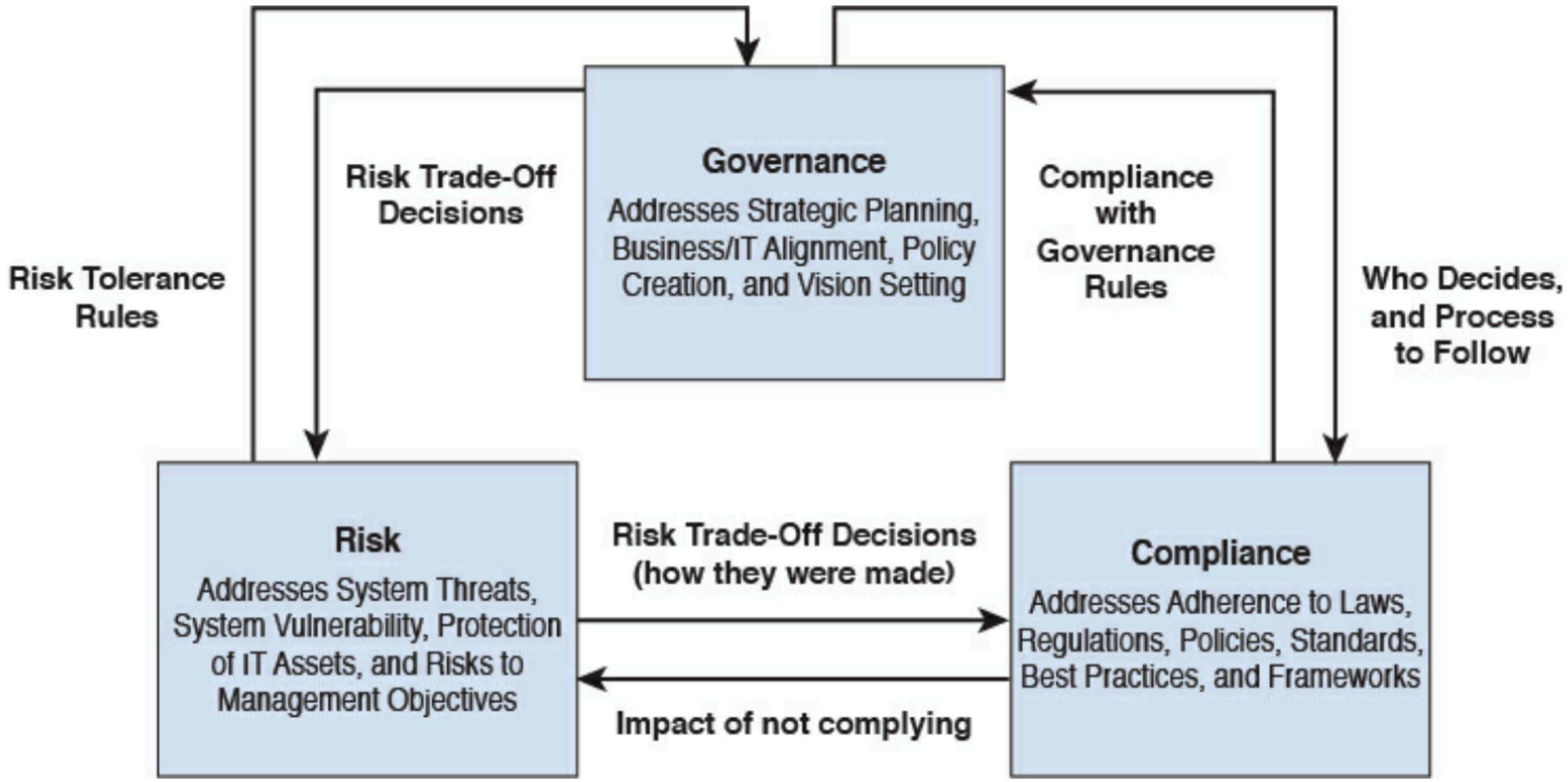



**Figure 1-6** GRC Relationship

# Contractual, Legal, Industry Standards, and Regulatory Compliance

- Laws vary; work with legal team
- Privacy Requirements Compliance
  - Regulates confidentiality of Personally Identifiable Information (PII)
- The General Data Protection Regulation (GDPR) is the new European standard

https://www.theregister.co.uk/2019/04/24/facebook_q1_fy2019_ftc_hit/

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS **PERSONAL TECH** SCIENCE

# Facebook: Not saying we've done anything wrong but... we're just putting $3bn profit aside for an FTC privacy fine

## Net income halved as antisocial network preps for big slap

By Iain Thomson in San Francisco 24 Apr 2019 at 23:18 22 SHARE ▼

# Legal and Regulatory Issues

# Computer Crime

- Computer as **target**
  - DoS, installing malware to send spam
- Computer as a **tool**
  - Stealing secrets from a database
  - Stealing credit card numbers
  - Espionage
  - Harassment
- **Attribution**
  - Difficult to prove who did a crime

# Major Legal Systems

- **Civil Law**
  - Laws and statutes determine what is allowed
  - Precedents and particular case rulings carry less weight than under **common law**
- **Common Law**
  - Used in the USA, Canada, the UK, and former British colonies
  - Significant emphasis on particular cases and precedents as determinants of laws
  - The major legal system in the CISSP exam

# Religious and Customary Law

- **Religious Law**
  - Mainly *Sharia* (Islamic religious law)
- **Customary Law**
  - Customs or practices that are commonly accepted and treated as law
  - Closely related to **Best Practices**
  - Less important

# Criminal and Civil Law

- **Criminal Law**
  - Victim is society itself
  - Enforced by police
  - Punishment is often prison time
  - Proof must be beyond a reasonable doubt
- **Civil Law (Tort Law)**
  - Injury resulting from failure to provide due care
  - Victim is an individual
  - Enforced by lawsuits
  - Result is financial damages paid to victim
  - Burden of proof: **preponderance of the evidence** (more likely than not)

## Table 2.1

### Common Types of Financial Damages

| Financial Damages | Description |
|---|---|
| Statutory | Statutory damages are those prescribed by law, which can be awarded to the victim even if the victim incurred no actual loss or injury. |
| Compensatory | The purpose of compensatory damages is to provide the victim with a financial award in effort to compensate for the loss or injury incurred as a direct result of the wrongdoing. |
| Punitive | The intent of punitive damages is to punish an individual or organization. These damages are typically awarded to attempt to discourage a particularly egregious violation where the compensatory or statutory damages alone would not act as a deterrent. |

# Administrative Law

- Also called **Regulatory Law**
- Specify rules and punishments for regulated industries
- Examples
  - FCC regulations
  - HIPAA security mandates
  - FDS regulations
  - FAA regulations

# Liability

- Due Care
  - Also called **Duty of Care**
  - **Prudent Man Rule**
    - Businesses should do what a prudent man would do
  - Best Practices
- Due Diligence
  - The management of due care
  - Follows a formal process

# Intellectual Property

- **Trademark**
  - Name, logo, or symbol used for marketing
  - Unregistered ™ or Registered ®
- **Patent**
  - Grants a monopoly for an invention
- **Copyright ©**
  - Restricts copying creative work
  - Software typically covered by copyright
  - **Fair sale** & **fair use** are allowed

# Intellectual Property

- **Licenses**
  - End-User License Agreement (EULA)
- **Trade secrets**
  - Special sauce
  - Protected by non-disclosure agreements (NDAs) & non-compete agreements (NCAs)

# Intellectual Property Attacks

- Software piracy
- Copyright infringement
- Corporate espionage
- Cybersquatting & Typosquatting
  - Using a domain close to a company's domain, like *yahoo.net* or *yahooo.com*

# Digital Rights Management (DRM)

- Controls use of digital content
- Digital Millennium Copyright Act (DMCA) of 1998
  - Imposes penalties on those who make available technologies to circumvent copy protection

# Import / Export Restrictions

- USA restricted exports of cryptographic technology in the 1990s
- Restrictions have been relaxed since then
- But cryptography is still regulated
- https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-country-groups-1/file

# Export of cryptography from the United States

From Wikipedia, the free encyclopedia

## U.S. export rules [ edit ]

U.S. non-military exports are controlled by Export Administration Regulations (EAR), a short name for the U.S. Code of Federal Regulations (CFR) Title 15 chapter VII, subchapter C.

Export destinations are classified by the EAR Supplement No. 1 to Part 740 into four *country groups* (A, B, D, E) with further subdivisions;[14] a country can belong to more than one group. For the purposes of encryption, groups B, D:1, and E:1 are important:

- **B** is a large list of countries that are subject to relaxed encryption export rules
- **D:1** is a short list of countries that are subject to stricter export control. Notable countries on this list include China and Russia
- **E:1** is a very short list of "terrorist-supporting" countries (as of 2009, includes five countries; previously contained six countries and was also called "terrorist 6" or T-6)

# Example Countries

- Group B (Relaxed)
  - Canada, Israel, Japan, Jordan, Saudi Arabia, Singapore
- Group D-1 (Stricter)
  - China,  Iraq, N Korea, Russia

# Cyber Crimes and Data Breaches

- Data Breach
  - Confidential information is exposed to unauthorized parties
- Cyber Crime
  - Any criminal act carried out with computers or the Internet
- Going Dark
  - Inability of law enforcement to access evidence

# Privacy

- Confidentiality of personal information
- **EU Data Protection Directive**
  - Individuals must be notified how their data is used & allowed to opt out
- **OECD Privacy Guidelines**
  - Organization for Economic Cooperation and Development
  - Includes EU, USA, Mexico, AU & more

# EU-US Safe Harbor

- Part of EU Data Protection Directive
- Sending personal data from EU to other countries is forbidden
  - Unless the receiving country adequately protects its data
- The USA **lost** this privilege in Oct. 2015 because of the Snowden leaks

# Privacy Shield

- Replaced Safe Harbor
- Approved by the EU in 2016 and Switzerland in 2017

# International Cooperation

- Council of Europe Convention on Cybercrime
  - Includes most EU countries and the USA
  - Promotes cooperation

# Important Laws and Regulations

# HIPAA

- Health Insurance Portability and Accountability Act
- Guidance on Administrative, Physical, and Technical safeguards
- For Protected Health Information (PHI)

# CFAA

- Computer Fraud and Abuse Act
- Protects government and financial computers
  - Including every computer on the Internet (probably not the law's original intent)
- It's a crime to exceed your authorization to use such a computer

# ECPA & The PATRIOT Act

- Electronic Communications Privacy Act
- Protected electronic communications from warrantless wiretapping
- Weakened by the PATRIOT Act
- The PATRIOT Act
  - A response to 9/11 attacks
  - Greatly expanded law enforcement's electronic monitoring capabilities

# GLBA & SOX

- Gramm-Leach-Bailey Act
  - Forces financial institutions to protect customer financial information
- Sarbanes-Oxley Act
  - Response to ENRON scandal
  - Regulatory compliance mandates for publicly traded companies
  - Ensures financial disclosure and auditor independence

# PCI-DSS

- Payment Card Industry Data Security Standard
- Self-regulation by major vendors
- Mandates security policy, devices, controls, and monitoring to protect cardholder data

# US Breach Notification Laws

- 47 states require notification
- No federal law yet
- Safe harbor for data that was encrypted at time of compromise

# Professional Ethics

# (ISC)^2 Code of Ethics

- Four Canons
  - Protect society, the commonwealth, and the infrastructure
  - Act honorably, honestly, justly, responsibly, and legally
  - Provide diligent and competent service to principals
  - Advance and protect the profession

# Ethics Complaint


(ISC)²

29 September 2011

Mr. Sam Bowne

[redacted]

***SENT VIA:*** ***USPS Certified Mail***
***Return Receipt Requested***

*RE: Ethics Complaint*

Dear Mr. Bowne:

This letter serves as notice to you that (ISC)² is in receipt of a formal ethics complaint that has been filed against you.

# Accusation

On June 28, 2011, I was reading the ccsf.edu site to learn more about Sam Bowne's role at the college. During the course of normal browsing, I found several concerns on the web site that had serious security concerns. What I observed indicated the possibility a system had been compromised, or was potentially misconfigured in such a way as to mislead visitors into providing sensitive data from third-party sites. Knowing that Bowne is a professor at the college, I asked him through public Twitter messages and direct messages who I should contact, and did not receive reply.

9:51 PM Jun 27th to sambowne - I am serious. Can I get a security contact for ccsf.edu please? Ran into what I consider a serious issue on the web site.
10:11 PM Jun 27th from sambowne - Please tell me what you have found.
10:17 PM Jun 27th to sambowne - I cannot validate that you are the appropriate security contact for the City College of San Francisco.

I called the college directly and received two security contacts in their IT department that would handle security concerns. Neither of those contacts were Sam Bowne. When I emailed the two contacts to provide the information regarding their web site, I also asked if Bowne was a legitimate security contact for such issues. Tim Ryan, Technical Operations Manager for City College of SF (ccsf.edu) indicated that Bowne "is a Faculty Member in our academic Computer Networking Department (CNIT), he is not part of our internal security team".

Sam Bowne misrepresented himself as being a security contact for his university, when he was not. In

# Verdict

## FINDINGS:

While the Complainant accuses the Respondent of misrepresenting his role with his employer, he does not provide any evidence supporting such a claim. Complainant further claimed that Respondent discontinued communication with Complainant; however, we can find no duty incumbent upon the Respondent to respond to Complainant. It is also noted that Complainant admits in his complaint that he "called the college directly and received two security contacts."

## RECOMMENDATION

It is the unanimous recommendation of the Ethics Committee that the $(ISC)^2$ Board of Directors dismiss the complaint with prejudice.

RESPECTFULLY SUBMITTED,

*(ISC) ETHICS COMMITTEE*
18 November 2011


**1e**

# Security Documentation

## Table 2.3

## Summary of Security Documentation

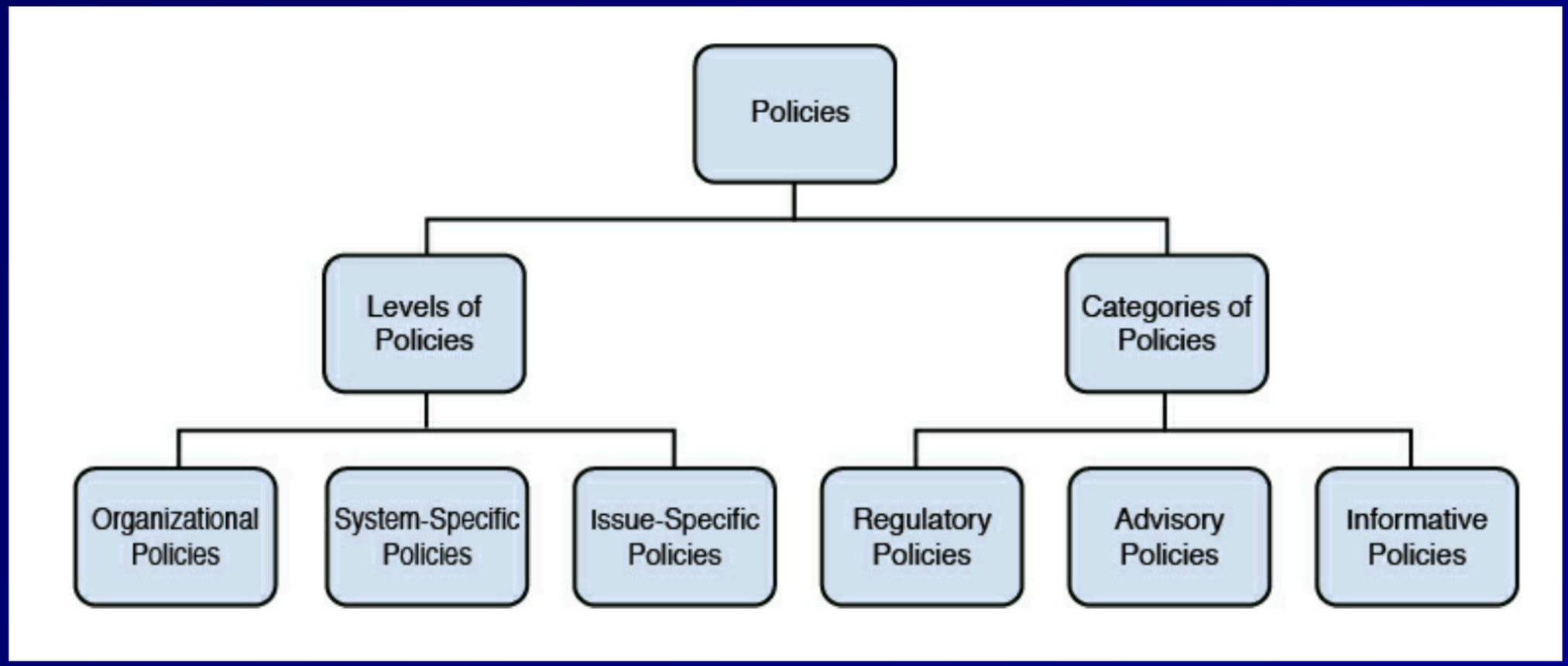
| Document | Example | Mandatory or Discretionary? |
|---|---|---|
| Policy | *Protect the CIA of PII by hardening the operating system* | Mandatory |
| Procedure | *Step 1: Install pre-hardened OS Image. Step 2: Download patches from update server. Step 3: …* | Mandatory |
| Standard | *Use Nexus-6 laptop hardware* | Mandatory |
| Guideline | *Patch installation may be automated via the use of an installer script* | Discretionary |
| Baselines | *Use the CIS Security Benchmarks Windows Benchmark* | Discretionary |

# Security Structure Components

- Policies
- Processes
- Procedures
- Standards
- Guidelines
- Baselines

# 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
- Must contain an exception area


Policies
Levels of Policies
Organizational Policies
System-Specific Policies
Issue-Specific Policies
Categories of Policies
Regulatory Policies
Advisory Policies
Informative Policies

# Types of Security Policies

- Organizational
  - Issues relevant to every aspect of an organization
- Issue-specific
  - Such as a specific network service
  - Like email, privacy, employee termination
- 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

# Processes

- Series of steps or actions to achieve a particular end
- Examples
  - Process to enter an online order
  - Process to process a payment
- Processes then lead to procedures

# Security Procedures

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

# 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

# Guidelines

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

# Baselines

- Reference point
  - Defined and captured for future reference
- Should be captured when the system is properly configured and fully updated

Kahoot!

**1f**

# Business Continuity

# Business Continuity Planning (BCP)

- **Ensures that business will continue to operate before, throughout, and during a disaster**
- **Ensures that critical services can be carried out**
- **Strategic, long-term: focuses on business as a whole**
- **An umbrella plan that includes multiple plans, most importantly the Disaster Recovery Plan (DRP)**

# Disaster Recovery Planning (DRP)

- **Tactical, short-term**
- **Plan to deal with specific disruptions, such as a malware infection**

# Business Impact Analysis (BIA)

- **Determine Maximum Tolerable Downtime (MTD) for specific IT assets**
- **First, identify critical assets**
- **Second, comprehensive risk analysis**
- **Including vulnerability analysis**

| Develop Contingency Planning Policy | Conduct Business Impact Analysis | Identify Preventive Controls | Create Contingency Strategies | Develop Contingency Plan* | Plan Testing, Training, and Exercises | Plan Maintenance |
|---|---|---|---|---|---|---|
| • Identify Statutory or Regulatory Requirements<br>• Develop IT Contingency Planning Policy Statement<br>• Reflect FIPS 199<br>• Publish Policy | • Determine Business Processes and Recovery Criticality<br>• Identify Outage Impacts and Estimated Downtime<br>• Identify Resource Requirements<br>• Identify Recovery Priorities for System | • Identify Controls<br>• Implement Controls<br>• Maintain Controls | • Backup and Recovery<br>• Consider FIPS 199<br>• Identify Roles and Responsibilities<br>• Address Alternate Site<br>• Identify Equipment and Cost Considerations<br>• Integrate into System Architecture | • Document Recovery Strategy | • Plan Testing<br>• Train Personnel<br>• Plan Exercises<br>• TT&E Activities | • Review and Update Plan<br>• Coordinate with Internal/ External Organizations<br>• Control Distribution<br>• Document Changes |

**Figure 1-12 NIST Special Publication 800-34 Rev. 1**

# Personnel Security Policies and Procedures

# Personnel Security Policies and Procedures

- Candidate Screening
- Employment Agreements and Policies
- Non-Disclosure Agreement (NDA)
- Acceptable Use Policy (AUP)
- Code of Conduct
- Conflict of Interest
- Ethics

# Employee Onboarding and Offboarding

- Onboarding
  - Orientation and provisioning
- Offboarding (Termination)
  - Knowledge transfer
  - Exit interview

# Job Rotation and Separation of Duties

- **Job Rotation**
  - Moves personnel from one job to another periodically
  - Prevents one person from being irreplaceable
  - Helps to detect fraud
- **Separation of Duties** requires two or more people to work on portions of a task
  - Prevents fraud without collusion

# Risk Management Concepts

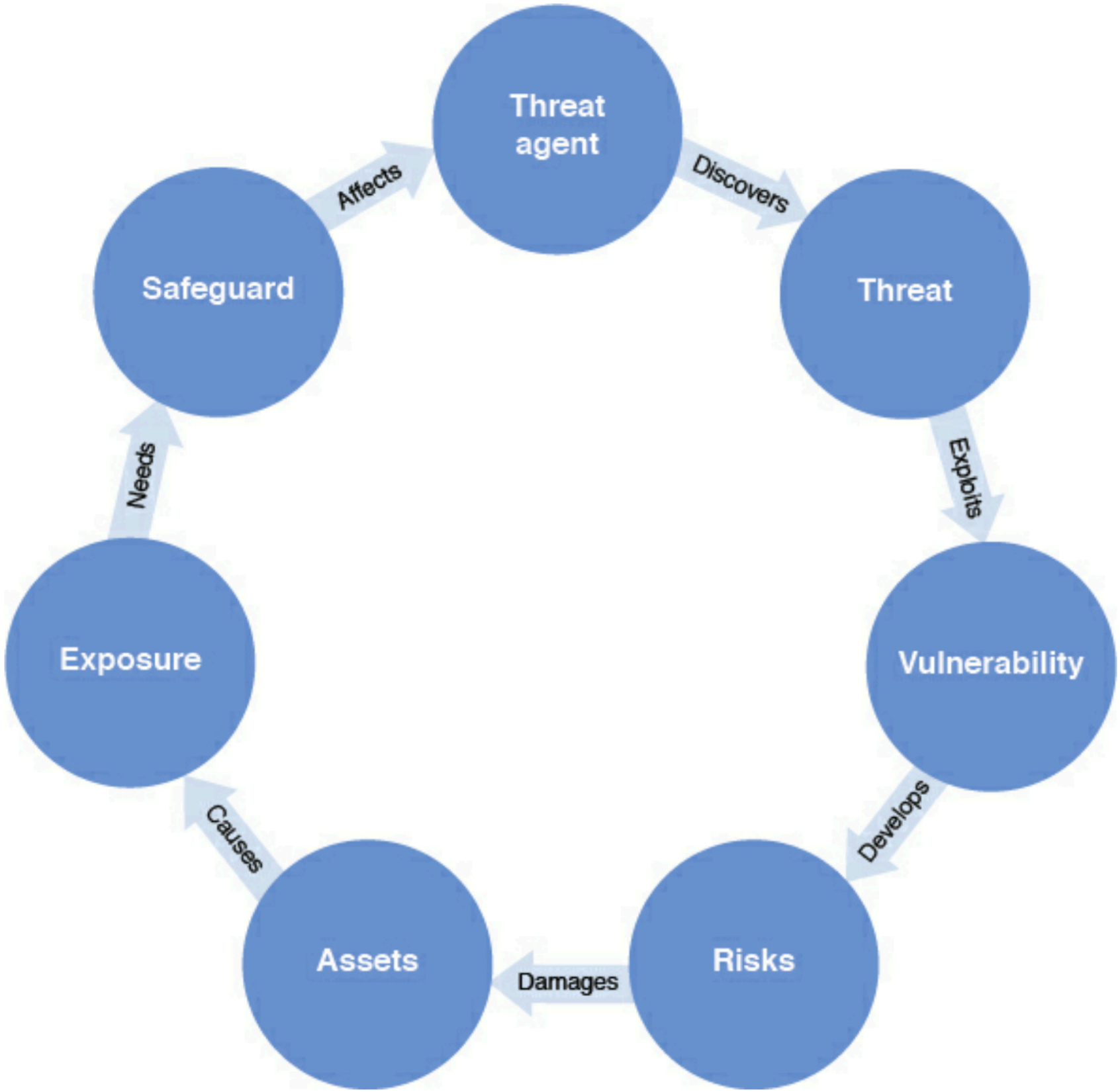



**Figure 1-13** Security Concept Cycle

# Risk Assesment/Analysis

# Risk Analysis

- Assets
  - Valuable resources to protect
- Threat
  - A potentially harmful occurrence
- Vulnerability
  - A weakness

# Risk = Threat x Vulnerability

- Earthquake risk is the same in Boston and San Francisco
- Boston
  - Earthquakes are rare, but buildings are old and vulnerable
- San Francisco
  - Earthquakes are common, but buildings are newer and safer

# Impact

- Severity of the damage in dollars
- Risk = Threat x Vulnerability x Impact
- Human life is considered near-infinite impact

## Table 2.4

### Risk Analysis Matrix

| | | Consequences | | | | |
|---|---|---|---|---|---|---|
| | | Insignificant 1 | Minor 2 | Moderate 3 | Major 4 | Catastrophic 5 |
| Likelihood | 5. Almost Certain | H | H | E | E | E |
| | 4. Likely | M | H | H | E | E |
| | 3. Possible | L | M | H | E | E |
| | 2. Unlikely | L | L | M | H | E |
| | 1. Rare | L | L | M | H | H |

## Table 2.5

## Summary of Risk Equations

| | Formula | Description |
|---|---|---|
| **Asset Value (AV)** | **AV** | Value of the Asset |
| **Exposure Factor (EF)** | **EF** | Percentage of Asset Value Lost |
| **Single Loss Expectancy (SLE)** | **AV x EF** | Cost of One Loss |
| **Annual Rate of Occurrence (ARO)** | **ARO** | Number of Losses per Year |
| **Annualized Loss Expectancy (ALE)** | **SLE x ARO** | Cost of Losses per Year |

# Total Cost of Ownership (TCO)

- Of a mitigating safeguard includes
  - Upfront costs
  - Annual cost of maintenance
    - Staff hours
    - Maintenance fees
    - Software subscriptions

# Return on Investment (ROI)

- Amount of money saved by implementing a safeguard
- If Total Cost of Ownership is less than Annualized Loss Expectancy, you have a positive ROI

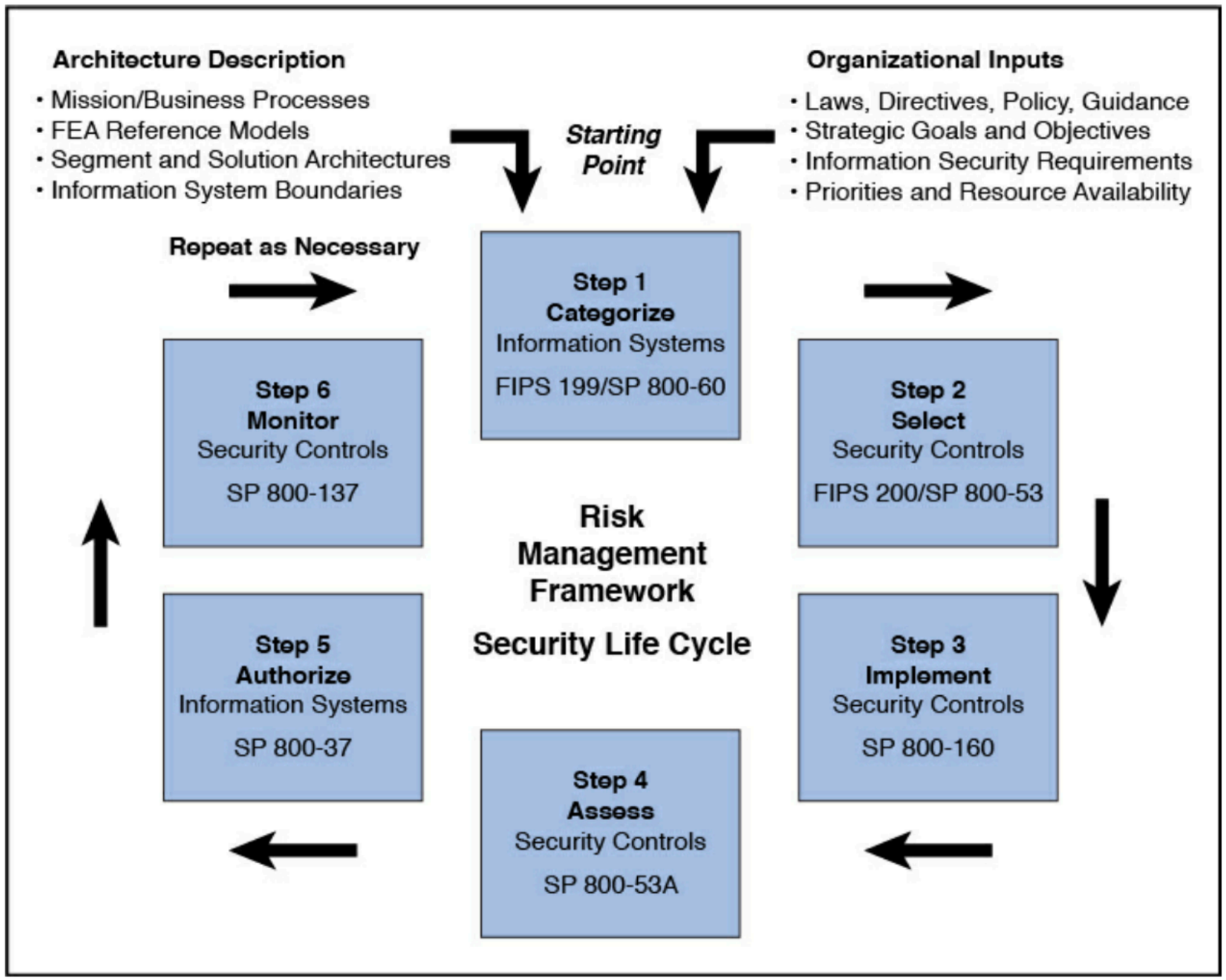
# Risk Choices

- Accept the risk
- Mitigate the risk
- Transfer the risk
- Risk avoidance

# Quantitative and Qualitative Risk Analysis

- Quantitative
  - Uses hard metrics, like dollars
- Qualitative
  - Use simple approximate values
  - Or categories like High, Medium, Low

**Figure 1-14 shows the NIST risk management framework.**



# Control Categories and Types

# Access Control Types

- Preventive
- Detective
- Corrective
- Recovery
- Deterrent
- Compensating

# Access Control Types

- Preventive
  - Prevents actions, such as limited privileges
- Detective
  - Alerts during or after an attack, like video surveillance
- Corrective
  - Corrects a damaged system or process, like antivirus removing a suspicious file

# Access Control Types

- Recovery
  - Restores functionality after a security incident, such as restoring from backups
- Deterrent
  - Scares away attackers, like a "Beware of Dog" sign
- Compensating
  - Additional control to compensate for weakness in other controls
  - e. g. reviewing server logs to detect violations of the Computer Use Policy (an administrative control)

# Access Control Categories

- Administrative
  - Policy, procedure, or regulation
- Technical
  - Software, hardware, or firmware
- Physical
  - Locks, security guards, etc.

# Threat Modeling

# Threat Modeling

- Application-centric
- Asset-centric
- Attacker-centric

1. **Identify assets.**
2. **Identify threat agents and possible attacks.**
3. **Research existing countermeasures in use by the organization.**
4. **Identify any vulnerabilities that can be exploited.**
5. **Prioritize the identified risks.**
6. **Identify countermeasures to reduce the organization’s risk.**

# Microsoft STRIDE Threat Categorization

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege
- Other modeling tools: PASTA, Trike, VAST

| What Users Want in a Threat Modeling Methodology | | | | |
|---|---|---|---|---|
| | **STRIDE** | **PASTA** | **Trike** | **VAST** |
| **Implements application security at design time** | ✓ | ✓ | ✓ | ✓ |
| **Identifies relevant mitigating controls** | ✓ | ✓ | ✓ | ✓ |
| **Directly contributes to risk management** | | ✓ | ✓ | ✓ |
| **Prioritizes threat mitigation efforts** | | ✓ | ✓ | ✓ |
| **Encourages collaboration among all stakeholders** | | | ✓ | ✓ |
| **Outputs for stakeholders across the organization** | | | | ✓ |
| **Consistent repeatability** | | | ✓ | ✓ |
| **Automation of threat modeling process** | | | ✓ | ✓ |
| **Integrates into an Agile DevOps environment** | | | | ✓ |
| **Ability to scale across thousands of threat models** | | | | |

# Risks in the Supply Chain

- Hardware, Software, Services
- Third-Party Assessment and Monitoring
- Service Level Agreements


1g