CISSP® Common Body of Knowledge Review

Information Security Governance & Risk Management Domain

Version: 5.10

CISSP Common Body of Knowledge Review by Alfred Ouyang is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Learning Objectives

Information Security & Risk Management Domain …1/3

The Information Security Governance and Risk Management domain entails the identification of an organization’s information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

Reference: *CISSP CIB*, January 2012 (4.17.14 Rev. 13)

cc BY-NC-SA

Learning Objectives

Information Security & Risk Management Domain ...2/3

The candidate is expected to understand the planning, organization, roles, and responsibilities of individuals in identifying and securing organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary, and private information; third party management and service level agreements related to information security; employment agreements, employee hiring and termination practices, and risk management practices, and tools to identify, rate, and reduce the risk to specific resources.

Reference: *CISSP CIB*, January 2012 (4.17.14 Rev. 13)

(cc) BY-NC-SA

Learning Objectives

Information Security & Risk Management Domain ...3/3

New knowledge requirement for 2012 & 2013:

- Management knowledge in budget, metrics, and resources for security programs.
- Privacy requirements compliance. (Will this topic in the Legal, Regulations, Investigations and Compliance domain.)

Reference: *CISSP CIB*, January 2012 (4.17.14 Rev. 13)

(cc) BY-NC-SA

Topics

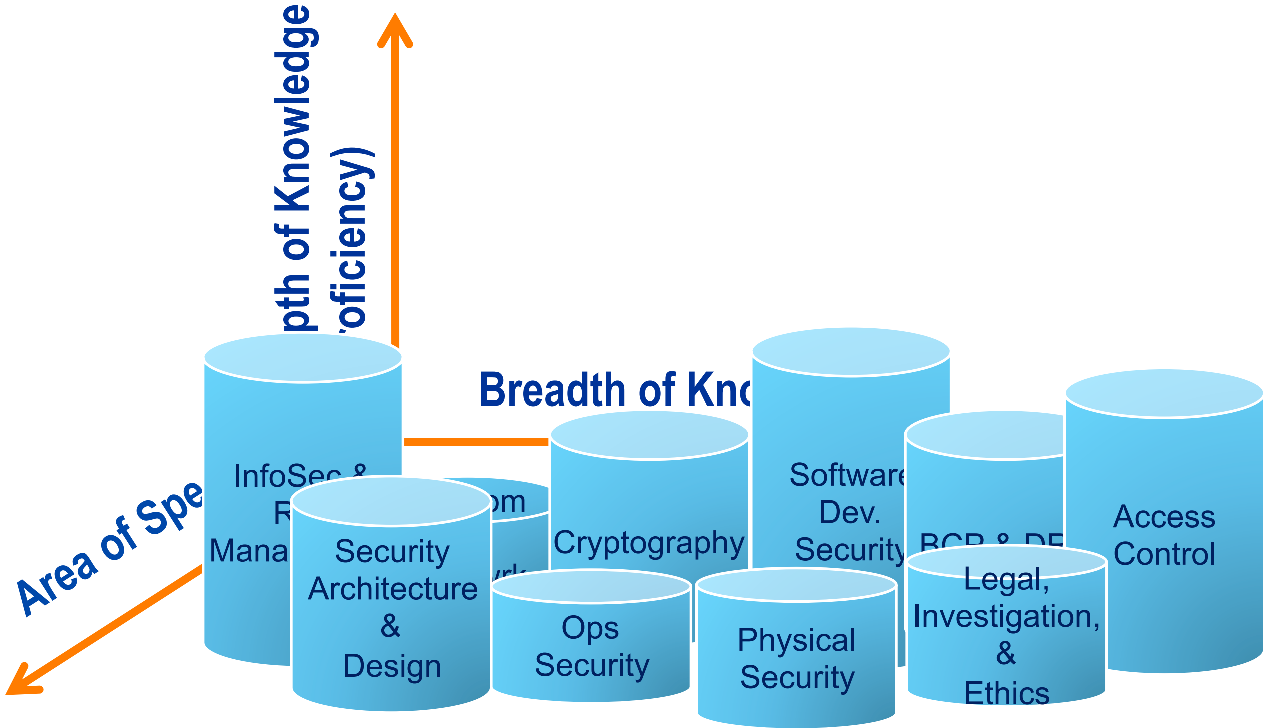
Information Security & Risk Management Domain

➡ Information Security Concept
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Dimensions of Information Security Practice

- Area of Specialty
  - Securely Provision; Operate & Maintain; Protect & Defend; Investigate; Collect & Operate; Analyze; and Oversight & Development.
- Breadth of Disciplines
  - Families of security controls, security technologies, best-practices, etc. (e.g., CISSP, CISM, CISA)
- Depth of Knowledge
  - Systems/software/network engineering, cryptography, IT governance, vulnerability assessment, security certification & accreditation, etc.



(cc) BY-NC-SA

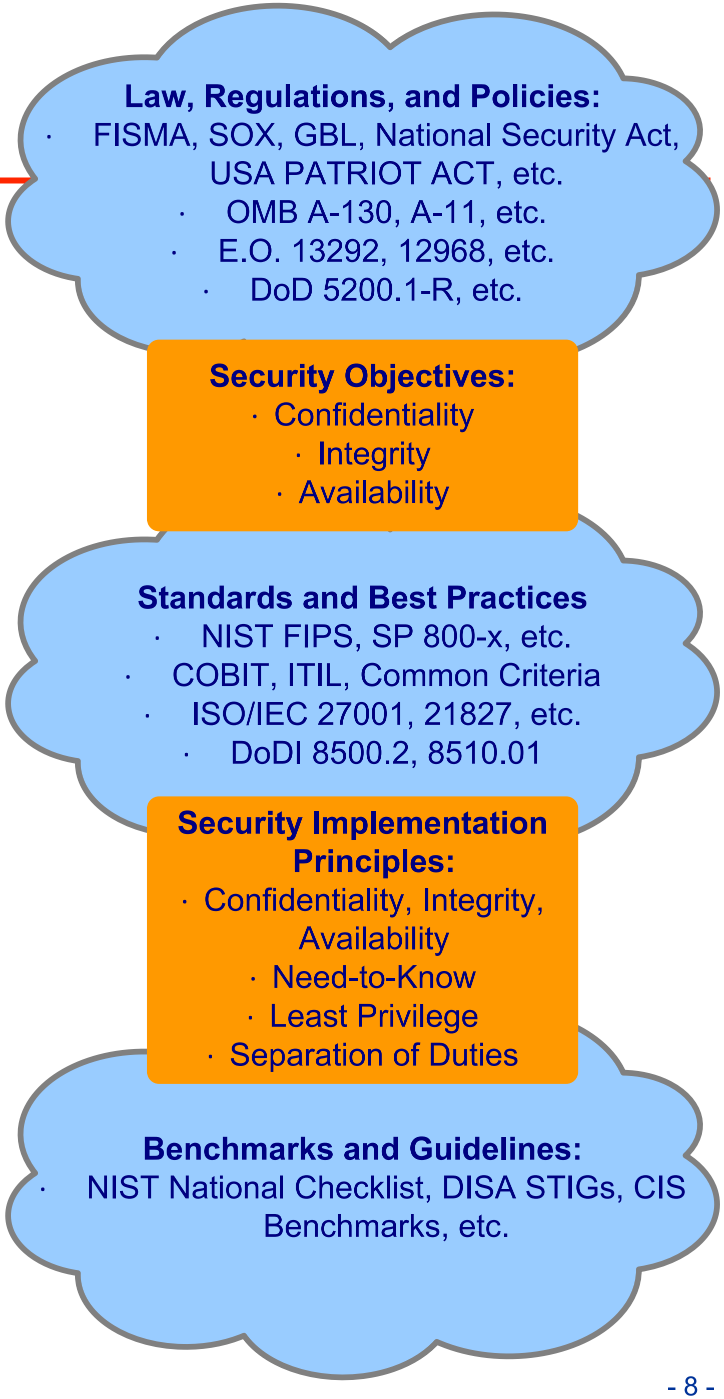
Security Objectives

- Confidentiality
  - “Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.” (44 USC Sec. 3542)
- Integrity
  - “Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.” (44 USC Sec. 3542)
- Availability
  - “Ensuring timely and reliable access and use of information.” (44 USC Sec. 3542)

(cc) BY-NC-SA

Security Implementation Principles

- Confidentiality, Integrity, Availability
- Need-to-know
  - – Users should only have access to information (or systems) that enable them to perform their assigned job functions.
- Least privilege
  - – Users should only have sufficient access privilege that allow them to perform their assigned work.
- Separation of duties
  - – No person should be responsible for completing a task involving sensitive, valuable or critical information from the beginning to end.
  - – No single person should be responsible for approving his/her own work.



Law, Regulations, and Policies:
- FISMA, SOX, GBL, National Security Act, USA PATRIOT ACT, etc.
- OMB A-130, A-11, etc.
- E.O. 13292, 12968, etc.
- DoD 5200.1-R, etc.

Security Objectives:
- Confidentiality
- Integrity
- Availability

Standards and Best Practices
- NIST FIPS, SP 800-x, etc.
- COBIT, ITIL, Common Criteria
- ISO/IEC 27001, 21827, etc.
- DoDI 8500.2, 8510.01

Security Implementation Principles:
- Confidentiality, Integrity, Availability
- Need-to-Know
- Least Privilege
- Separation of Duties

Benchmarks and Guidelines:
- NIST National Checklist, DISA STIGs, CIS Benchmarks, etc.

(cc) BY-NC-SA

Security Best Practices

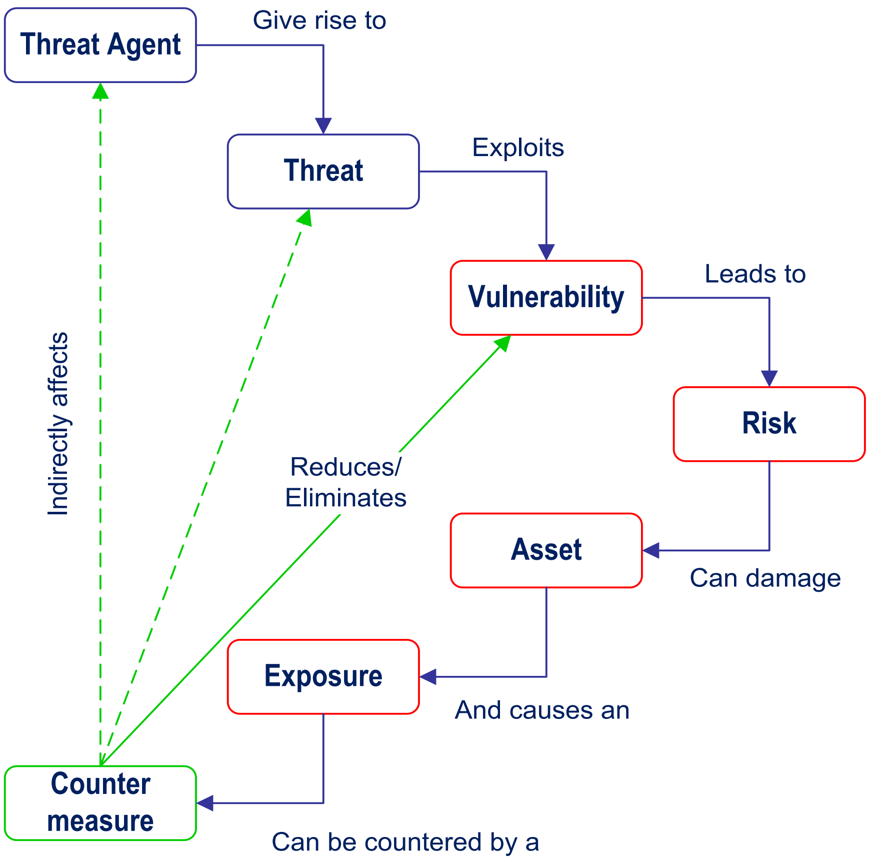
- Confidentiality
- Integrity
- Availability
- Need-to-know
- Least privilege
- Separation of duties
- Job rotation
  - To reduce risk of collusion
  - To ensure no single point of failure
- Mandatory vacation
  - To allow auditors to review records

http://youtu.be/b63hL4gq1Wg

(cc) BY-NC-SA

Relationships between Threat, Risk, and Countermeasure

- Threat Agent. An entity that may act on a vulnerability.
- Threat. Any potential danger to information life cycle.
- Vulnerability. A weakness or flaw that may provide an opportunity for a threat agent.
- Risk. The likelihood of a threat agent exploits the discovered vulnerability.
- Exposure. An instance of being compromised by a threat agent.
- Countermeasure / safeguard. An administrative, operational, or logical mitigation against potential risk(s).



Reference: *Information Assurance Technical Framework (IATF)*, Release 2.3

(cc) BY-NC-SA

Security Controls

"Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information."

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have the selected controls or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented are effective in their application?

Reference: NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems*.

(cc) BY-NC-SA

Categories of Security Controls ...(1/4)

- Management (Administrative) Controls.
  - Policies, Standards, Processes, Procedures, & Guidelines
    - Administrative Entities: Executive-Level, Mid.-Level Management
- Operational (and Physical) Controls.
  - Operational Security (Execution of Policies, Standards & Process, Education & Awareness)
    - Service Providers: IA, Program Security, Personnel Security, Document Controls (or CM), HR, Finance, etc
  - Physical Security (Facility or Infrastructure Protection)
    - Locks, Doors, Walls, Fence, Curtain, etc.
    - Service Providers: FSO, Guards, Dogs
- Technical (Logical) Controls.
  - Access Controls, Identification & Authorization, Confidentiality, Integrity, Availability, Non-Repudiation.
    - Service Providers: Enterprise Architect, Security Engineer, CERT, NOSC, Helpdesk.

(cc) BY-NC-SA

Categories of Security Controls …(2/4)

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Security Assessment and Authorization	CA
	Program Management	**PM**
Operational	Personnel Security	PS
	Physical and Environmental Protection	PE
	Contingency Planning	CP
	Configuration Management	CM
	Maintenance	MA
	System and Information Integrity	SI
	Media Protection	MP
	Incident Response	IR
	Awareness and Training	AT
Technical	Identification and Authentication	IA
	Access Control	AC
	Audit and Accountability	AU
	System and Communications Protection	SC

Reference: NIST SP800-53, Rev 3, *Recommended Security Controls for Federal Information Systems*

cc BY-NC-SA

Categories of Security Controls …(3/4)

- Committee for National Security System (CNSS) Instruction No. 1253
  - Harmonize definition of security controls by leveraging NIST SP 800-53, Rev. 4.
    - Facilitate reciprocity of system certifications between National Security Community.
  - Selection of security controls are based on risks in meeting security objectives, rather than FIPS 199 high-water mark (HWM) approach.
    - Provides "control profiles" to facilitate selection of security controls.

SC (post-RA) $_{\text{NSS}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}, where the acceptable values for potential impact are low, moderate, or high.

(cc) BY-NC-SA

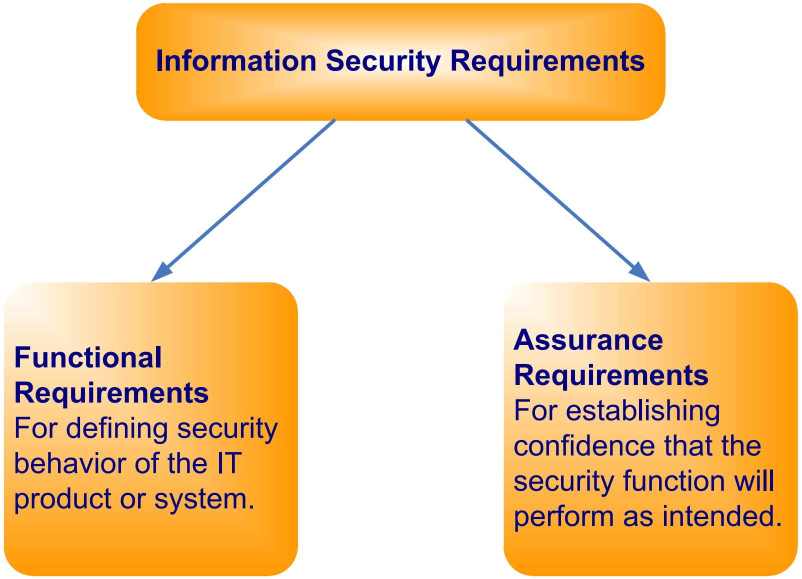
Categories of Security Controls ...(4/4)

ISO/IEC 27001:2005, *Information Technology – Security Techniques – Security Management System – Requirements*

CONTROL CATEGORY	SUB-CATEGORY OF CONTROLS
Security Policy	Information security policy
Organization of Information Security	Internal organization; External parties
Asset Management	Responsibility for assets; Information classification
Human Resource Security	Prior to employment; During employment; Termination or change of employment
Physical and Environmental Security	Secure areas; Equipment security
Communications and Operations Management	Operational procedures and responsibilities; Third party service delivery management; System planning and acceptance; Protection against malicious and mobile code; Back-up; Network security management; Media handling; Exchange of information; Electronic commerce services; Monitoring
Access Control	Business requirement for access control; User access management; User responsibilities; Network access control; Operating system access control; Application and information access control; Mobile computing and teleworking
Information Systems Acquisition, Development, and Maintenance	Security requirements of information systems; Correct processing in applications; Cryptographic controls; Security of system files; Security in development and support processes; Technical vulnerability management
Information Security Incident Management	Reporting information security events and weaknesses; Management of information security incidents and improvements
Business Continuity Management	Information security aspects of business continuity management
Compliance	Compliance with legal requirements; Compliance with security policies and standards, and technical compliance; Information system audit considerations

(cc) BY-NC-SA

Concept of Security Requirements



Information Security Requirements

Functional Requirements
For defining security behavior of the IT product or system.

Assurance Requirements
For establishing confidence that the security function will perform as intended.

- Assurance requirements

  Example:

  SC-3: Security Function Isolation. The information system isolates security functions from non-security functions.

- Functional requirements

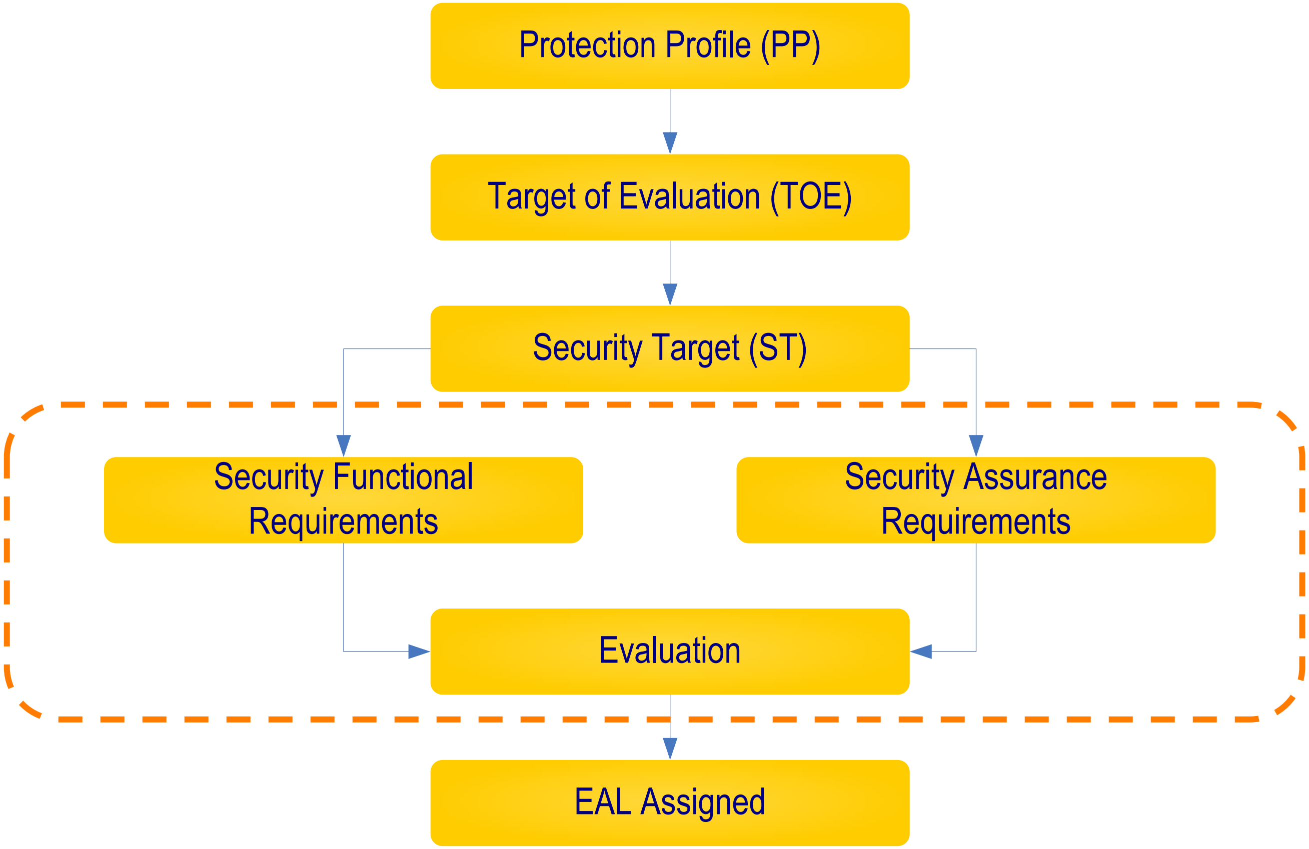
  Example:

  - VLAN technology shall be created to partition the network into multiple mission-specific security domains.
  - The integrity of the internetworking architecture shall be preserved by the access control list (ACL).

BY-NC-SA

Concept of Security Requirements & Common Criteria (ISO/ IEC 15408)

- The new draft NIST SP 800-53, Rev. 4 now maps its security controls to Common Criteria


Protection Profile (PP)
Target of Evaluation (TOE)
Security Target (ST)
Security Functional Requirements
Security Assurance Requirements
Evaluation
EAL Assigned

Reference:

- Draft NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, February 2013.
- ISO/IEC 15408, *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

(cc) BY-NC-SA

Types of Security Controls

- Directive Controls. Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use the organization's information systems.
- Preventive Controls. Included in preventive controls are physical, administrative, and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- Detective Controls. Detective controls involve the use of practices, processes, and tools that identify and possibly react to security violations.
- Corrective Controls. Corrective controls also involve physical, administrative, and technical measures designed to react to detection of an incident in order to reduce or eliminate the opportunity for the unwanted event to recur.
- Recovery Controls. Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.

Reference: *CISM Review Manual – 2007*, ISACA.

(cc) BY-NC-SA

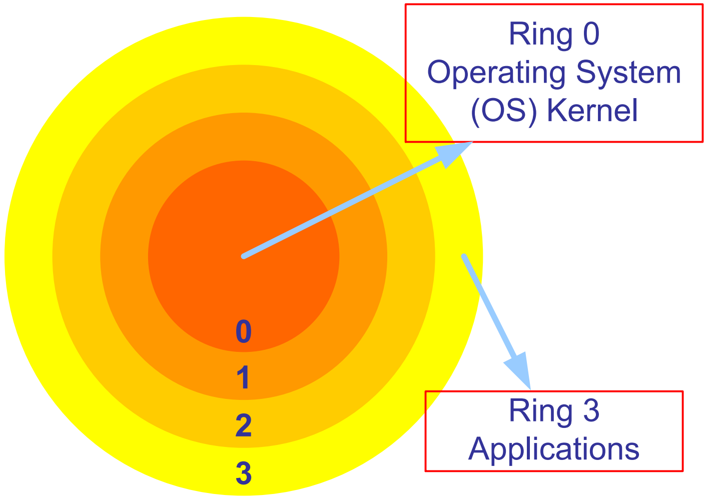
Due Care vs. Due Diligence

- Due Care
  - Policies and implemented actions that an organization has taken to minimize risk to its tangible and intangible assets (i.e. information assets, customers, employees, resources and reputation.)

- Due Diligence
  - Continual actions that an organization are doing to protect and minimize risk to its tangible and intangible assets.

(cc) BY-NC-SA

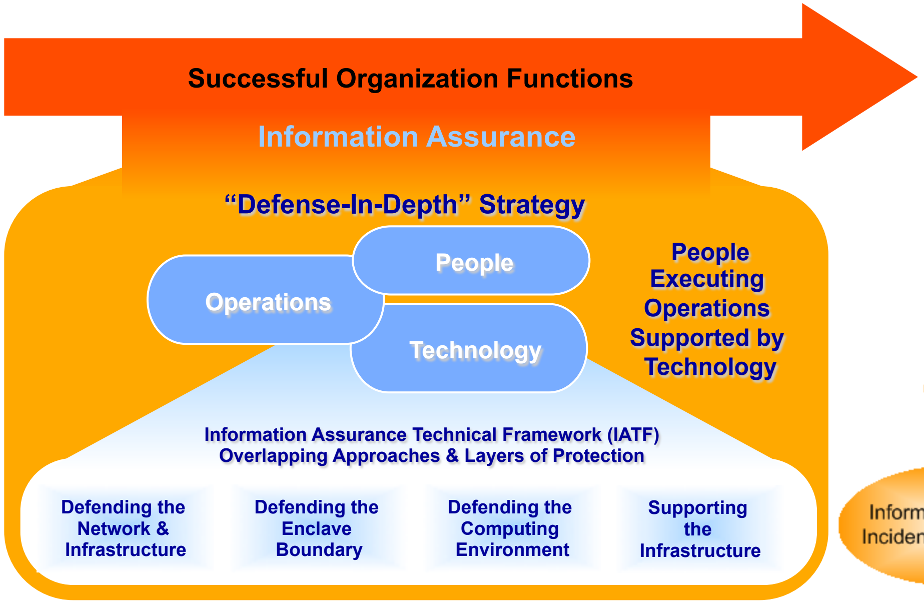
Defense-in-Depth Model – Rings of Protection



- Ring number determines the access level.
- A program may access only data that resides on the same ring, or a less privileged ring.
- A program may call services residing on the same, or a more privileged ring.
- Ring 0 contains kernel functions of the OS.
- Ring 1 contains the OS.
- Ring 2 contains the OS utilities.
- Ring 3 contains the applications.

(cc) BY-NC-SA

Defense-in-Depth Model – Information Security



Successful Organization Functions

Information Assurance

"Defense-In-Depth" Strategy

Operations

People

Technology

People Executing Operations Supported by Technology

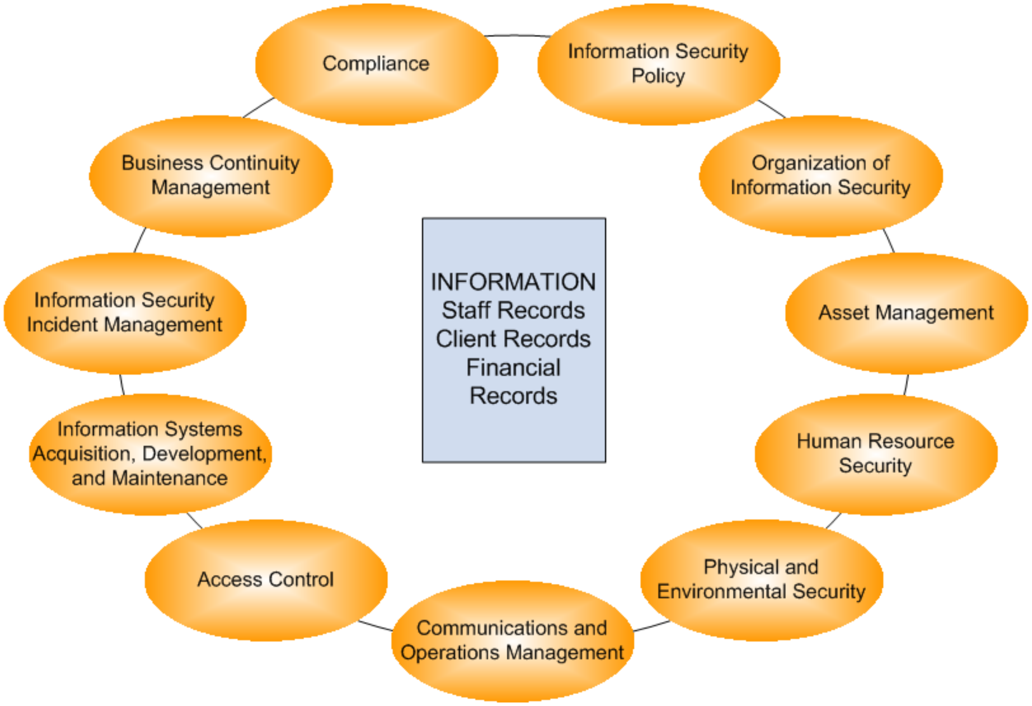
Information Assurance Technical Framework (IATF)
Overlapping Approaches & Layers of Protection

Defending the Network & Infrastructure

Defending the Enclave Boundary

Defending the Computing Environment

Supporting the Infrastructure



INFORMATION
Staff Records
Client Records
Financial Records

Compliance

Information Security Policy

Organization of Information Security

Asset Management

Human Resource Security

Physical and Environmental Security

Communications and Operations Management

Access Control

Information Systems Acquisition, Development, and Maintenance

Information Security Incident Management

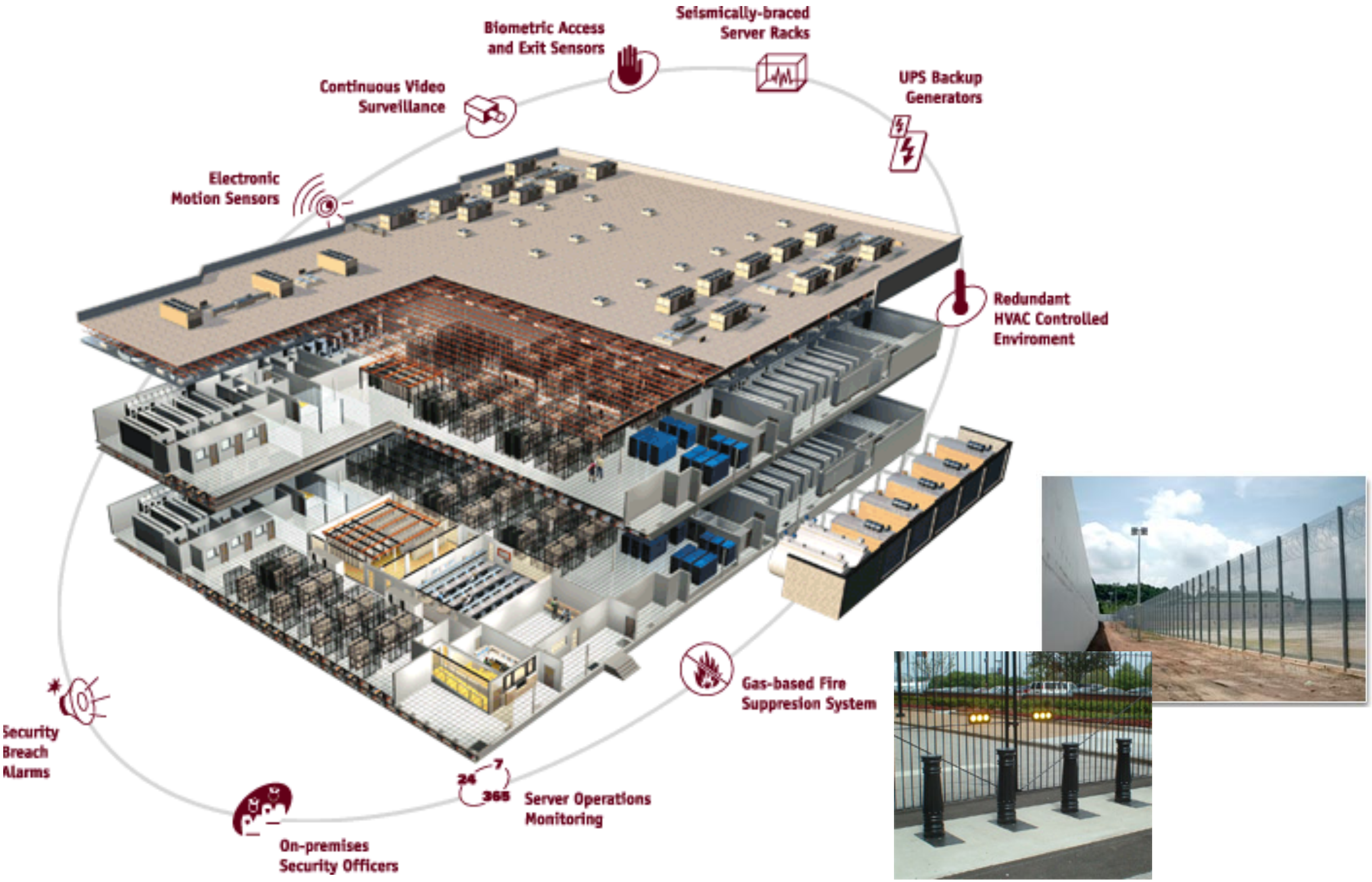
Business Continuity Management

References

- NSA IA Solution Directions, *Information Assurance Technical Framework*, Release 3.1
- ISO/IEC 27002:2005, *Code of Practice for Information Security Management*

BY-NC-SA

Defense-in-Depth Model – Physical Security



(cc) BY-NC-SA

Source: Global Crossing website

Questions:

- What are the three security objectives?
  - –
  - –
  - –

- What are the six security implementation principles?
  - –
  - –
  - –
  - –
  - –
  - –

(cc) BY-NC-SA

Answers:

- What are the three security objectives?
  - Confidentiality
  - Integrity
  - Availability

- What are the six security implementation principles?
  - Confidentiality
  - Integrity
  - Availability
  - Need to know
  - Least privilege
  - Separation of duties

(cc) BY-NC-SA

Questions:

- What are the eight security “best practices”?

  –

  –

  –

  –

  –

  –

  –

  –

- What are the three categories of security controls?

  –

  –

  –

(cc) BY-NC-SA

Answers:

- What are the eight security “best practices”?
  - Confidentiality
  - Integrity
  - Availability
  - Need to know
  - Least privilege
  - Separation of duties
  - Job rotation
  - Mandatory vacation

- What are the three categories of security controls?
  - Management (Administrative)
  - Operational (and Physical)
  - Technical (Logical)

(cc) BY-NC-SA

Information Security Management Domain

- Information Security Concept
- ➡ Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Information Security Management Planning

- Information Security Governance
- Information Classification
- Systems and Services Acquisition & Development
- Risk Management
- Certification & Accreditation
- Security Assessment

Typical Outputs:

- Policies, Standards, and Procedures
- System Security Plan (SSP) or System Security Authorization Agreement (SSAA)
- ST&E Report, Risk Statement, and POA&M for Risk Mitigation

(cc) BY-NC-SA

DoD Information Assurance Program – Competencies

DoD takes risk management approach to define core competencies of any DoD IA Programs…

- The ability to assess security needs and capabilities (Risk Management – Assess, Mitigate & Evaluate)
- The ability to develop a purposeful security design or configuration that adheres to a common architecture and maximizes the use of common services (ISSE, IATF)
- The ability to implement required controls and safeguards (ISSE Process)
- The ability to test and verify (ST&E, CT&E)
- The ability to manage changes to an established baseline in a secure manner (CM, Continuous Monitoring)

Reference: DoDI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

(cc) BY-NC-SA

Learning Objectives

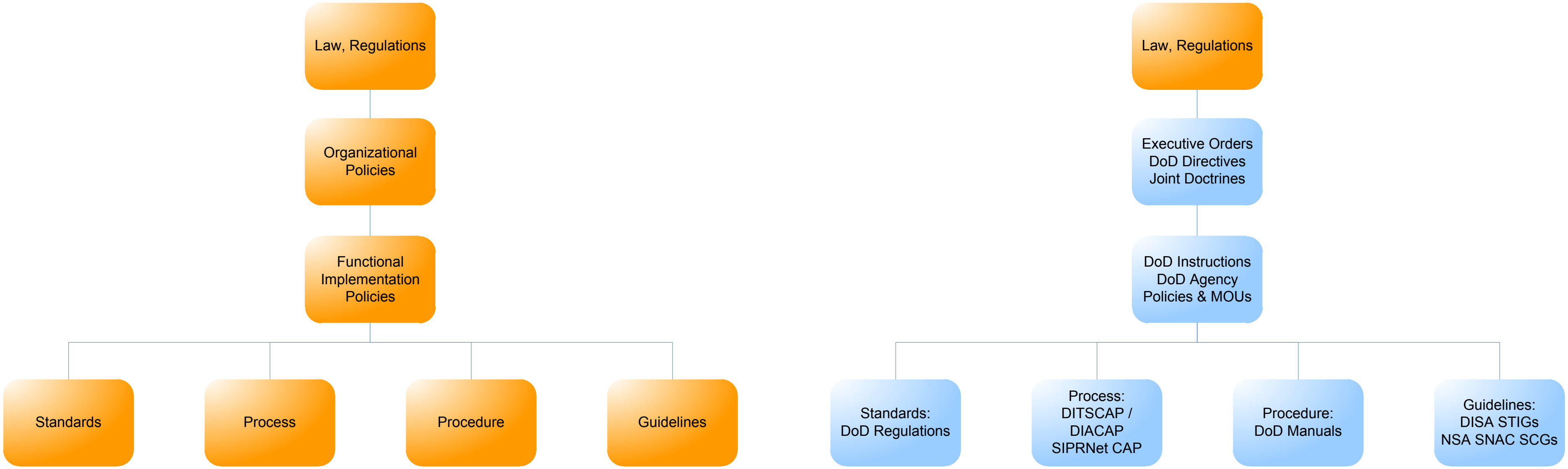
Information Security Management Domain

- Information Security Concept
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

cc BY-NC-SA

Information Security Governance

- Policy. Management directives that establish expectations (goals & objectives), and assign roles & responsibilities
- Standards. Functional specific mandatory activities, actions, and rules
- Process & Procedure. Step-by-step implementation instructions
- Guideline. General statement, framework, or recommendations to augment process or procedure



Law, Regulations

Organizational Policies

Functional Implementation Policies

Standards

Process

Procedure

Guidelines

Law, Regulations

Executive Orders
DoD Directives
Joint Doctrines

DoD Instructions
DoD Agency
Policies & MOUs

Standards:
DoD Regulations

Process:
DITSCAP /
DIACAP
SIPRNet CAP

Procedure:
DoD Manuals

Guidelines:
DISA STIGs
NSA SNAC SCGs

(cc) BY-NC-SA

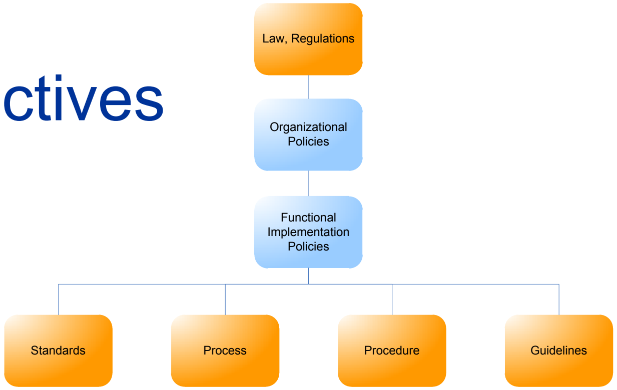
Policies

Policies:

- Explain laws, regulations, business/mission needs, and management expectations (goals & objectives).
- Identify roles and delineate responsibilities.

Examples:

- Executive Orders, Presidential Directives
  - E.O. 13526, PDD-67, HSPD-7, etc.
- Federal (/Civil)
  - OMB Circulars: A-11, A-130, etc.
- Military
  - DoD Directives, Instructions, Manuals, etc.
- Intelligence
  - Director, Central Intelligence Directives (DCID).



(cc) BY-NC-SA

Policies – Roles & Responsibilities

- In order to have an effective security program, the roles, responsibilities and authority must be clearly communicated and understood by all.
  - Information owner. Executive management are responsible for the protection of information assets. (Tangible and Intangible)
    - C[X]Os
    - Functional managers
    - Solutions providers
    - Configuration Management (CM) /CCB
  - Information custodian. Information security professionals are delegated with responsibilities to provide security services that supports the execution of business processes within an organization.
    - Security managers / officers
    - Security administrators (network, systems, databases, etc.)
    - Security analysts
    - Network, system, database administrators
    - Application owner (i.e.
  - Information user. End users are responsible for safeguarding & handling of information. (i.e. marking & labeling, printing, transporting, NdA, etc.)
    - Line managers
    - Analyst
  - Information (systems) auditor. The auditors provide independent assessment of the security of information and/or information systems.
    - Military: White, Blue & Red Teams, IGs
    - Commercial: Auditors, Black-hat Teams

(cc) BY-NC-SA

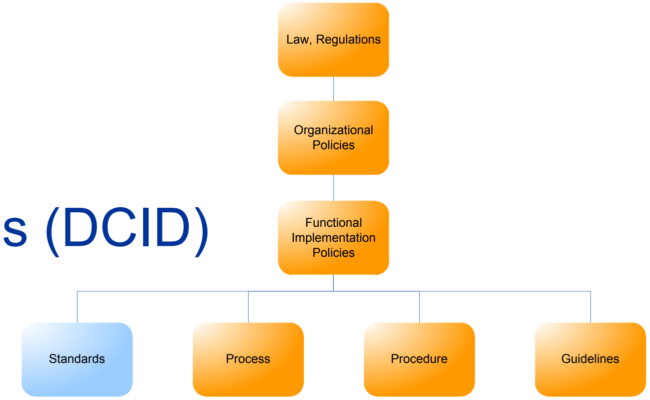
Standards

Standards:

- Mandatory activities, actions, and rules for the execution of management (or administrative) policies

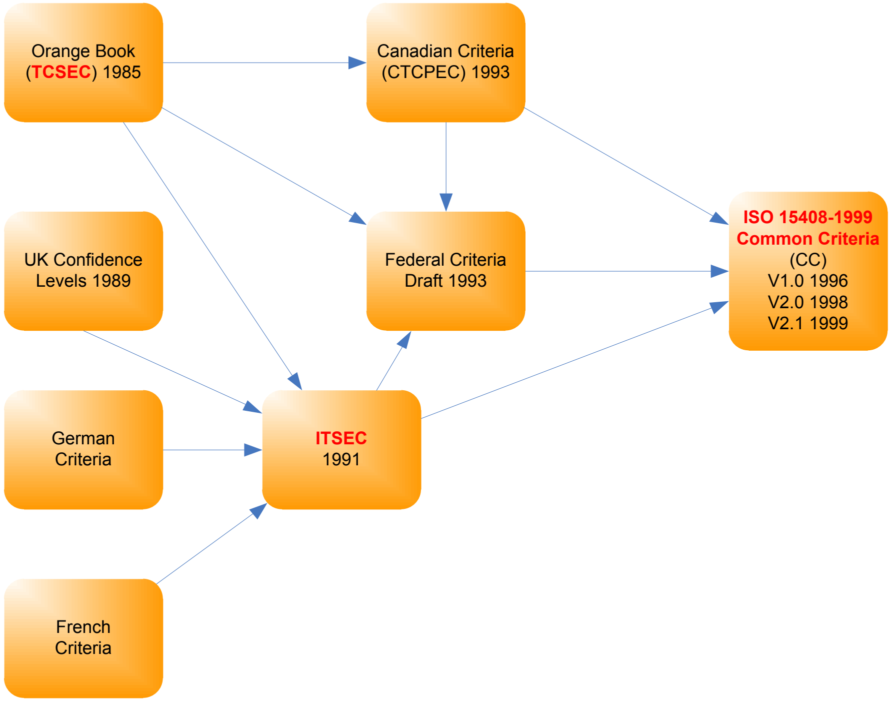
Examples:

- Federal (/ Civil)
  - Federal Information Processing Standards (FIPS)
- Military
  - DoD Regulations, DoD Manuals, etc.
- Intelligence
  - Director, Central Intelligence Directives (DCID)
- Commercial (/ Industry)
  - ISO/IEC 27001, BS 7799, etc.



(cc) BY-NC-SA

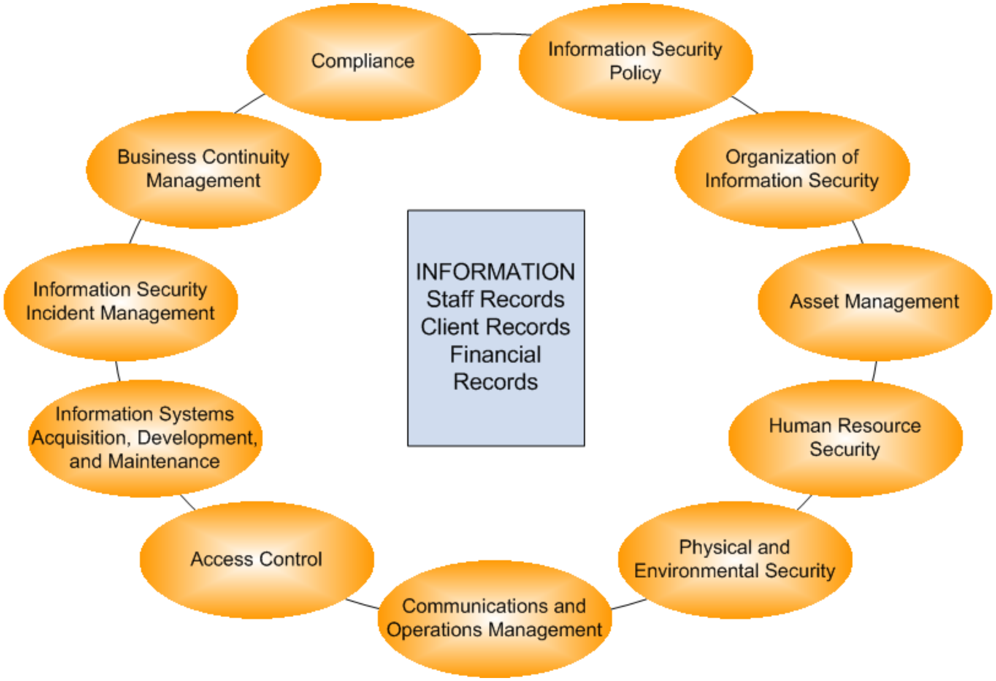
Standards


Orange Book (TCSEC) 1985
Canadian Criteria (CTCPEC) 1993
UK Confidence Levels 1989
Federal Criteria Draft 1993
ISO 15408-1999 Common Criteria (CC) V1.0 1996 V2.0 1998 V2.1 1999
German Criteria
ITSEC 1991
French Criteria

- DoD 5200.28-STD *Trusted Computer System Evaluation Criteria* (TCSEC)
  - Evaluates Confidentiality.
- Information Technology Security Evaluation Criteria (ITSEC)
  - Evaluates Confidentiality, Integrity and Availability.
- Common Criteria (CC)
  - Provided a common structure and language.
  - It’s an International standard (ISO 15408).

(cc) BY-NC-SA

Standards – ISO/IEC 27001:2005


Compliance
Information Security Policy
Business Continuity Management
Organization of Information Security
Information Security Incident Management
INFORMATION
Staff Records
Client Records
Financial Records
Asset Management
Information Systems Acquisition, Development, and Maintenance
Human Resource Security
Access Control
Physical and Environmental Security
Communications and Operations Management

- ISO/IEC 27001 is an Information Security Management System Standard.
- Commercially, the systems are certified based on meeting ISO/IEC 27001 (not ISO/IEC 27002!)
- ISO/IEC 27002:2005 is a “Code of practice” for information security management

Reference:
ISO/IEC 27001:2005, *Information Security Management Systems - Requirements*, 2005.
ISO/IEC 27002:2005, *Code of Practice for Information Security Management*, 2005.

(cc) BY-NC-SA

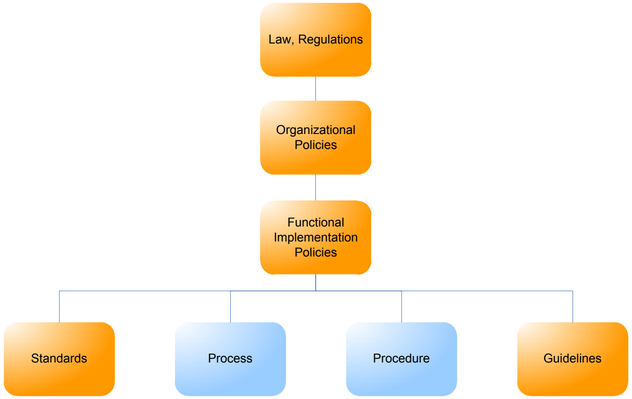
Process & Procedure

Process & Procedure:

- Step-by-step explanation of how to implement or execute security instructions.

Examples:

- System Development Life Cycle (SDLC) System & Services Acquisition Process
  - Project Planning and Management Process
  - Change Control Process
  - Risk Management Process
  - Certification & Accreditation Process
- Standard Operations Procedure (SOP)
- Incident Management Process
- Contingency Planning Process
- Security Assessment Process



(cc) BY-NC-SA

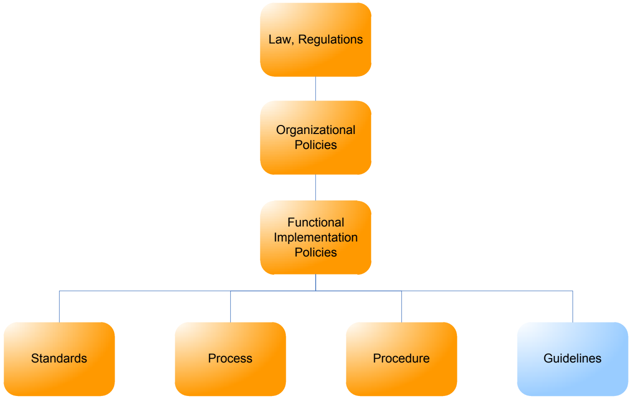
Guidelines

Guidelines:

- Frameworks or recommendations that facilitate implementation of policies, standards, processes, and procedures.

Examples:

- Federal (/ Civil)
  - NIST Special Publications (NIST SP 800 series).
- Military
  - NSA-IATF, NSA-IAM, NSA-IEM.
  - NSA SNAC SCGs, DISA FSO STIGs.
- Commercial
  - ISO/IEC 17799: 2005.
  - CIS Benchmarks.



BY-NC-SA

Question:

- What are the four types of documents that provide governance to IT security?

    –

    –

    –

    –

cc BY-NC-SA

Answer:

- What are the four types of documents that provide governance to IT security?
  - Policy
  - Standard
  - Procedure (or Manual)
  - Guideline

(cc) BY-NC-SA

Information Security Management Domain

- Information Security Concept
- Information Security Management
- Information Security Governance
- ➡ Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training & Awareness

(cc) BY-NC-SA

Information Classification

- Identifies and characterizes the critical information assets (i.e. sensitivity)
- Explains the level of safeguard (protection level) or how the information assets should be handled (sensitivity and confidentiality)

Commercial

- Public
- Private / Sensitive
- Confidential / Proprietary

Military and Civil Gov.

- Unclassified
- Sensitive But Unclassified (SBU)
- Confidential
- Secret
- Top Secret

(cc) BY-NC-SA

Example: Executive Order 13526

- Who can best determine the sensitivity of information?
  - Information owner
- Example: E.O. 13526, *Classified National Security Information*, Dec. 29, 2009
  - President, VP, agency heads, official designated by the President, and delegated USG officials
  - It specifically identifies what information shall be classified
    - a) military plans, weapons systems, or operations;
    - b) foreign government information;
    - c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
    - d) foreign relations or foreign activities of the United States, including confidential sources;
    - e) scientific, technological, or economic matters relating to the national security;
    - f) United States Government programs for safeguarding nuclear materials or facilities;
    - g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
    - h) the development, production, or use of weapons of mass destruction.

(cc) BY-NC-SA

Example: DoD Manual 5200.01 Vol. 1 to Vol. 4

DoDM 5200.01, *DoD Information Security Program*, February 24, 2012.

- Volume 1: Overview, Classification, and Declassification
- Volume 2: Marking of Classified Information
- Volume 3: Protection of Classified Information
- Volume 4: Controlled Unclassified Information (CUI)

(for meeting the E.O. 13556, *Controlled Unclassified Information*, November 4, 2010.)

(cc) BY-NC-SA

Questions:

- What is the importance of information classification?
  - –

- When should the sensitivity and the protection level should be determined in the system life cycle?
  - –

- What is the importance of FIPS 199?
  - –

cc BY-NC-SA

Answers:

- What is the importance of information classification?
  - Explains the **sensitivity** of the information, and the **level of protection** required to meet the security objectives

- When should the sensitivity and the protection level should be determined in the system life cycle?
  - At the **Initial Phase**. It is a part of system characterization activity

- What is the importance of FIPS 199?
  - Explains the sensitivity of the information in terms of **impact in meeting the security objectives**

(cc) BY-NC-SA

Notes on NIST SP 800-59

The information classification concept is also implemented for information systems that store, process, and distribute national security information…

- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
  - It's a guideline for identification only,
  - It does not discuss how information should be managed, and
  - Agencies have to establish their own policies

(cc) BY-NC-SA

Learning Objectives

Information Security Management Domain

- Information Security Concept
- Information Security Management
- Information Security Governance
- Information Classification
- ➡ System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

System Development Life Cycle (SDLC) Models

- Waterfall Development Models
  - Waterfall: DoD-STD-2167A (replaced by MIL-STD-498 on 11/1994).
  - Modified Waterfall: MIL-STD-498 (cancelled on 5/1998)
  - ISO/IEC 12207, *Software Life Cycle Processes* (IEEE/EIA 12207 US implementation) (based on MIL-STD-499B)
  - ISO/IEC 15288, *Systems Engineering – System Life Cycle Processes* (IEEE std 1220 – 2005, US implementation)

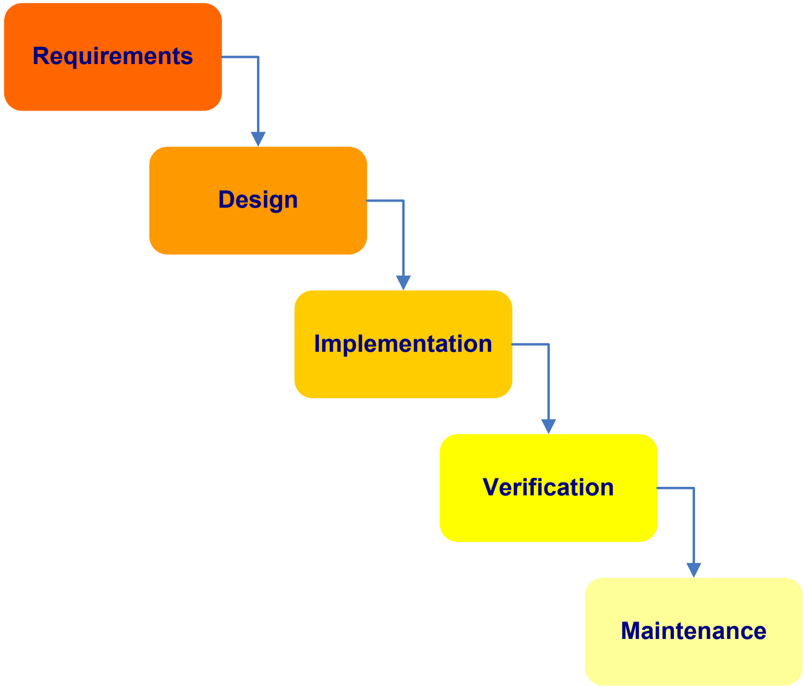
- Iterative Development Models
  - Boehm's Spiral Model.
  - Rapid Application Development (RAD) & Joint Application Development (JAD)

(cc) BY-NC-SA

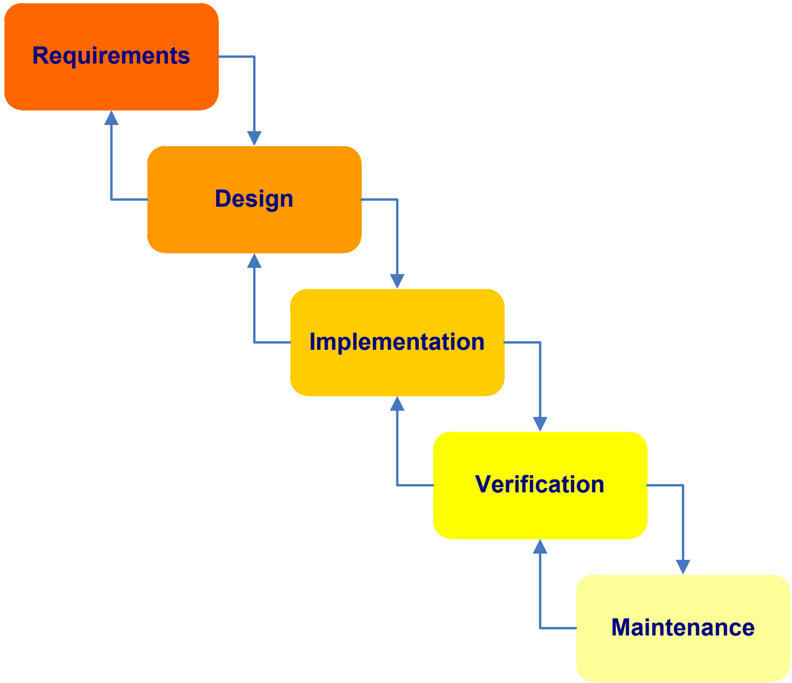
System Life Cycle (SLC) and System Development Life Cycle (SDLC)

Waterfall Development Models

- Classic Waterfall: DoD-STD-2167A

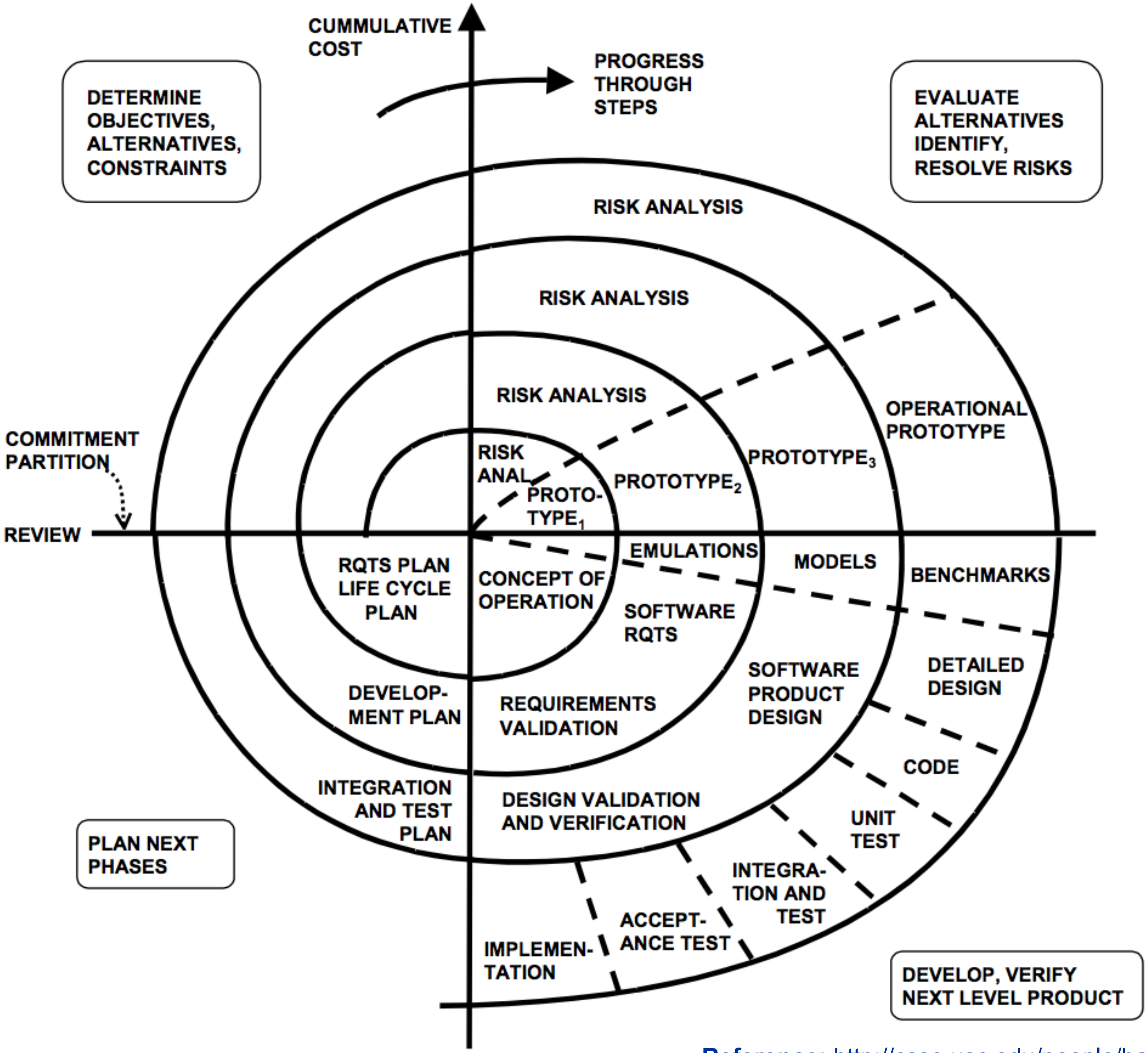


- Modified Waterfall: MIL-STD-498



(cc) BY-NC-SA

Boehm’s Spiral Model

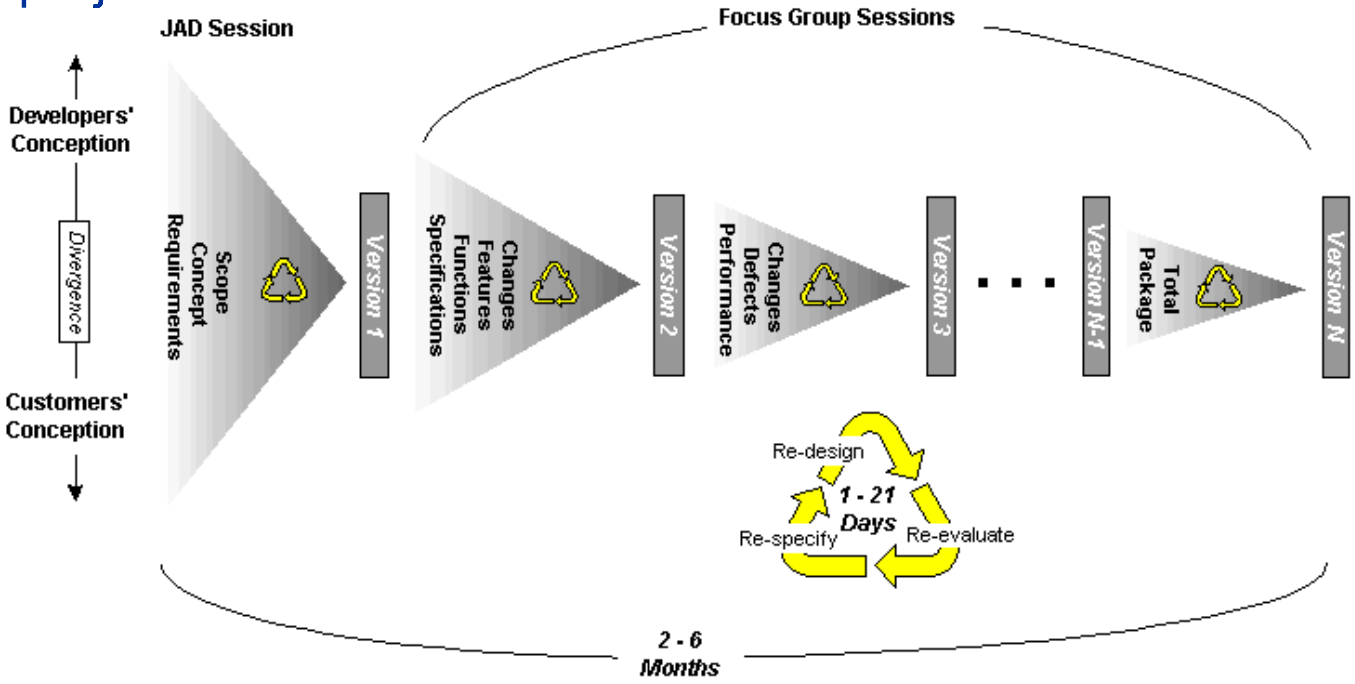


(cc) BY-NC-SA

Reference: http://csse.usc.edu/people/barry.html

Rapid Application Development (RAD) Model

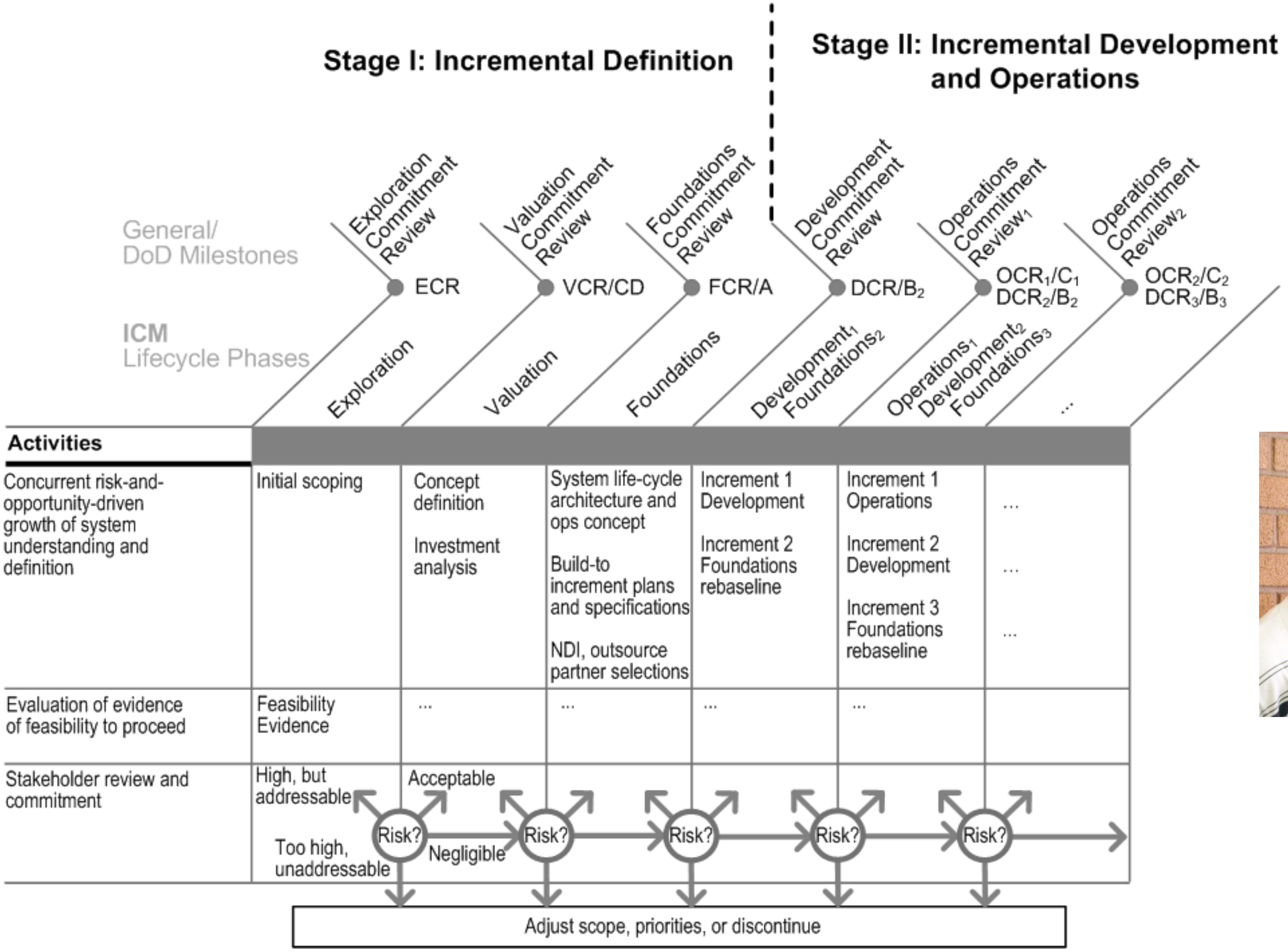
- Iterative, but spiral cycles are much smaller.
- Risk-based approach, but focus on “good enough” outcome.
- SDLC fundamentals still apply…
  - Requirements, configuration, and quality management, design process, coding, test & integration, technical and project reviews etc.



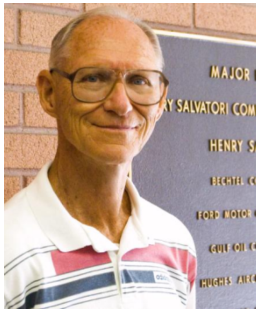
Reference:
- S. McConnell, *Rapid Development: Taming Wild Software Schedules*
- http://www.cs.bgsu.edu/maner/domains/RAD.htm

(cc) BY-NC-SA

Incremental Commitment Model


Stage I: Incremental Definition
Stage II: Incremental Development and Operations
General/ DoD Milestones
Exploration Commitment Review
Valuation Commitment Review
Foundations Commitment Review
Development Commitment Review
Operations Commitment Review$_1$
Operations Commitment Review$_2$
ECR
VCR/CD
FCR/A
DCR/B$_2$
OCR$_1$/C$_1$ DCR$_2$/B$_2$
OCR$_2$/C$_2$ DCR$_3$/B$_3$
ICM Lifecycle Phases
High, but addressable
Acceptable
Risk?
Risk?
Risk?
Risk?
Risk?
Too high, unaddressable
Negligible
Adjust scope, priorities, or discontinue

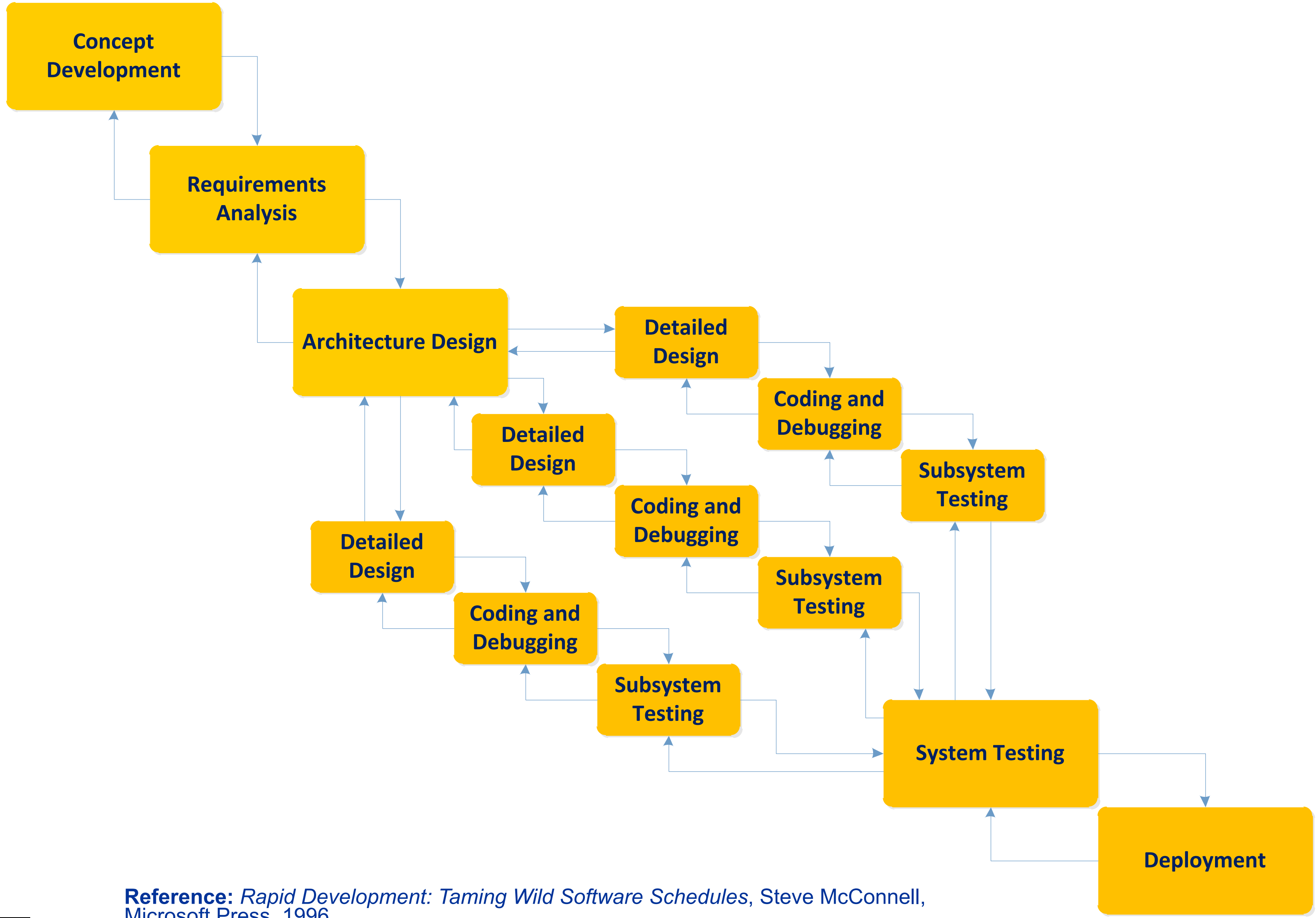
Activities	Exploration	Valuation	Foundations	Development$_1$ Foundations$_2$	Operations$_1$ Development$_2$ Foundations$_3$	...
Concurrent risk-and-opportunity-driven growth of system understanding and definition	Initial scoping	Concept definition Investment analysis	System life-cycle architecture and ops concept Build-to increment plans and specifications NDI, outsource partner selections	Increment 1 Development Increment 2 Foundations rebaseline	Increment 1 Operations Increment 2 Development Increment 3 Foundations rebaseline	… … …
Evaluation of evidence of feasibility to proceed	Feasibility Evidence	...	...	...	...	
Stakeholder review and commitment						



Reference: B. Boehm, J.A. Lane, *Using the Incremental Commitment Model to Integrate System Acquisition, Systems Engineering, and Software Engineering,* CrossTalk, October 2007.

(cc) BY-NC-SA

Other SDLC Models – Modified Waterfall w/ Subprojects

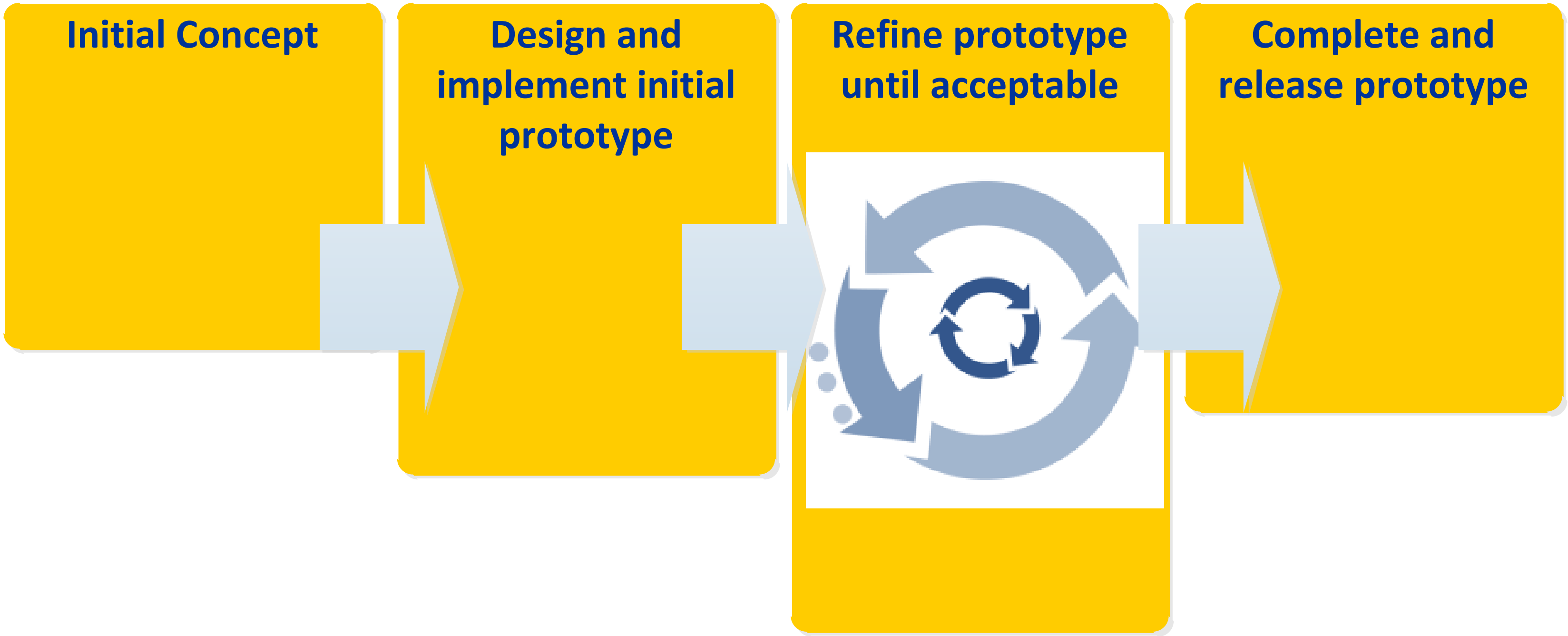


Reference: *Rapid Development: Taming Wild Software Schedules*, Steve McConnell, Microsoft Press, 1996

(cc) BY-NC-SA

Other SDLC Models – Evolutionary Prototyping

- The system concept is refined continuously…
  - The focus is on “good enough” concept, requirements, and prototype.
  - However, it is difficult to determine level of effort (LOE), cost, and schedule.


Initial Concept
Design and implement initial prototype
Refine prototype until acceptable
Complete and release prototype

Reference: *Rapid Development: Taming Wild Software Schedules*, Steve McConnell, Microsoft Press, 1996

(cc) BY-NC-SA

Are there other SDLC models?

- Have you heard of “Rugged DevOps”?
- Rugged DevOps*
  - Idea observed from cloud computing...
  - 2009, Flickr reported 10 deployments per day
  - Amazon EC2 reported in May 2011:**
    - Mean time between deployments: 11.6 seconds
    - Maximum # of deployments in an hour: 1,079
    - Mean # of hosts simultaneously receiving a deployment: 10k
    - Maximum # of hosts simultaneously receiving a deployment: 30k

Reference:

* J. Gorman, G. Kim, *Security is Dead. Long Live Rugged DevOps: IT at Ludicrous Speed*, RSA Conference 2012 (http://www.slideshare.net/realgenekim/security-is-dead-long-live-rugged-devops-it-at-ludicrous-speed)

** Jon Jenkins, Velocity Culture, O’Reilly Velocity 2011, (http://www.youtube.com/watch?v=dxk8b9rSKOo)

(cc) BY-NC-SA

Philosophy behind the Rugged DevOps

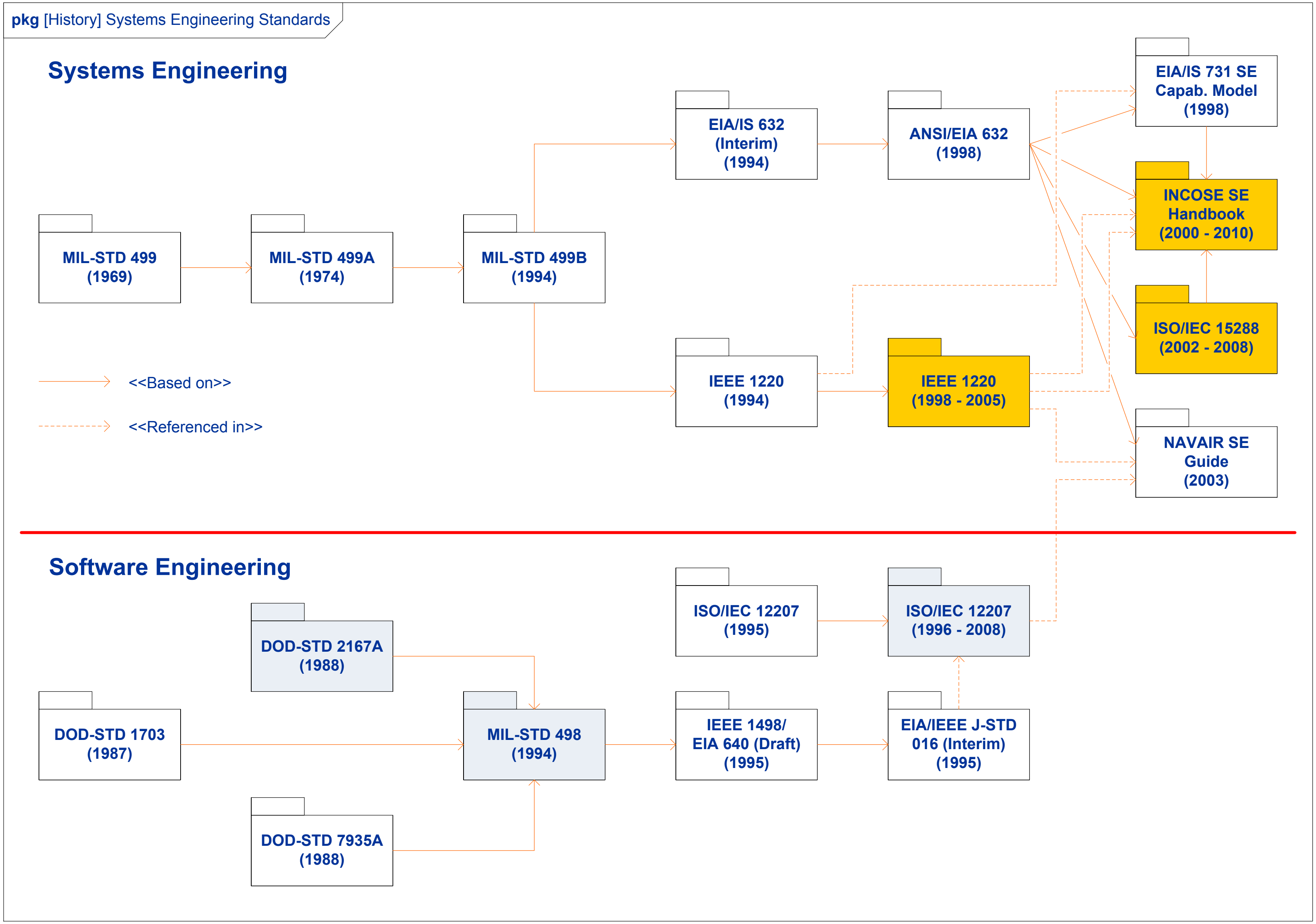
- Seamless integration of software development and IT operations
- Focus on the "big picture" rather than security controls
  - Standard configuration
  - Process discipline
  - Controlled access to production systems
- Results
  - 75% reduction in outages triggered by software deployment since 2006
  - 90% reduction in outage minutes triggered by software deployments
  - Instantaneous automated rollback
  - Reduction in complexity
- Back to our study...

Reference:

- Jon Jenkins, *Velocity Culture*, O'Reilly Velocity 2011, (http://www.youtube.com/watch?v=dxk8b9rSKOo)

(cc) BY-NC-SA

History of Systems/Software Engineering Process Standards



pkg [History] Systems Engineering Standards

Systems Engineering

MIL-STD 499 (1969)

MIL-STD 499A (1974)

MIL-STD 499B (1994)

EIA/IS 632 (Interim) (1994)

ANSI/EIA 632 (1998)

IEEE 1220 (1994)

IEEE 1220 (1998 - 2005)

EIA/IS 731 SE Capab. Model (1998)

INCOSE SE Handbook (2000 - 2010)

ISO/IEC 15288 (2002 - 2008)

NAVAIR SE Guide (2003)

<<Based on>>

<<Referenced in>>

Software Engineering

DOD-STD 1703 (1987)

DOD-STD 2167A (1988)

DOD-STD 7935A (1988)

MIL-STD 498 (1994)

IEEE 1498/ EIA 640 (Draft) (1995)

EIA/IEEE J-STD 016 (Interim) (1995)

ISO/IEC 12207 (1995)

ISO/IEC 12207 (1996 - 2008)

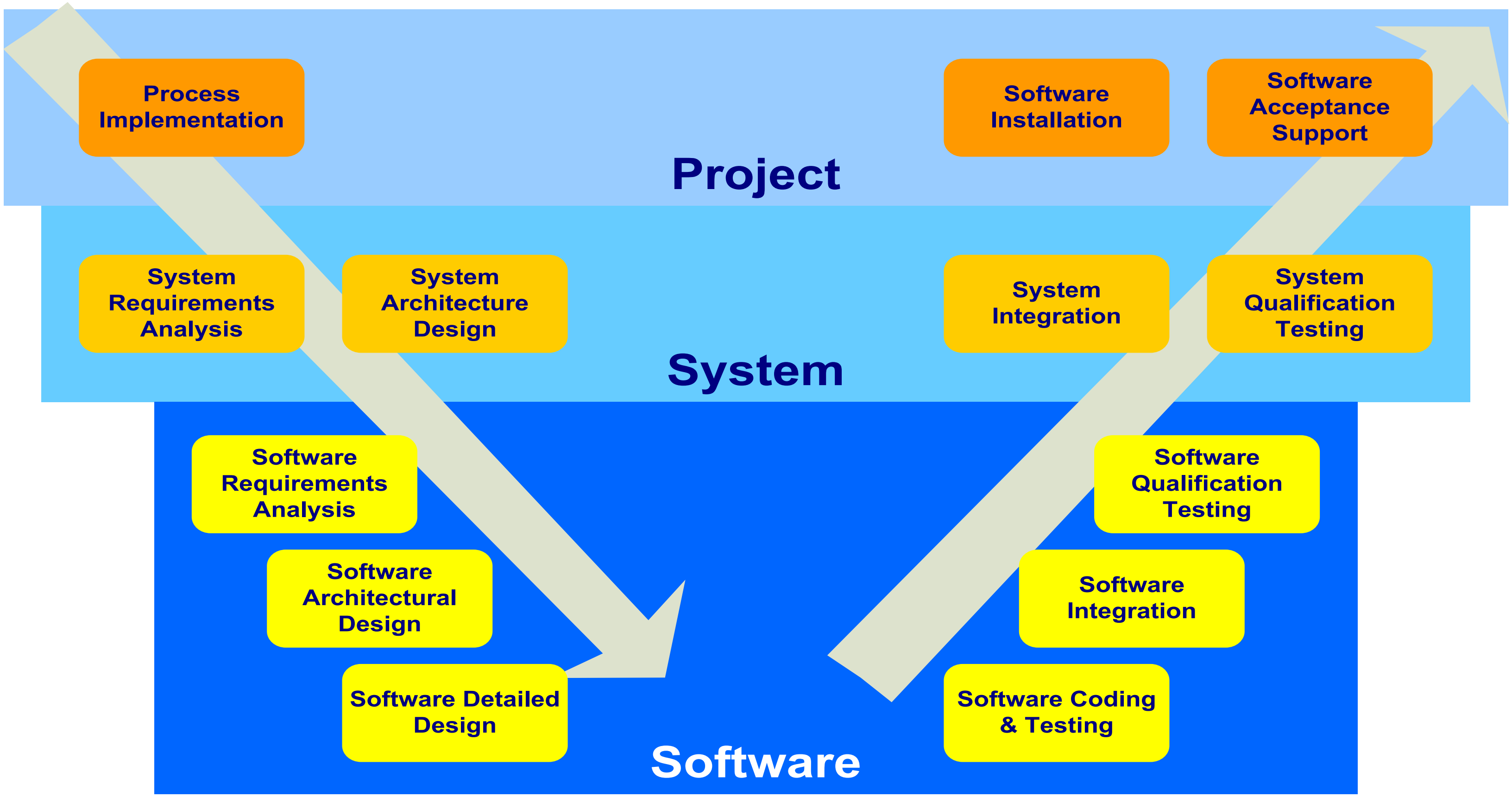
(cc) BY-NC-SA

Software & System Engineering Management Processes

- There are more and more “software-intensive” systems…
  - Systems are getting more complex. Hardware problems are often addressed through software;
  - Operating environments are stochastic. Software are more flexible than hardware.
- As SDLC models evolves, management processes are evolving too…
  - DoD-STD-2167A: Waterfall SDLC + SE Process
  - MIL-STD-498: Modified Waterfall SDLC + SE Process
  - IEEE 1220: System Engineering Process
  - ISO 12207: Software + System Engineering Mgmt Process
  - ISO 15288: System Engineering Mgmt Process

(cc) BY-NC-SA

DoD-STD-2167A – System Engineering Process

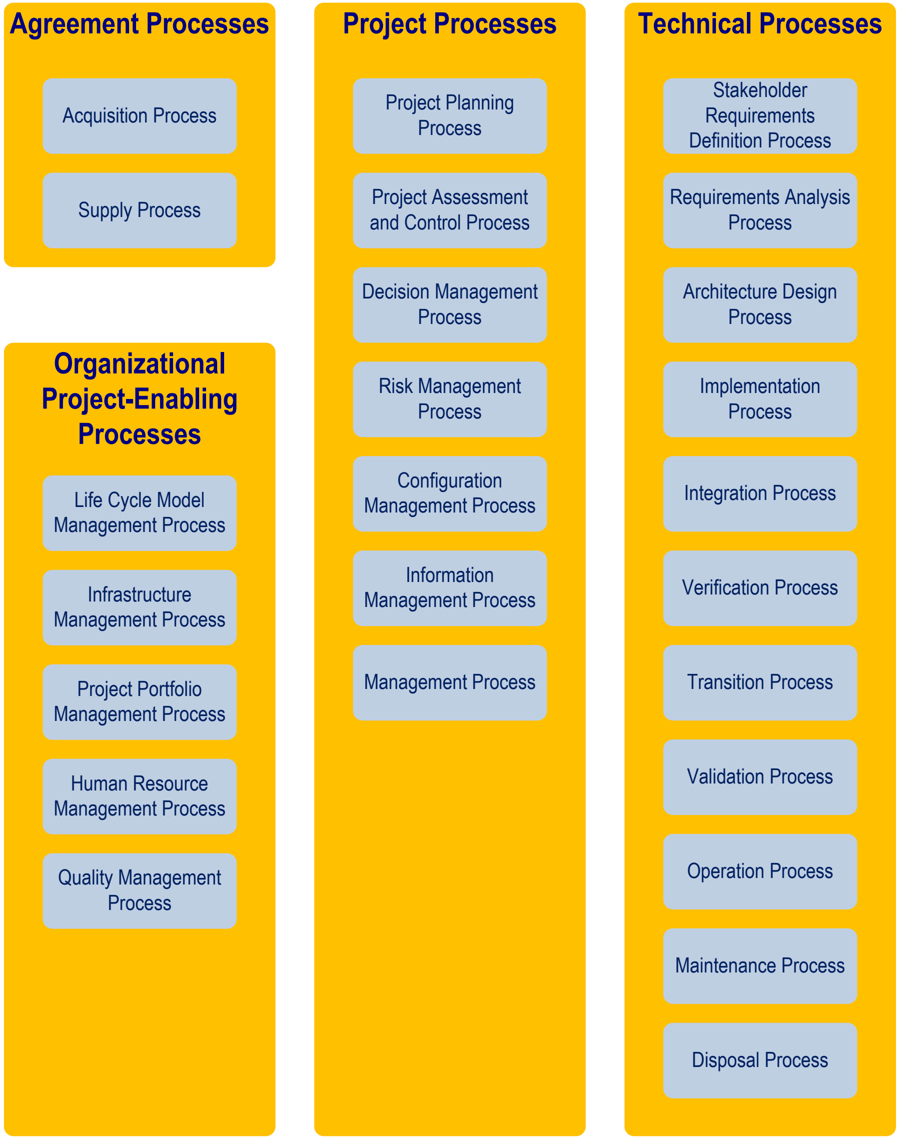

Process Implementation
Software Installation
Software Acceptance Support
Project
System Requirements Analysis
System Architecture Design
System Integration
System Qualification Testing
System
Software Requirements Analysis
Software Qualification Testing
Software Architectural Design
Software Integration
Software Detailed Design
Software Coding & Testing
Software

Reference: DoD-STD-2167A, *Defense System Software Development*, February 29, 1988

(cc) BY-NC-SA

ISO/IEC 15288:2008, System Life Cycle Processes

- ISO/IEC 15288* encompasses:
  - Systems/software engineering processes (Technical Processes)
  - Project management processes
  - Project support infrastructure (Organizational Project-Enabling Processes)
  - Contract/business management processes (Agreement Processes)



Agreement Processes

- Acquisition Process
- Supply Process

Organizational Project-Enabling Processes

- Life Cycle Model Management Process
- Infrastructure Management Process
- Project Portfolio Management Process
- Human Resource Management Process
- Quality Management Process

Project Processes

- Project Planning Process
- Project Assessment and Control Process
- Decision Management Process
- Risk Management Process
- Configuration Management Process
- Information Management Process
- Management Process

Technical Processes

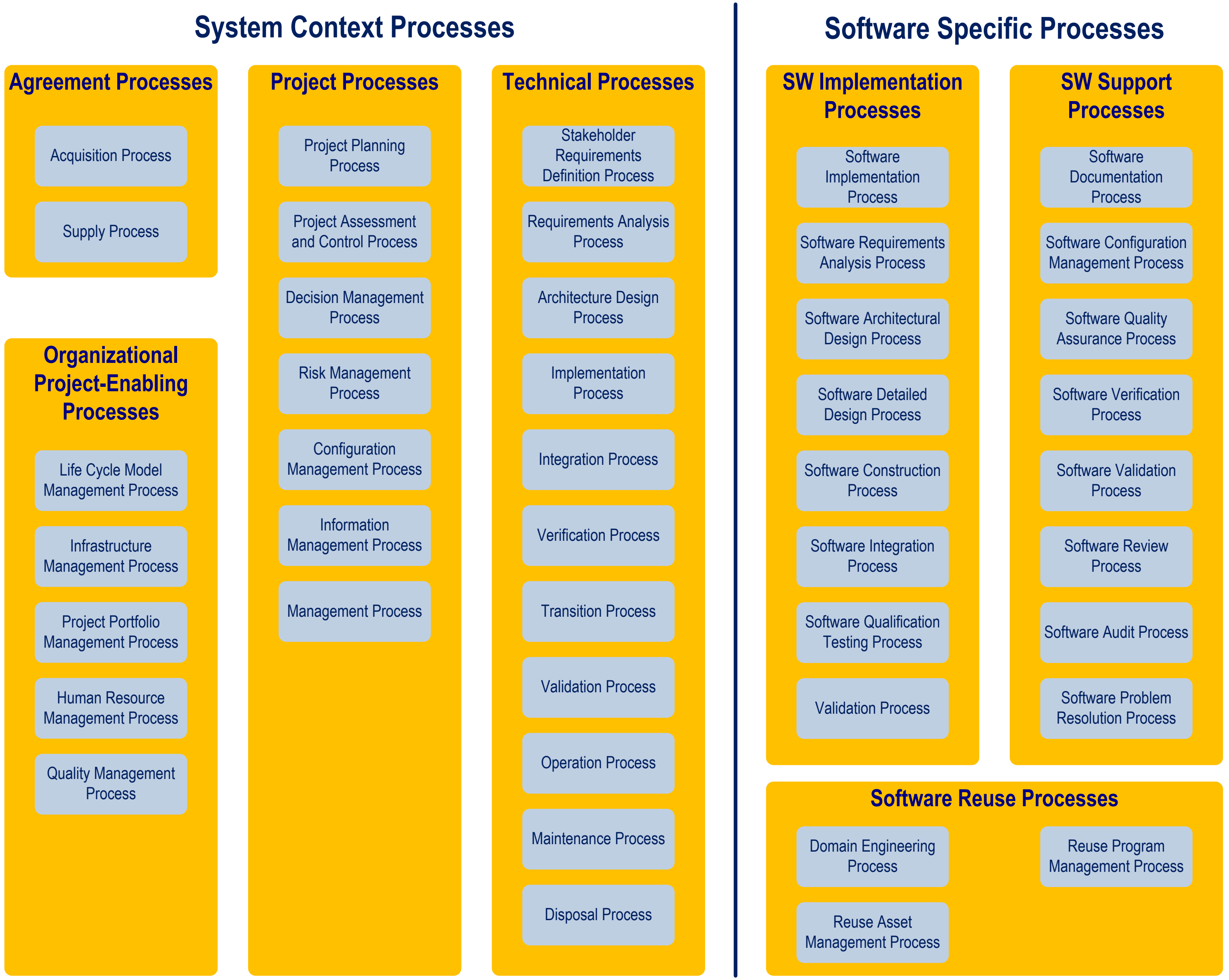
- Stakeholder Requirements Definition Process
- Requirements Analysis Process
- Architecture Design Process
- Implementation Process
- Integration Process
- Verification Process
- Transition Process
- Validation Process
- Operation Process
- Maintenance Process
- Disposal Process

* Note: ISO/IEC 15288 is identical to IEEE Std 15288

(cc) BY-NC-SA

System Life Cycle (SLC) and System Development Life Cycle (SDLC)

ISO/IEC 12207:2008, Software Life Cycle Processes



System Context Processes

Agreement Processes

- Acquisition Process
- Supply Process

Organizational Project-Enabling Processes

- Life Cycle Model Management Process
- Infrastructure Management Process
- Project Portfolio Management Process
- Human Resource Management Process
- Quality Management Process

Project Processes

- Project Planning Process
- Project Assessment and Control Process
- Decision Management Process
- Risk Management Process
- Configuration Management Process
- Information Management Process
- Management Process

Technical Processes

- Stakeholder Requirements Definition Process
- Requirements Analysis Process
- Architecture Design Process
- Implementation Process
- Integration Process
- Verification Process
- Transition Process
- Validation Process
- Operation Process
- Maintenance Process
- Disposal Process

Software Specific Processes

SW Implementation Processes

- Software Implementation Process
- Software Requirements Analysis Process
- Software Architectural Design Process
- Software Detailed Design Process
- Software Construction Process
- Software Integration Process
- Software Qualification Testing Process
- Validation Process

SW Support Processes

- Software Documentation Process
- Software Configuration Management Process
- Software Quality Assurance Process
- Software Verification Process
- Software Validation Process
- Software Review Process
- Software Audit Process
- Software Problem Resolution Process

Software Reuse Processes

- Domain Engineering Process
- Reuse Program Management Process
- Reuse Asset Management Process

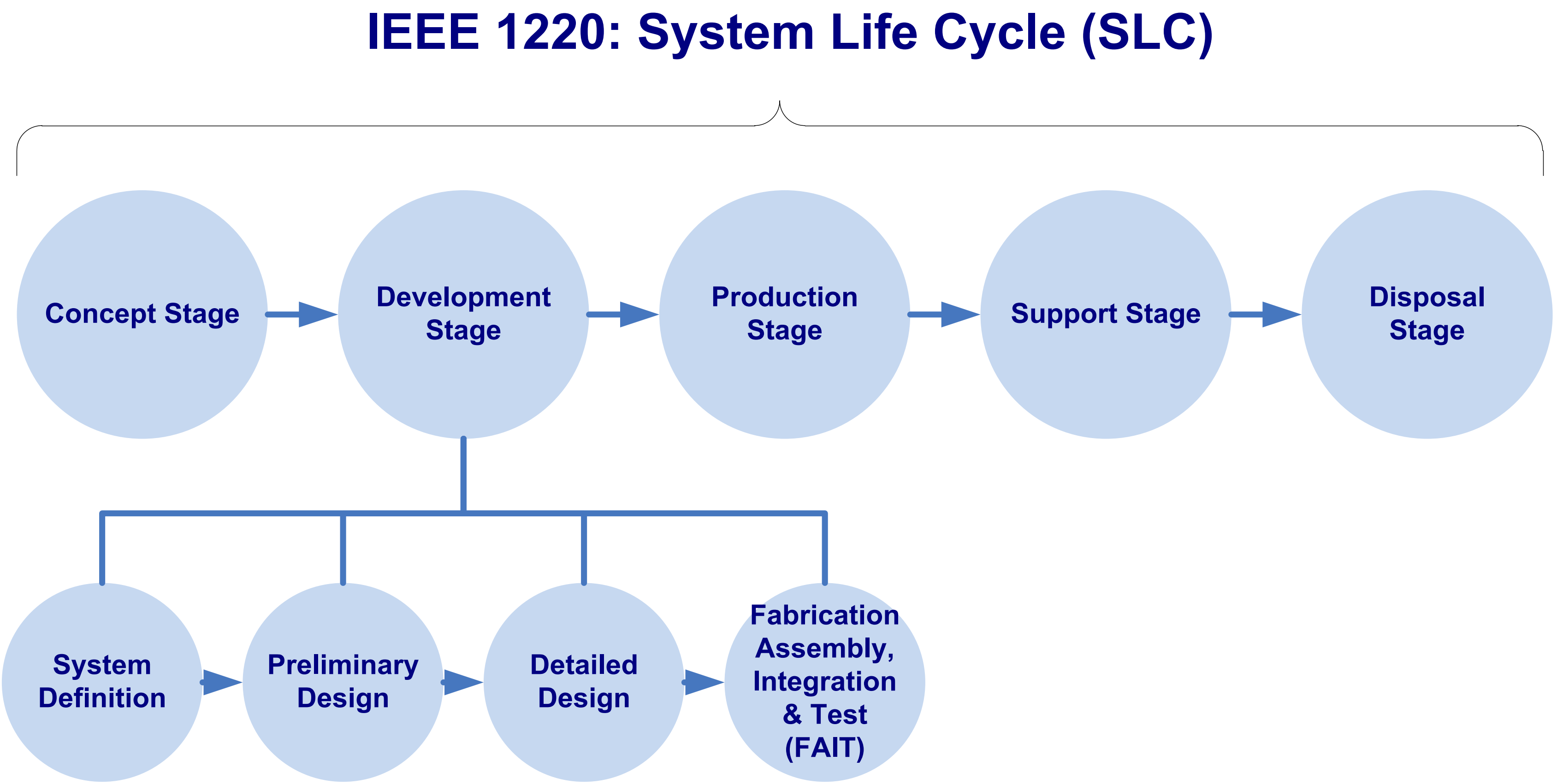
* Note: ISO/IEC 12207is identical to IEEE Std 12207

Reference: IEEE/IEC 12207:2008, *Information Technology Software Life Cycle Processes*

(cc) BY-NC-SA

System Life Cycle (SLC) and System Development Life Cycle (SDLC)

IEEE std 1220, System Engineering Process



(cc) BY-NC-SA

System Life Cycle (SLC)

1. Initiation Phase (IEEE 1220: Concept Stage)
   - Survey & understand the policies, standards, and guidelines.
   - Identify information assets (tangible & intangible).
   - Define information security categorization & protection level.
   - Conduct business impact analysis (BIA) (a.k.a. risk assessment).
   - Define rules of behavior & security CONOPS.

2. Acquisition / Development Phase (IEEE 1220: Development Stage)
   - Define security requirements and select security controls.
   - Assess system risk.
   - Perform cost/benefit analysis (CBA).
   - Security planning (based on risks & CBA).
   - Practice Information Systems Security Engineering (ISSE) Process to develop security controls.
   - Develop security test & evaluation (ST&E) plan.

Reference: NIST SP 800-64, Rev 2,*Security Considerations in the Information System Development Life Cycle*.

(cc) BY-NC-SA

Systems Life Cycle (SLC)

3. Implementation Phase (IEEE 1220: Production Stage)
   - Implement security controls in accordance with baseline system design and update system security plan (SSP).
   - Integrate system
   - Perform Security Certification & Accreditation of target system.

4. Operations / Maintenance Phase (IEEE 1220: Support Stage)
   - Review operational readiness.
   - Configuration management & perform change control.
   - Continuous monitoring of security posture
   - Perform periodic security assessment.

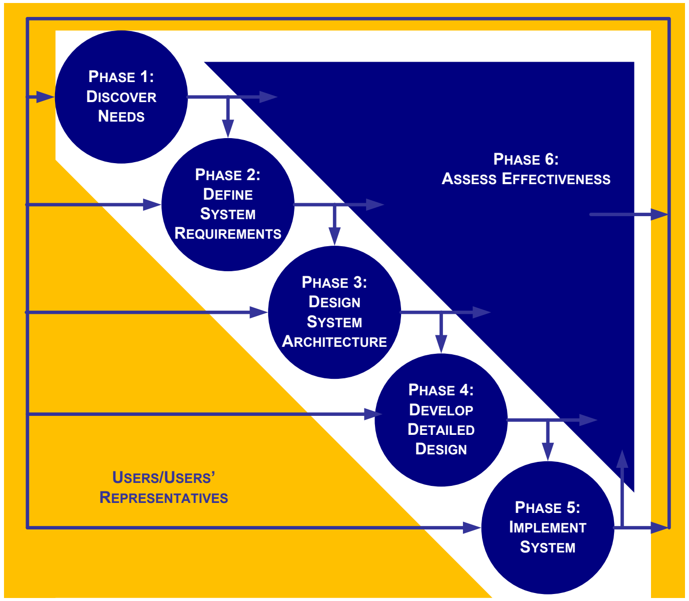
5. Disposition Phase (IEEE 1220: Disposal Stage)
   - Preserve information. archive and store electronic information
   - Sanitize media. Ensure the electronic data stored in the disposed media are deleted, erased, and over-written
   - Dispose hardware. Ensure all electronic data resident in hardware are deleted, erased, and over-written (i.e. EPROM, BIOS, etc.

Reference: NIST SP 800-64, Rev 2,*Security Considerations in the Information System Development Life Cycle*.

(cc) BY-NC-SA

Information System Security Engineering (ISSE) Process

- Phase 1: Discover Information Protection Needs
  - Ascertain the system purpose.
  - Identify information asset needs protection.
- Phase 2: Define System Security Requirements
  - Define requirements based on the protection needs.
- Phase 3: Design System Security Architecture
  - Design system architecture to meet on security requirements.
- Phase 4: Develop Detailed Security Design
  - Based on security architecture, design security functions and features for the system.
- Phase 5: Implement System Security
  - Implement designed security functions and features into the system.
- Phase 6: Assess Security Effectiveness
  - Assess effectiveness of ISSE activities.


Phase 1: Discover Needs
Phase 2: Define System Requirements
Phase 3: Design System Architecture
Phase 4: Develop Detailed Design
Phase 5: Implement System
Phase 6: Assess Effectiveness
Users/Users' Representatives

Reference: *Information Assurance Technical Framework (IATF)*, Release 3.1

(cc) BY-NC-SA

Examples of SDLC and Systems Engineering Activities

<table>
<tr><th colspan="14">IEEE 1220, Application and Management of the Systems Engineering Process</th></tr>
<tr><td colspan="3">Concept Stage</td><td colspan="9">Development Stage</td><td>Production Stage</td><td>Operations & Maintenance</td></tr>
<tr><th colspan="14">Defense Acquisition Life Cycle (DoD 5000)</th></tr>
<tr><td>User needs & Technology Opportunities</td><td colspan="2">Concept Refinement</td><td colspan="3">Technology Development</td><td colspan="6">System Development & Demonstration</td><td>Production and Deployment</td><td>Operations & Support</td></tr>
<tr><th colspan="14">IRS Enterprise Life Cycle (ELC)</th></tr>
<tr><td>Vision & Strategy</td><td colspan="2">Project Initiation</td><td colspan="2">Domain Architecture</td><td colspan="4">Preliminary Design</td><td colspan="2">Detailed Design</td><td>System Development</td><td>System Deployment</td><td>Operations & Maintenance</td></tr>
<tr><th colspan="14">FBI Information Technology Life Cycle Management Directive (IT LCMD)</th></tr>
<tr><td colspan="2">Concept Exploration</td><td colspan="2">Requirements Development</td><td colspan="3">Acq. Planning</td><td>Source Select'n.</td><td colspan="3">Design</td><td>Develop &amp; Test</td><td>Implementation & Integration</td><td>Operations & Maintenance</td></tr>
<tr><th colspan="14">Systems Engineering (SE) Tasks</th></tr>
<tr><td colspan="3">Discover Mission/Business Needs</td><td colspan="3">Define System Requirements</td><td colspan="4">Design System Architecture</td><td colspan="2">Develop Detailed System Design</td><td>Implement System Design</td><td>Sustainment</td></tr>
<tr><th colspan="14">Information Systems Security Engineering (ISSE) Tasks</th></tr>
<tr><td colspan="3">Discover Information Protection Needs</td><td colspan="3">Define Security Requirements</td><td colspan="4">Design System Security Architecture</td><td colspan="2">Develop Detailed System Security Controls</td><td>Implement Security Controls</td><td>Continuous Monitoring</td></tr>
</table>

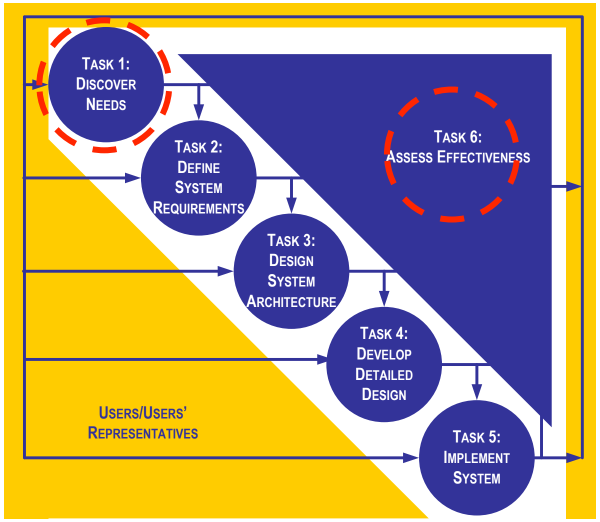
We need to do more on understanding the mission/business needs and align to EA

(cc) BY-NC-SA

It starts at the beginning of a SDLC…

IEEE 1220	DoD Acquisition SDLC	Key System Engineering Tasks	Key Security Engineering Tasks*
Concept Stage	User Needs & Technology Opportunities	**Task 1: Discover Mission/Business Needs**	**Task 1: Discover Information Protection Needs**
		• Understand customer's mission/business goals (i.e., initial capability, project risk assessment)	• Understand customer's information protection needs (i.e., infosec. risk assessment)
	Concept Refinement	• Understand system concept of operations (CONOPS)	• Understand operating environment (i.e., sensitivity of information assets, mode of operations)
		• Create high-level entity-data relations model (i.e., system context diagram)	• Create information management model (IMM)
		• Define engineering project strategy and integrate into the overall project strategy	• Define information protection policy (IPP) and integrate into the project strategy
		• Create system engineering management plan (SEMP)	• Create system security plan (SSP) and integrate into SEMP
	Milestone A	**Task 6: Assess project performance in meeting mission/business needs**	

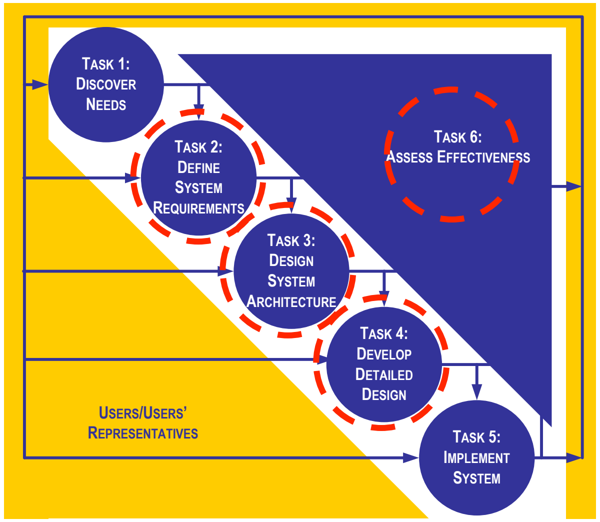
* Reference: *Information Assurance Technical Framework* (IATF), Release 3.1


Task 1: Discover Needs
Task 2: Define System Requirements
Task 3: Design System Architecture
Task 4: Develop Detailed Design
Task 5: Implement System
Task 6: Assess Effectiveness
Users/Users' Representatives

- Key Deliverables
  - Mission Needs Statement / Project Goal(s) and Objectives
  - System Capabilities
  - Preliminary CONOPS
  - Preliminary System Context Descriptions
  - Project Risk Assessment
  - Draft System Engineering Management Plan (SEMP)

BY-NC-SA

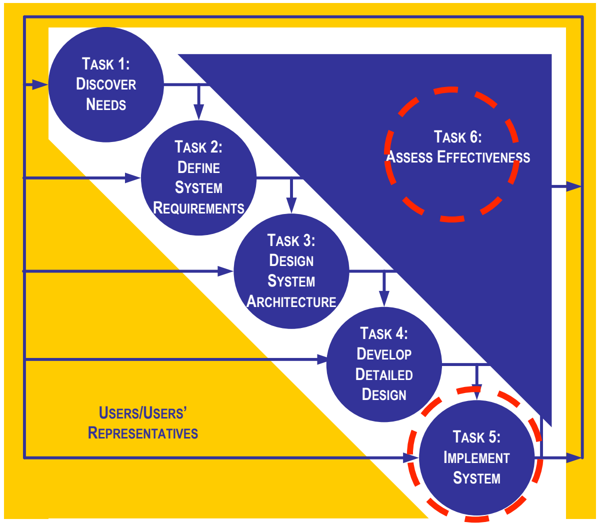
IEEE 1220	DoD Acquisition SDLC	Key System Engineering Tasks	Key Security Engineering Tasks
Development Stage	Technology Development	**Task 2: Define System Requirements**	**Task 2: Define Security Requirements**
		• Refine system context (e.g., functional components)	
		• Define system requirements (e.g., functional, performance, operational, support, etc.)	• Select assurance requirements and define security functional requirements
		• Refine CONOPS	• Refine IMM and SSP
		• Baseline system requirements	
	Milestone B	**Task 6: Assess project performance in meeting mission/business needs**	
	System Development & Demonstration	**Task 3: Design System Architecture**	**Task 3: Design System Security Architecture**
		• Determine & select architecture framework	
		• Design system architecture and allocate system requirements to subsystems and components (i.e., RTM)	• Allocate system security requirements to subsystems and service components (i.e., RTM)
		• Analyze gaps (i.e., risk assessment)	
		Task 4: Develop Detailed System Design (Logical & Physical)	**Task 4: Develop Detailed System Security Design (Logical & Physical)**
		• Refine entity-data relations model (i.e., UML diagrams, data-flow, network, etc.)	• Refine IMM, embed security controls into system design products (i.e., UML, data-flow, network, etc.)
		• Perform system synthesis analysis to assure system integration (i.e., system design, system architecture, system requirements, and project mission/business needs)	
	Milestone C	**Task 6: Assess project performance in meeting mission/business needs**	


TASK 1: DISCOVER NEEDS
TASK 2: DEFINE SYSTEM REQUIREMENTS
TASK 3: DESIGN SYSTEM ARCHITECTURE
TASK 4: DEVELOP DETAILED DESIGN
TASK 5: IMPLEMENT SYSTEM
TASK 6: ASSESS EFFECTIVENESS
USERS/USERS' REPRESENTATIVES

- Key Deliverables
  - – System Requirements
  - – Functional Definitions (+ allocation of system requirements)
  - – System Architecture (Contextual + Logical)
  - – Detailed System Design (Logical + Physical)
  - – Requirements Traceability Matrix (RTM)

(cc) BY-NC-SA

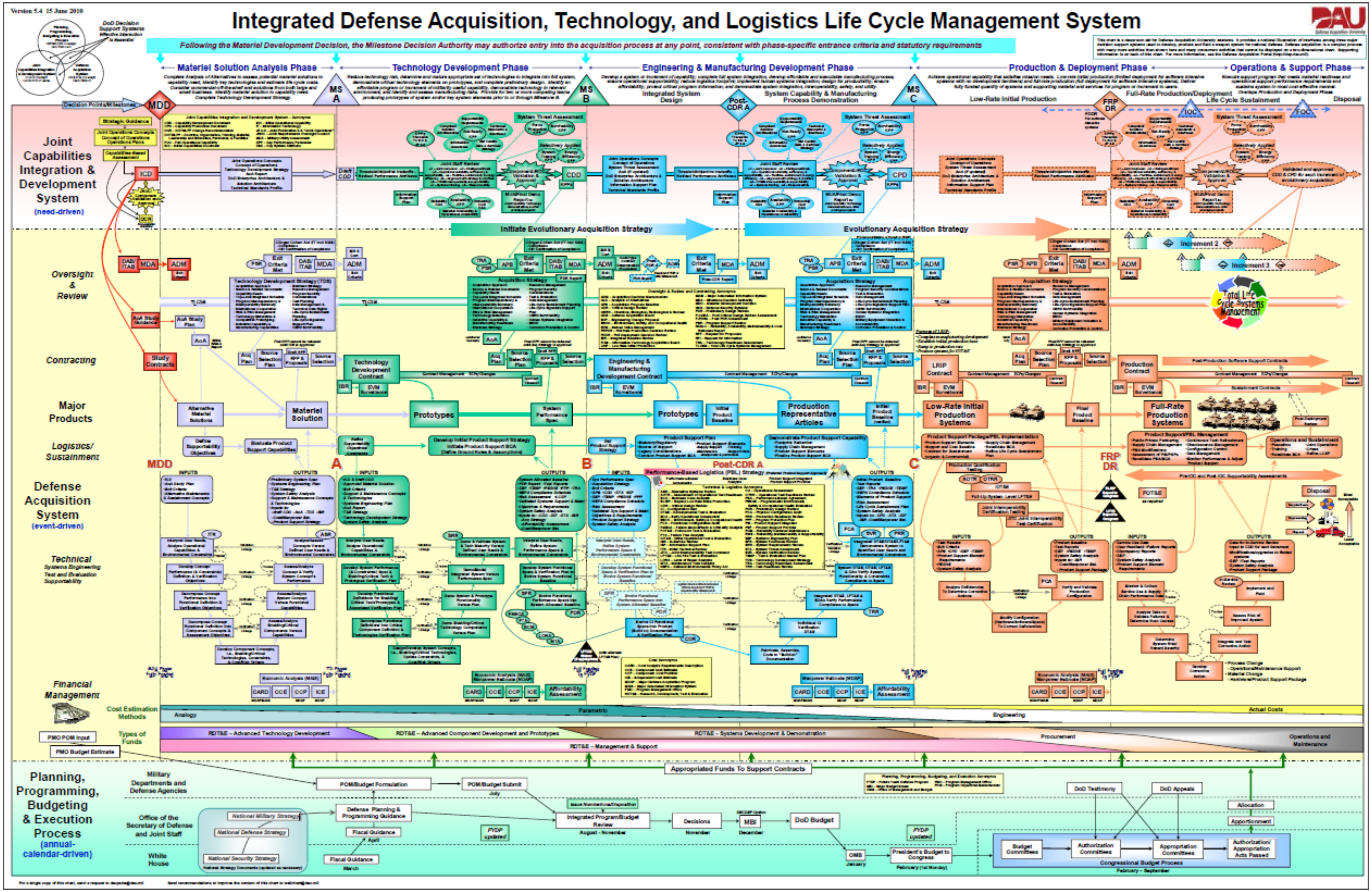
IEEE 1220	DoD Acquisition SDLC	Key System Engineering Tasks	Key Security Engineering Tasks
Production Stage	Production and Deployment	**Task 5: Implement System Design**	**Task 5: Implement Security Controls**
		• Procure system components / construct system	
		• Code/ customize/ configure system functional components	
		• Conduct code inspection/ walk-through/ unit test	
		• Perform system integration	
		• Conduct system test	• Conduct security test & evaluation (ST&E)
		Task 6: Assess project performance in meeting mission/business needs	
		• Generate system operations procedure (SOP) and users guide/ manual	• Generate SOP (a.k.a. trusted facility manual (TFM)), Incident response plan, business continuity plan (BCP)
		• Conduct system readiness review	• Obtain system certification
		• Deploy system	
		• Conduct system acceptance test	• Assess security effectiveness
		• Obtain approval to operate (ATO)	


Task 1: Discover Needs
Task 2: Define System Requirements
Task 3: Design System Architecture
Task 4: Develop Detailed Design
Task 5: Implement System
Task 6: Assess Effectiveness
Users/Users' Representatives

- Key Deliverables
  - Implement detailed system design
  - Perform test & evaluations (unit, system, security tests)
  - Test reports
  - Standard Operating Procedure (SOP) + User Manuals
  - Deploy system
  - Conduct acceptance tests

(cc) BY-NC-SA

Example of SDLC in a Defense Acquisition Lifecycle


Version 5.4 15 June 2010
Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System
DAU
DoD Decision Support Systems Effective Interaction Is Essential
Following the Materiel Development Decision, the Milestone Decision Authority may authorize entry into the acquisition process at any point, consistent with phase-specific entrance criteria and statutory requirements
Materiel Solution Analysis Phase
Technology Development Phase
Engineering & Manufacturing Development Phase
Production & Deployment Phase
Operations & Support Phase
Decision Points/Milestones
MDD
MS A
MS B
MS C
Integrated System Design
Post-CDR A
System Capability & Manufacturing Process Demonstration
Low-Rate Initial Production
FRP DR
Full-Rate Production/Deployment
Life Cycle Sustainment
Disposal
IOC
FOC
Joint Capabilities Integration & Development System
(need-driven)
Strategic Guidance
Joint Operations Concepts Concept of Operations Operations Plans
Capabilities-Based Assessment
ICD
Draft CDD
CDD
CPD
System Threat Assessment
Selectively Applied
Joint Staff Review
Initiate Evolutionary Acquisition Strategy
Evolutionary Acquisition Strategy
Increment 2
Increment 3
Oversight & Review
DAB/ITAB
MDA
ADM
AoA Study Guidance
AoA Study Plan
AoA
Exit Criteria Met
Acquisition Strategy
Total Life Cycle Systems Management
Contracting
Study Contracts
Technology Development Contract
Engineering & Manufacturing Development Contract
LRIP Contract
Production Contract
Major Products
Alternative Materiel Solutions
Materiel Solution
Prototypes
System Performance Spec
Initial Product Baseline
Production Representative Articles
Initial Product Baseline Verified
Low-Rate Initial Production Systems
Final Product Baseline
Full-Rate Production Systems
Logistics/Sustainment
MDD
A
B
Post-CDR A
C
FRP DR
Performance-Based Logistics (PBL) Strategy
Defense Acquisition System
(event-driven)
INPUTS
OUTPUTS
Technical
Systems Engineering
Test and Evaluation
Supportability
Financial Management
Cost Estimation Methods
Analogy
Parametric
Engineering
Actual Costs
Types of Funds
RDT&E – Advanced Technology Development
RDT&E – Advanced Component Development and Prototypes
RDT&E – Systems Development & Demonstration
Procurement
Operations and Maintenance
RDT&E – Management & Support
PMO POM Input
PMO Budget Estimate
CARD
CCE
CCP
ICE
Affordability Assessment
Appropriated Funds To Support Contracts
Planning, Programming, Budgeting & Execution Process
(annual-calendar-driven)
Military Departments and Defense Agencies
Office of the Secretary of Defense and Joint Staff
White House
National Military Strategy
National Defense Strategy
National Security Strategy
POM/Budget Formulation
POM/Budget Submit
Defense Planning & Programming Guidance
Fiscal Guidance
Integrated Program/Budget Review
Decisions
MBI
DoD Budget
FYDP updated
OMB
President's Budget to Congress
DoD Testimony
DoD Appeals
Budget Committees
Authorization Committees
Appropriation Committees
Authorization/Appropriation Acts Passed
Allocation
Apportionment
Congressional Budget Process

* **Source**: *Integrated Life Cycle Chart* (https://ilc.dau.mil/)

BY-NC-SA

Example: SDLC in a Defense Acquisition Lifecycle

- Security engineering is ubiquitously in…
  - Planning, Programming, Budget & Execution (PPBE) Process
  - Joint Capabilities Integration & Development System (JCIDS) process
  - Management & Oversight process(Project/Program Management), and
  - Systems engineering process

(cc) BY-NC-SA

Questions:

- What classic system development life cycle (SDLC) model allows system engineers go back to the previous step?
  –

- What iterative SDLC model allows system engineers to evaluate, refine, plan and construct an information system utilizing a series of prototypes ?
  –

- Which SDLC model requires formal verification and validation of requirements at the unit-level, system-level, and operational-level?
  –

(cc) BY-NC-SA

Questions:

- What classic system development life cycle (SDLC) model allows system engineers go back to the previous step?
  - Modified Waterfall

- What iterative SDLC model allows system engineers to evaluate, refine, plan and construct an information system utilizing a series of prototypes ?
  - Spiral Model

- Which SDLC model requires formal verification and validation of requirements at the unit-level, system-level, and operational-level?
  - The V-Model, IEEE 12207 or ISO/IEC 12207

(cc) BY-NC-SA

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

What is a Risk?

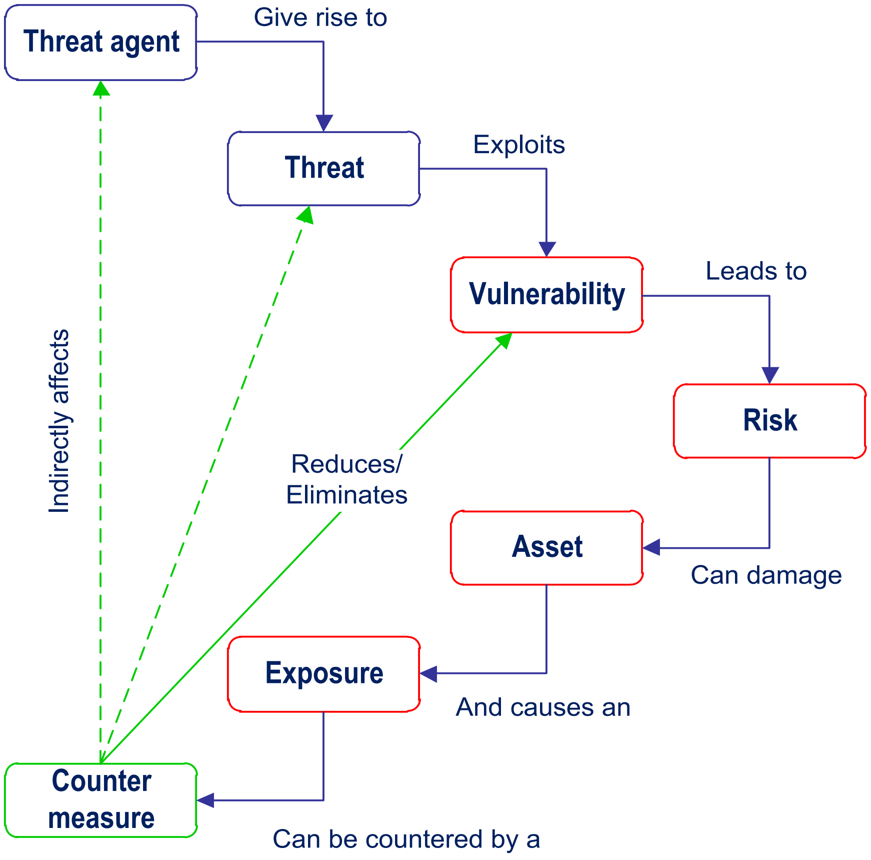
- Risk is the relationship between the likelihood of a loss and the potential impact to the business (/ mission).

- For information security, risk is defined as:
  - The likelihood of a threat agent (a threat) exploiting vulnerabilities in a “system” (/ system of systems), where “system” = people + process + technology; and
  - The potential impact of a successful attack to an organization’s information operations.

(cc) BY-NC-SA

Relationship between Threat, Risk, and Countermeasure

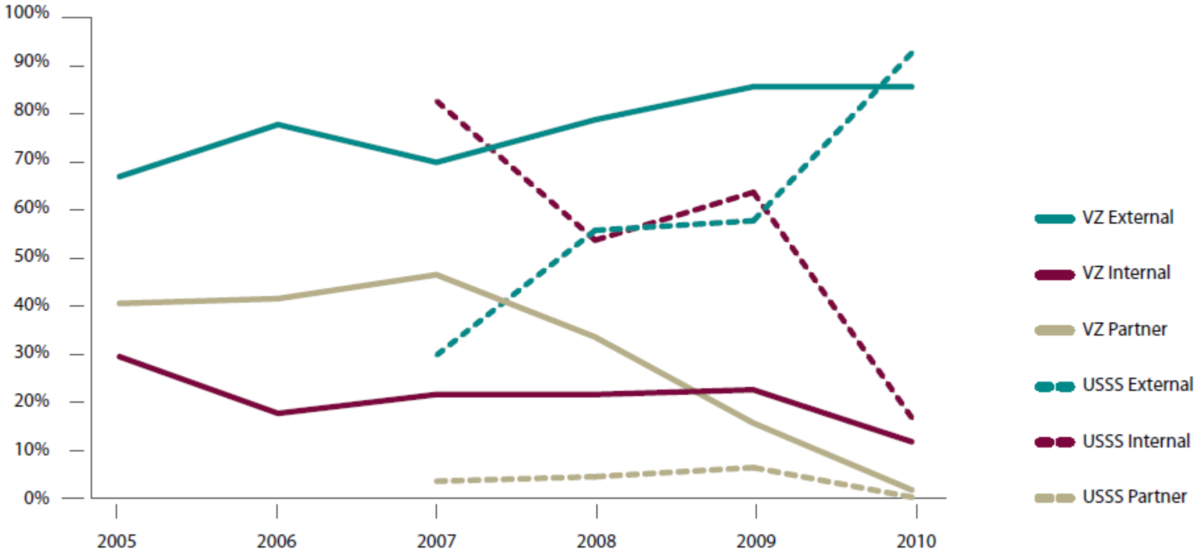
- Threat Agent. An entity that may act on a vulnerability.
- Threat. Any potential danger to information life cycle.
- Vulnerability. A weakness or flaw that may provide an opportunity for a threat agent.
- Risk. The likelihood of a threat agent exploits a discovered vulnerability.
- Exposure. An instance of being compromised by a threat agent.
- Countermeasure / safeguard. An administrative, operational, or logical mitigation against potential risk(s).



(cc) BY-NC-SA

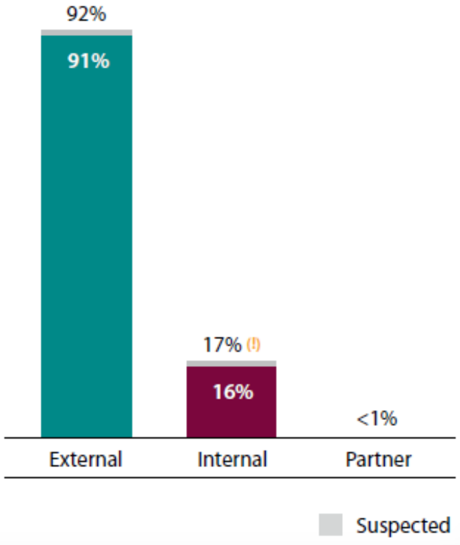
Threat to Information Operations

- Operations are getting better at addressing insider threats



  - » VZ (Verizon)
  - » USSS (United States Secret Service)

- Most of threats are from external threat agents

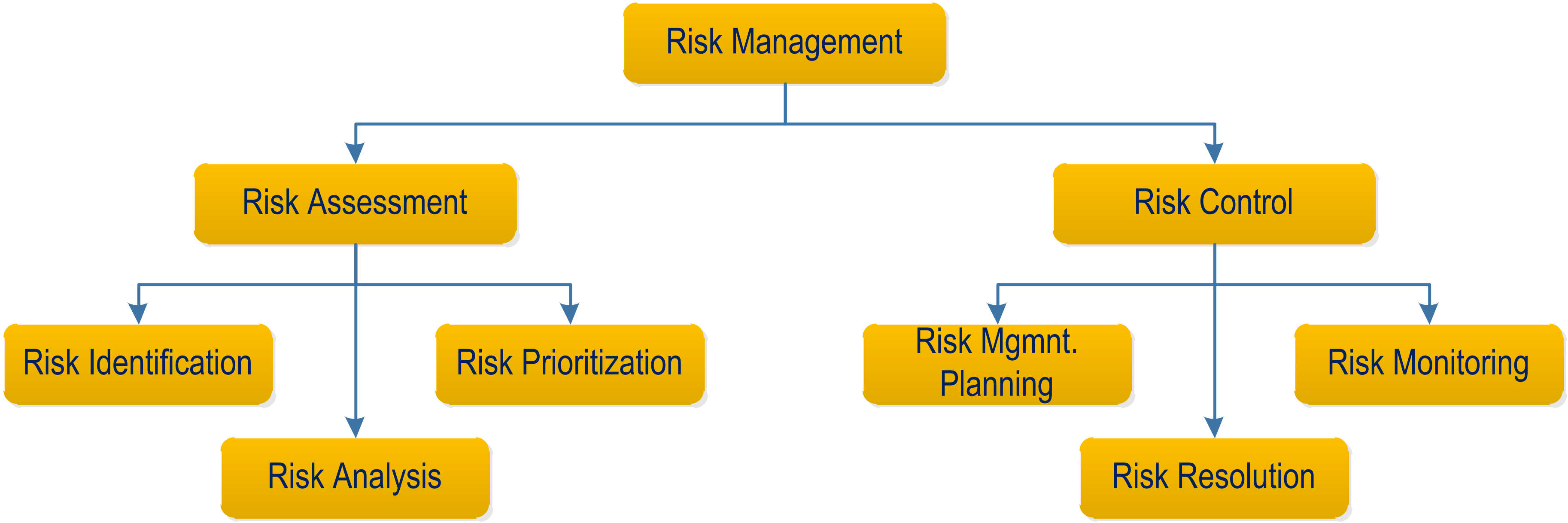


Reference: *2011 Data Breach Investigations Report*, Verizon, January 2012 (http://www.verizonbusi resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf)

(cc) BY-NC-SA

Risk Management Practice

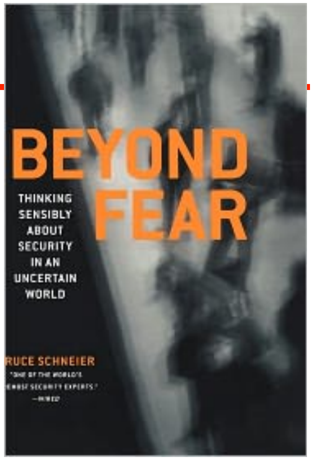
- Risk management practice is composed of:
  - Risk assessment activities: risk identification, risk analysis, and risk prioritization
  - Risk control activities: risk management planning, risk resolution, and risk monitoring



Reference: *Software Risk Management*, B. Boehm, IEEE Computer Society Press , 1989.

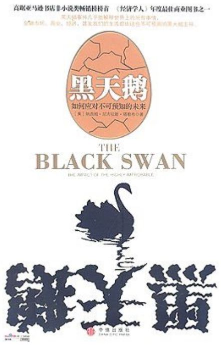
(cc) BY-NC-SA

"All Security Involves Trade-offs"



- Step 1: What assets are you trying to protect?
- Step 2: What are the risks to these assets?
- Step 3: How well does the security solution mitigate those risks?
- Step 4: What other risks does the security solution cause?
- Step 5: What cost and trade-offs does the security solution impose?

- And looking out for the "black swan"...



Reference:

- *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Bruce Schneier, Springer, 2003.
- *The Black Swan: The Impact of the Highly Improbable*, Nassim Nicholas Taleb, Random House, 2007.

(cc) BY-NC-SA

Current State of Insecurity in Federal Agencies

- "The 25 major agencies of Federal government continue to improve information security performance relative to C&A rate and testing of contingency plans and security controls." – OMB *FY 2008 Report to Congress on Implementation of FISMA*.

% of System with a:	FY 2005	FY 2006	FY 2007	FY 2008	FY 2009
Certification and Accreditation (C&A)	85%	88%	92%	96%	**95%**
Tested Contingency Plan	61%	77%	86%	92%	**86%**
Tested Security Controls	72%	88%	95%	93%	**90%**
Total Systems Reported	10,289	10,595	10,304	10,679	12,930

- # of security incidents keeps growing*…

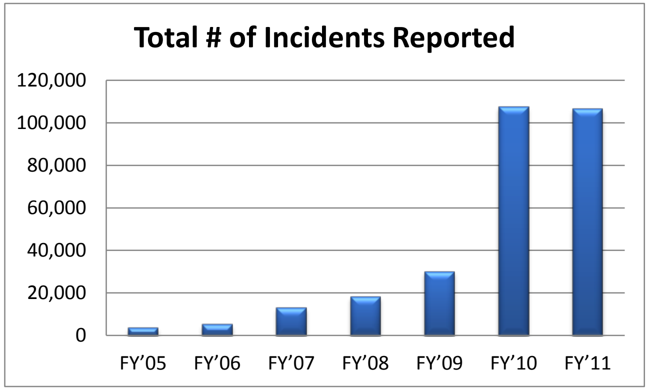
Incident Categories	FY 2005	FY 2006	FY 2007	FY2008	FY2009
1. Unauthorized Access	304	706	2,321	3,214	**4,848**
2. Denial of Service	31	37	36	26	48
3. Malicious Code	1,806	1,465	1,607	2,274	**6,977**
4. Improper Usage	370	638	3,305	3,762	**6,148**
5. Scans/Probes/Attempted Access	976	1,388	1,661	1,272	1,152
6. Under Investigation	82	912	4,056	7,502	**10,826**
Total Incidents Reported	3,569	5,146	12,986	18,050	29,999

* **Source:** OMB and US-CERT

(cc) BY-NC-SA

C&A ≠ Risk Management

- "… seven years after the passage of FISMA and approximately $40 billion later, I am troubled to learn that the Office of Management and Budget does not track how much agencies spend on cyber security or measure whether those expenditures actually resulted in improved security." * – Senator Tom Carper
  - For FY08, OMB reported 93% of federal information systems had their security controls tested.
  - Yet, between FY05 and FY09, the total number of reported security incidents had increased by over 740%.**



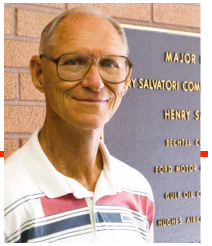
Source:

* Congressional hearing: *More Security, Less What Makes Sense for our Federal Cyber Defense*, October 29, 2009.

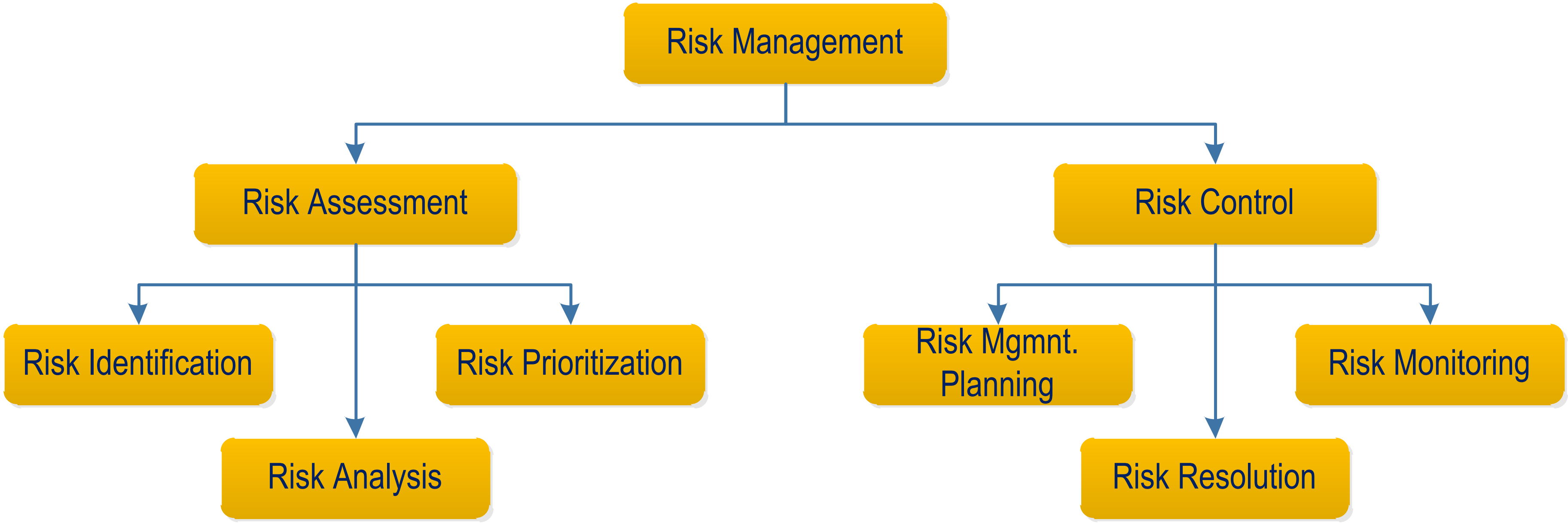
** US-CERT

BY-NC-SA

Fundamental revisited



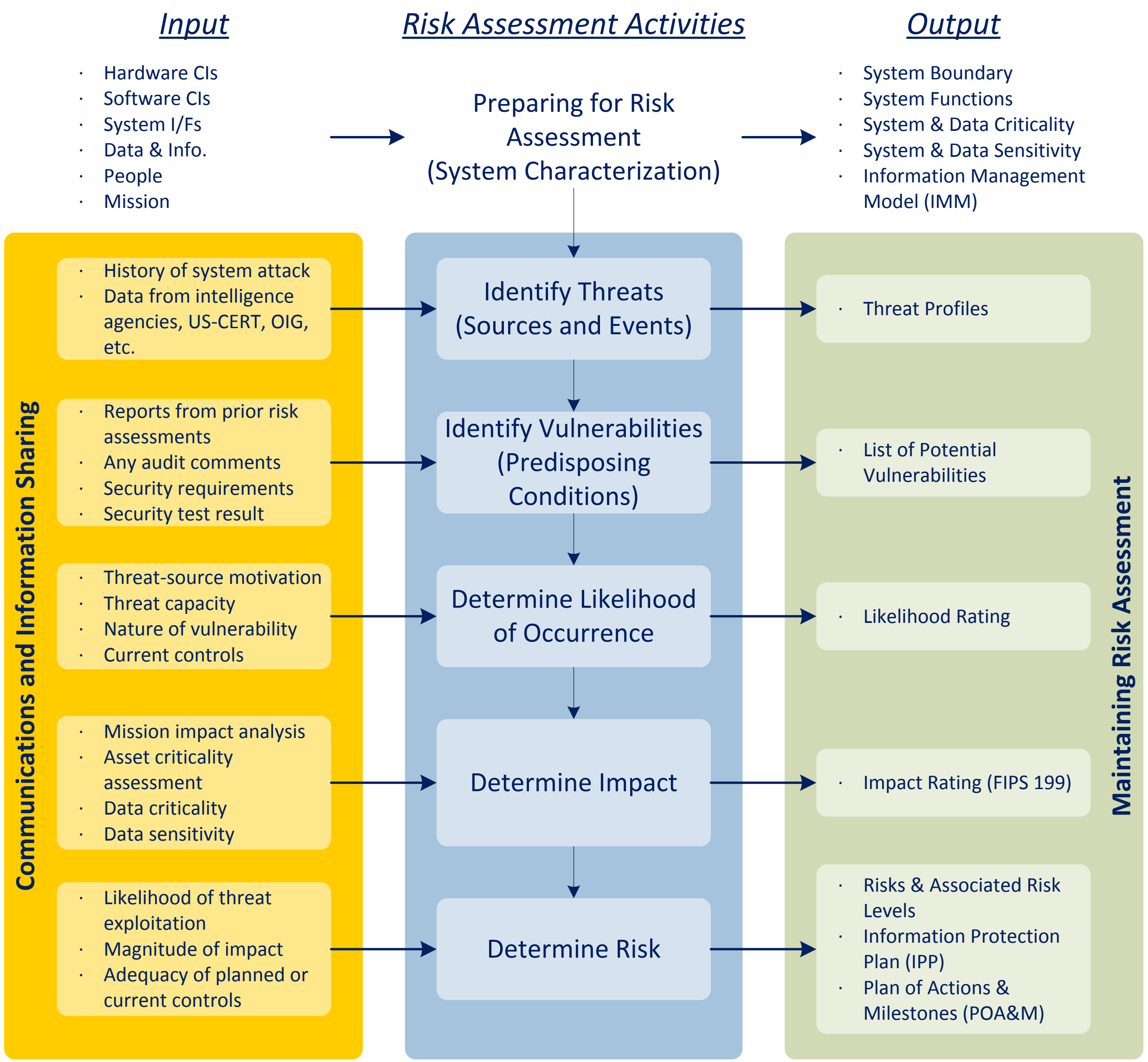
- Risk assessment activities: risk identification, risk analysis, and risk prioritization
- Risk control activities: risk management planning, risk resolution, and risk monitoring



Reference: *Software Risk Management*, B. Boehm, IEEE Computer Society Press , 1989.

(cc) BY-NC-SA

Risk Assessment Process



Input

- Hardware CIs
- Software CIs
- System I/Fs
- Data & Info.
- People
- Mission

Risk Assessment Activities

Preparing for Risk Assessment (System Characterization)

Output

- System Boundary
- System Functions
- System & Data Criticality
- System & Data Sensitivity
- Information Management Model (IMM)

Communications and Information Sharing

- History of system attack
- Data from intelligence agencies, US-CERT, OIG, etc.

Identify Threats (Sources and Events)

- Threat Profiles

- Reports from prior risk assessments
- Any audit comments
- Security requirements
- Security test result

Identify Vulnerabilities (Predisposing Conditions)

- List of Potential Vulnerabilities

- Threat-source motivation
- Threat capacity
- Nature of vulnerability
- Current controls

Determine Likelihood of Occurrence

- Likelihood Rating

- Mission impact analysis
- Asset criticality assessment
- Data criticality
- Data sensitivity

Determine Impact

- Impact Rating (FIPS 199)

- Likelihood of threat exploitation
- Magnitude of impact
- Adequacy of planned or current controls

Determine Risk

- Risks & Associated Risk Levels
- Information Protection Plan (IPP)
- Plan of Actions & Milestones (POA&M)

Maintaining Risk Assessment

Reference:
- NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments, Sept. 2011*

(cc) BY-NC-SA

Risk Assessment Methods

Quantitative

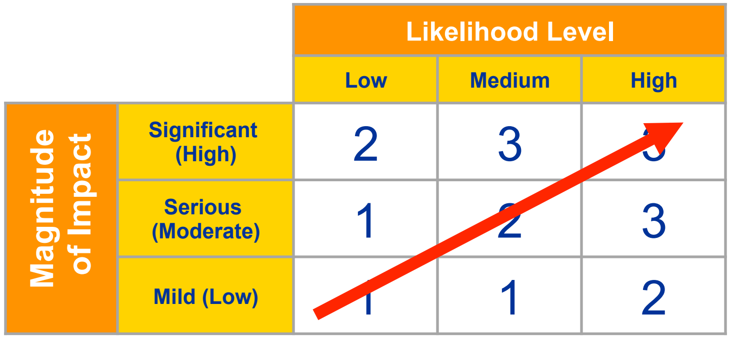
ALE = SLE x ARO

SLE = AV x EF

- Annualized Lost Expectance (ALE).
- Single Loss Expectance (SLE). Monetary loss (impact) for each occurrence of a threatened event
- Annualized Rate of Occurrence (ARO). The frequency which a threat is expected to occur on an annualized basis
- Asset Value (AV). Monetary value of the information asset
- Exposure Factor (EF). Percentage of loss from a specific threat.

Qualitative

- Likelihood Determination
  - Threat agent motivation & capability
  - Nature of the vulnerability
  - Existence and effectiveness of current controls.
- Impact Analysis (Confidentiality, Integrity & Availability)
  - System mission (e.g., the processes performed by the IT system)
  - System and data criticality (e.g., the system's value or importance to an organization)
  - System and data sensitivity.



		Likelihood Level		
		Low	Medium	High
Magnitude of Impact	Significant (High)	2	3	3
	Serious (Moderate)	1	2	3
	Mild (Low)	1	1	2

SC $_{\text{information type}}$ = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}, where the acceptable values for potential impact are low, medium, or high.

(cc) BY-NC-SA

Risk Assessment Methods: Quantitative vs. Qualitative

Quantitative

- **Pros**
  - Assessment & results are based substantially on independently objective processes & metrics. Thus, meaningful statistical analysis is supported.
  - The value of information are expressed in monetary terms with supporting rationale, is better understood. Thus, the basis for expected loss is better understood.
  - A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, information security budget decision-making is supported.
- **Cons**
  - Calculations are complex. If they are not understood or effectively explained, management may mistrust the results.
  - A substantial amount of information about the target information & its IT environment must be gathered
  - There is not yet a standard, independently developed & maintained threat population & frequency knowledge base.

Qualitative

- **Pros**
  - Calculations are simple and readily understood and executed.
  - Not necessary to determine quantitative threat frequency & impact data.
  - Not necessary to estimate the cost of recommended risk mitigation measures & calculate cost/benefit.
  - A general indication of significant areas of risk that should be addressed is provided.
- **Cons**
  - Risk assessment & results are essentially subjective in both process & metrics. Use of independently objective metrics is eschewed.
  - No effort is made to develop an objective monetary basis for the value of targeted information assets.
  - No basis is provided for cost/benefit analysis of risk mitigation measures. Only subjective indication of a problem.
  - It is not possible to track risk management performance objectively when all measures are subjective.

(cc) BY-NC-SA

Risk Control – Determine Information Protection Needs

Mode of Operations: **System-High**

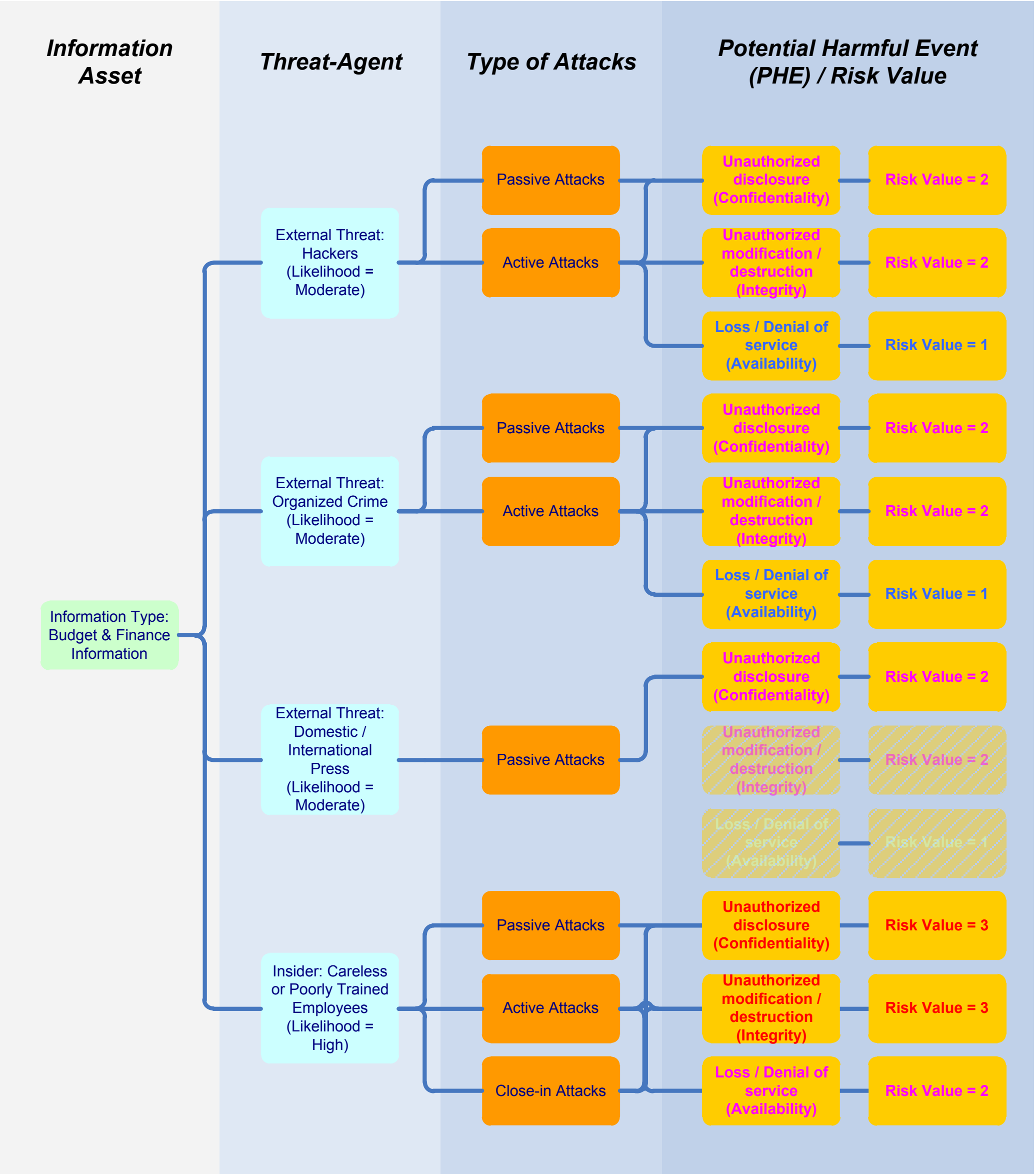
Data Sensitivity: **SBU/FOUO**

SC (**Budget & Finance**) = {Conf.(**M**), Integ.(**M**), Avail.(**L**)}

Threat agent (Likelihood):

- Hackers (**Moderate**)
- Organized Crime (**Moderate**)
- International Press (**Moderate**)
- Careless/Poorly Trained Employees (**High**)

	PHE (Threat Likelihood)		
Severity of HTI (Impact)	**Low**	**Moderate**	**High**
Significant (High)	2	3	3
Serious (Moderate)	1	2	3
Mild (Low)	1	1	2



Information Asset

Threat-Agent

Type of Attacks

Potential Harmful Event (PHE) / Risk Value

Information Type: Budget & Finance Information

External Threat: Hackers (Likelihood = Moderate)

Passive Attacks

Active Attacks

Unauthorized disclosure (Confidentiality) – Risk Value = 2

Unauthorized modification / destruction (Integrity) – Risk Value = 2

Loss / Denial of service (Availability) – Risk Value = 1

External Threat: Organized Crime (Likelihood = Moderate)

Passive Attacks

Active Attacks

Unauthorized disclosure (Confidentiality) – Risk Value = 2

Unauthorized modification / destruction (Integrity) – Risk Value = 2

Loss / Denial of service (Availability) – Risk Value = 1

External Threat: Domestic / International Press (Likelihood = Moderate)

Passive Attacks

Unauthorized disclosure (Confidentiality) – Risk Value = 2

Unauthorized modification / destruction (Integrity) – Risk Value = 2

Loss / Denial of service (Availability) – Risk Value = 1

Insider: Careless or Poorly Trained Employees (Likelihood = High)

Passive Attacks

Active Attacks

Close-in Attacks

Unauthorized disclosure (Confidentiality) – Risk Value = 3

Unauthorized modification / destruction (Integrity) – Risk Value = 3

Loss / Denial of service (Availability) – Risk Value = 2

BY-NC-SA

Risk Control – Risk Management Actions

- Risk Acceptance
  - Establish risk acceptance criteria to determine what is acceptable.
- Risk Mitigation
  - Establish plan of action & milestone (POA&M) for implementing safeguards and countermeasures.
- Risk Transfer
  - Transfer the potential liability to another entity (e.g., insurance company.)

- Total Risk = ∑ (Threats x Vulnerability x Asset value)
- Residual Risk = (Total Risk) – (Countermeasures and Safeguards)

(cc) BY-NC-SA

Questions

- What are the two types of risk analysis methods?
  - –
  - –

- What type of risk analysis requires the potential impact be measured in financial terms?
  - –

- What type of risk analysis requires the potential impact be adjudicated in terms of “severity of loss”?
  - –

(cc) BY-NC-SA

Answers

- What are the two types of risk analysis methods?
  - Qualitative
  - Quantitative

- What type of risk analysis requires the potential impact be measured in financial terms?
  - Quantitative

- What type of risk analysis requires the potential impact be adjudicated in terms of “severity of loss”?
  - Qualitative

(cc) BY-NC-SA

Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Policies, Standards, Procedures, and Guidelines
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- ➡ Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training & Awareness

(cc) BY-NC-SA

Concept

- Certification is a disciplined approach to evaluate level of conformance to the prescribed security requirements and the implemented security controls to a security enclave.

- Accreditation is the official management decision to operate the certified system(s). It is also a formal acceptance of the responsibility to the security of the certified system(s).

- C&A does not guarantee the system(s) free of vulnerability and risks… hence, the need for periodic security (or vulnerability) assessments.

(cc) BY-NC-SA

We are in a “Transition Period”

- The concept of C&A is still around...
  - It’s a cultural thing.
  - Most of IG security auditors, and many agency information assurance (IA) professionals are sorting out RMF & ongoing security authorization
- C&A has a long history...
  - Computer Security Act of 1987 → FISMA 2002
  - The Rainbow Series/DoD 5200.28-STD (TCSEC) → NIST SP 800-37/DoDI 8500.2 → NIST 800-37, Rev. 1/CNSSP-22
- For CISSP, we just need to learn the broad concept of C&A

(cc) BY-NC-SA

Process & Guideline

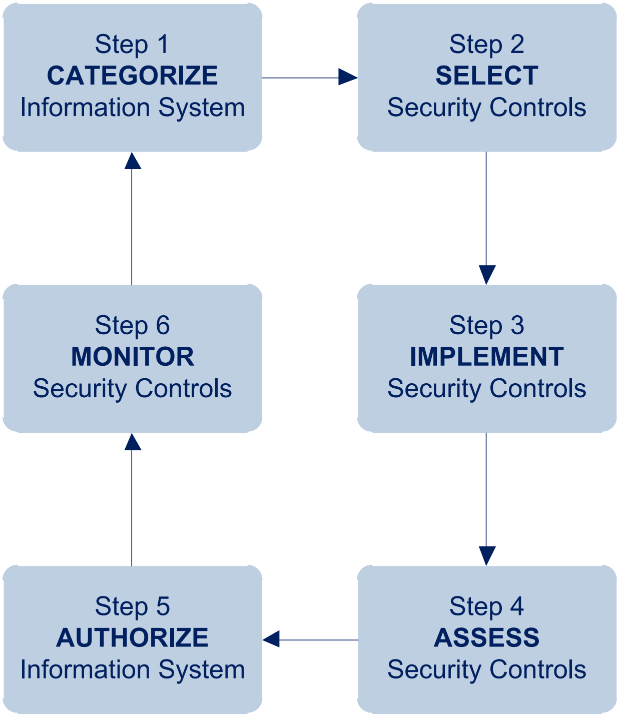
Standard ~~C&A~~ / Security Authorization Processes:

- For Federal Information Systems
  - Civil: NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010

- For National Security Systems (NSS)
  - Civil: CNSSP-22, *Information Assurance Risk Management Policy for National Security Systems*, January 2012
  - Military: DoDI 8510.01, ~~*Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*~~ → *Risk Management Framework (RMF) DoD Information Technology (IT)*, March 12, 2014.

(cc) BY-NC-SA

Risk Management Framework – Management Process



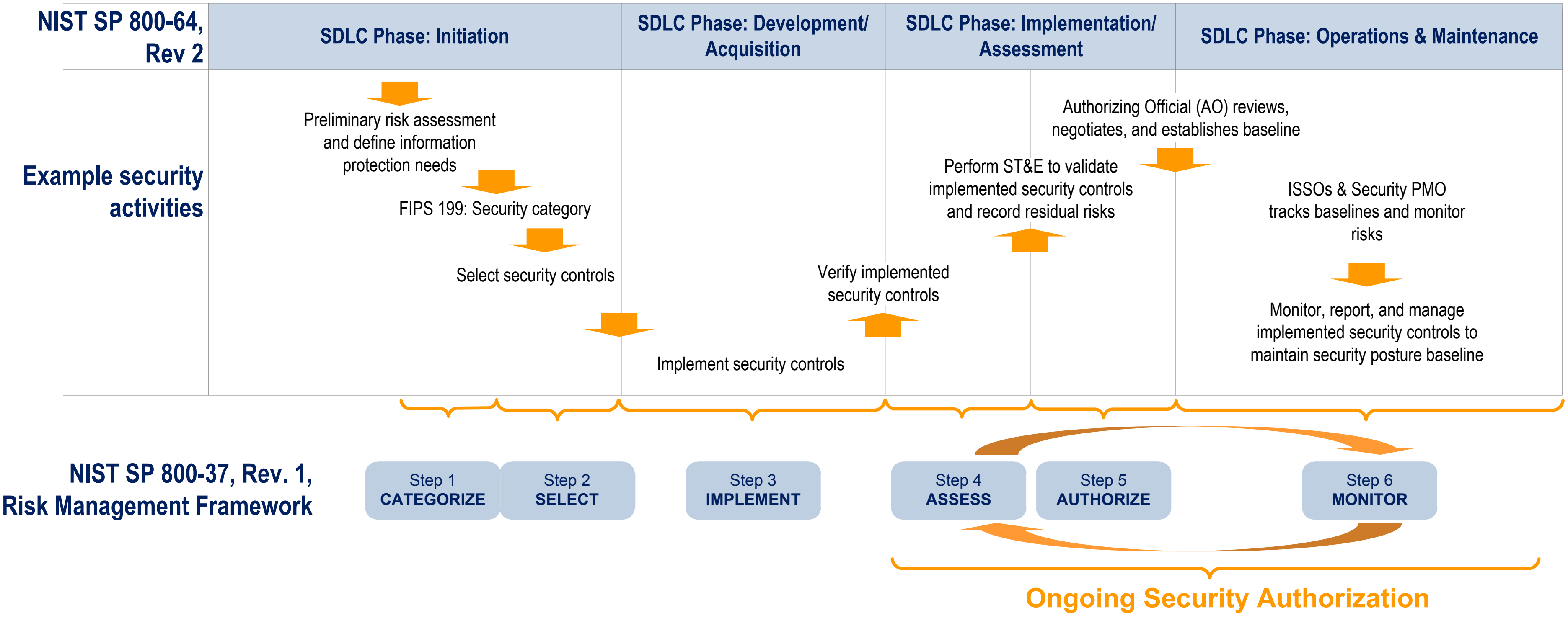
Objectives:

- To ensure that managing information system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy established by the senior leadership through the risk executive (function);
- To ensure that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes;
- To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity; and
- To achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.

Reference: NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach*, Joint Task Force Transformation Initiative, February 2010.

(cc) BY-NC-SA

Risk Management Framework & System Life Cycle



NIST SP 800-64, Rev 2

SDLC Phase: Initiation

SDLC Phase: Development/ Acquisition

SDLC Phase: Implementation/ Assessment

SDLC Phase: Operations & Maintenance

Example security activities

Preliminary risk assessment and define information protection needs

FIPS 199: Security category

Select security controls

Implement security controls

Verify implemented security controls

Perform ST&E to validate implemented security controls and record residual risks

Authorizing Official (AO) reviews, negotiates, and establishes baseline

ISSOs & Security PMO tracks baselines and monitor risks

Monitor, report, and manage implemented security controls to maintain security posture baseline

NIST SP 800-37, Rev. 1, Risk Management Framework

Step 1 CATEGORIZE

Step 2 SELECT

Step 3 IMPLEMENT

Step 4 ASSESS

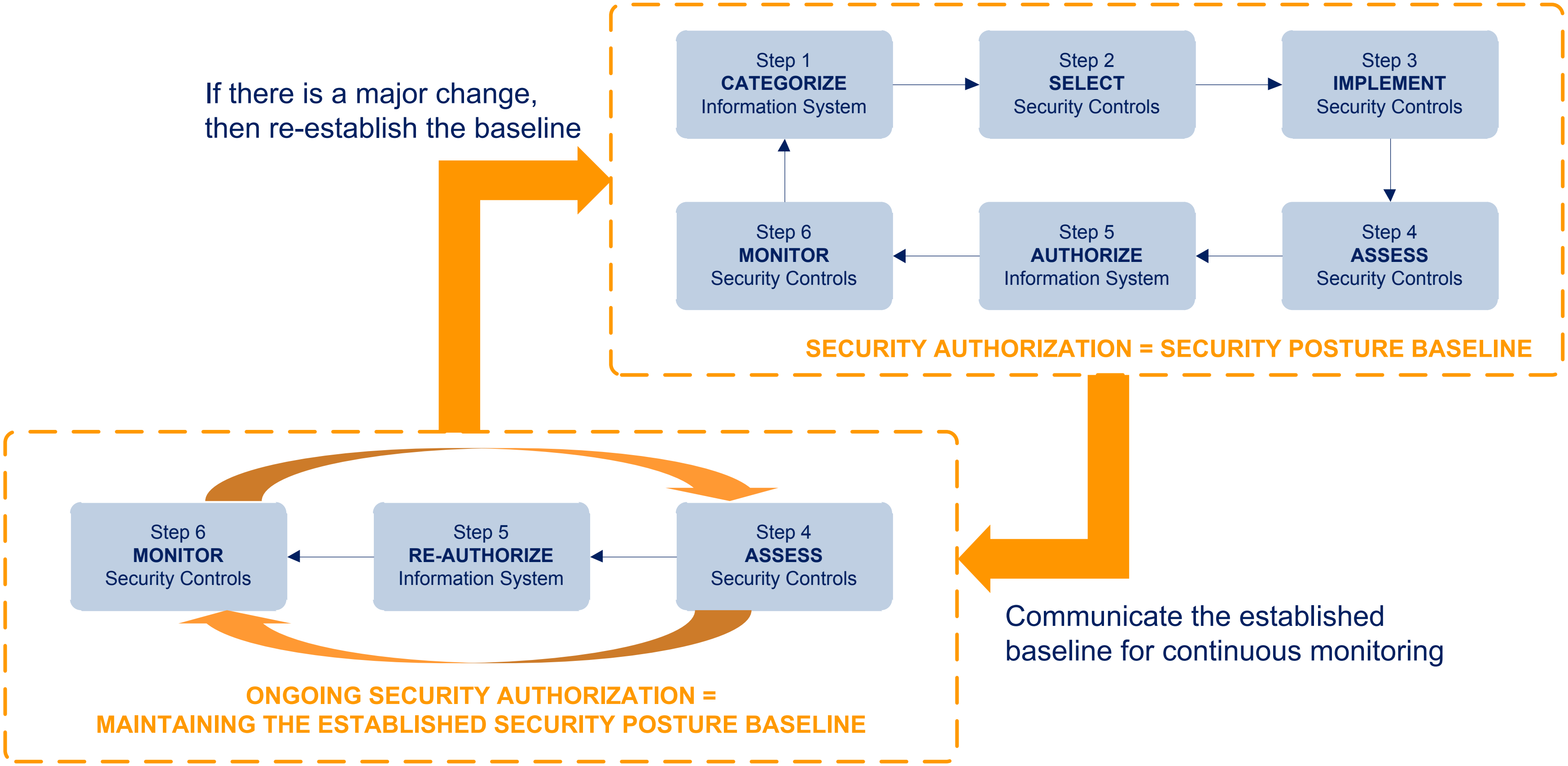
Step 5 AUTHORIZE

Step 6 MONITOR

Ongoing Security Authorization

BY-NC-SA

Risk Management Framework and Ongoing Security Authorization



If there is a major change, then re-establish the baseline

Step 1 **CATEGORIZE** Information System

Step 2 **SELECT** Security Controls

Step 3 **IMPLEMENT** Security Controls

Step 4 **ASSESS** Security Controls

Step 5 **AUTHORIZE** Information System

Step 6 **MONITOR** Security Controls

SECURITY AUTHORIZATION = SECURITY POSTURE BASELINE

Communicate the established baseline for continuous monitoring

Step 4 **ASSESS** Security Controls

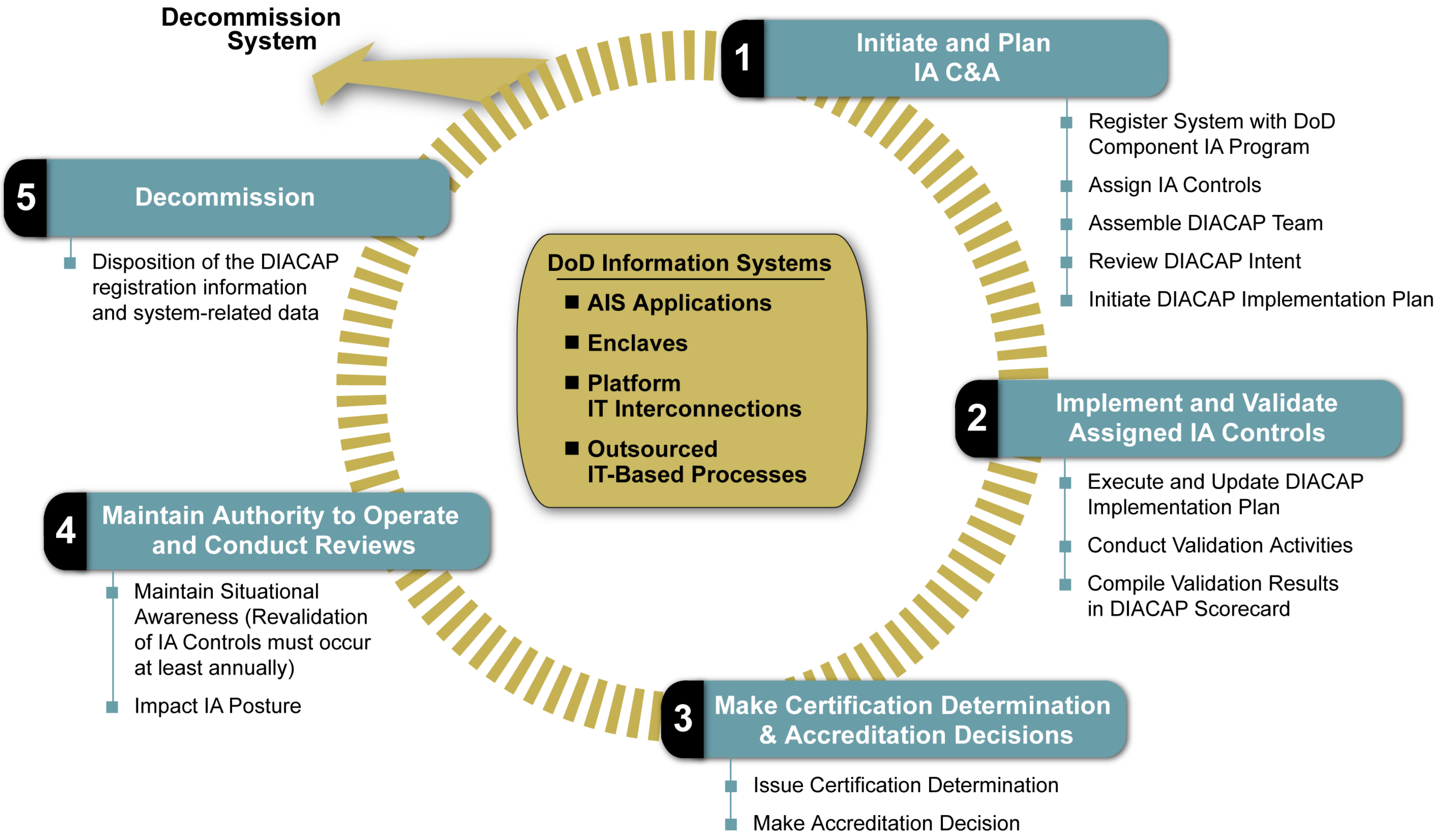
Step 5 **RE-AUTHORIZE** Information System

Step 6 **MONITOR** Security Controls

ONGOING SECURITY AUTHORIZATION = MAINTAINING THE ESTABLISHED SECURITY POSTURE BASELINE

(cc) BY-NC-SA

DIACAP



Decommission System

DoD Information Systems

- AIS Applications
- Enclaves
- Platform IT Interconnections
- Outsourced IT-Based Processes

1 Initiate and Plan IA C&A

- Register System with DoD Component IA Program
- Assign IA Controls
- Assemble DIACAP Team
- Review DIACAP Intent
- Initiate DIACAP Implementation Plan

2 Implement and Validate Assigned IA Controls

- Execute and Update DIACAP Implementation Plan
- Conduct Validation Activities
- Compile Validation Results in DIACAP Scorecard

3 Make Certification Determination & Accreditation Decisions

- Issue Certification Determination
- Make Accreditation Decision

4 Maintain Authority to Operate and Conduct Reviews

- Maintain Situational Awareness (Revalidation of IA Controls must occur at least annually)
- Impact IA Posture

5 Decommission

- Disposition of the DIACAP registration information and system-related data

Reference: DoDI 8510.1 *Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*

(cc) BY-NC-SA

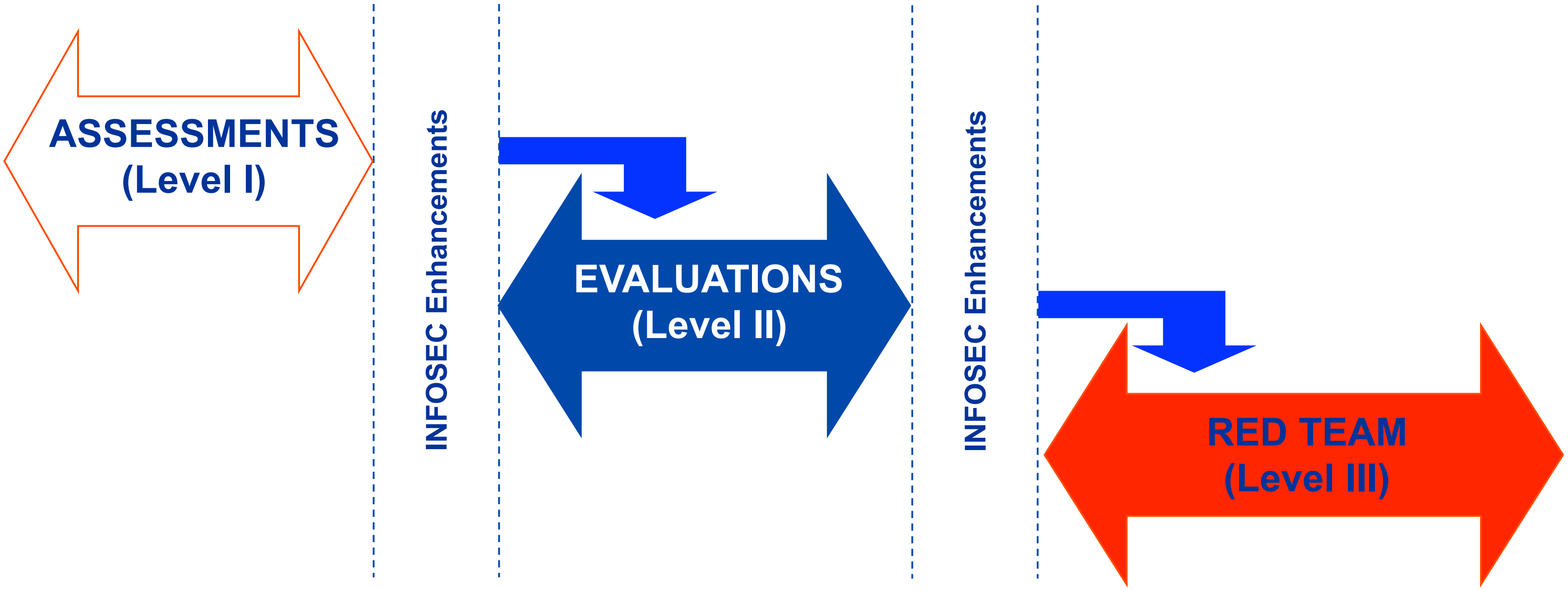
Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- ➡ Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

NSA Defined Security Assessment Methodology



- Cooperative High Level Overview
- Information / Mission Critical Analysis (Compliance Audit)
- Inventory Audit of Assets
- Information / Data Flow Analysis

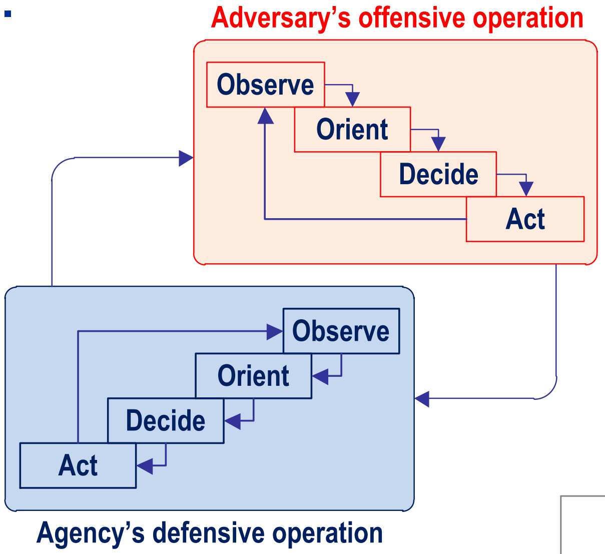
- Security Process Audit / Analysis
- Detailed Inventory Audit of Assets
- Cooperative Security Testing / Audit
  - Non-Intrusive Tests
  - Penetration Tests

- Non-cooperative Security Testing
  - External Penetration Tests
- Simulation of Appropriate Adversary

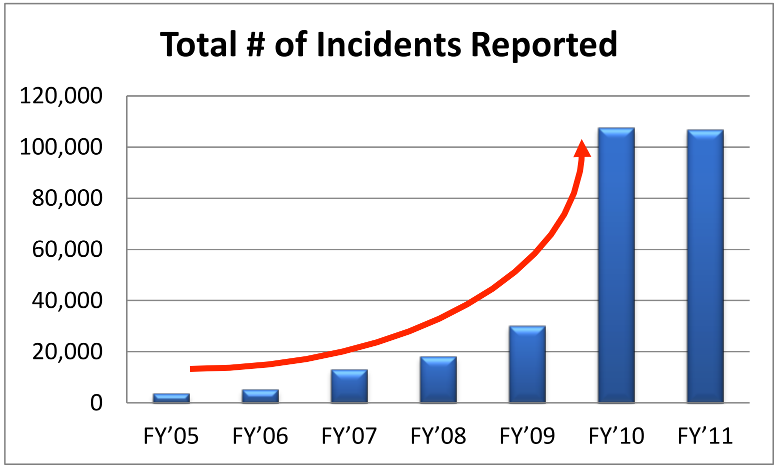
BY-NC-SA

The "Current State" of Cyber Defense Operating Model

- Cyber adversary attacks and cyber defense operation reacts...



- Not very effective...*

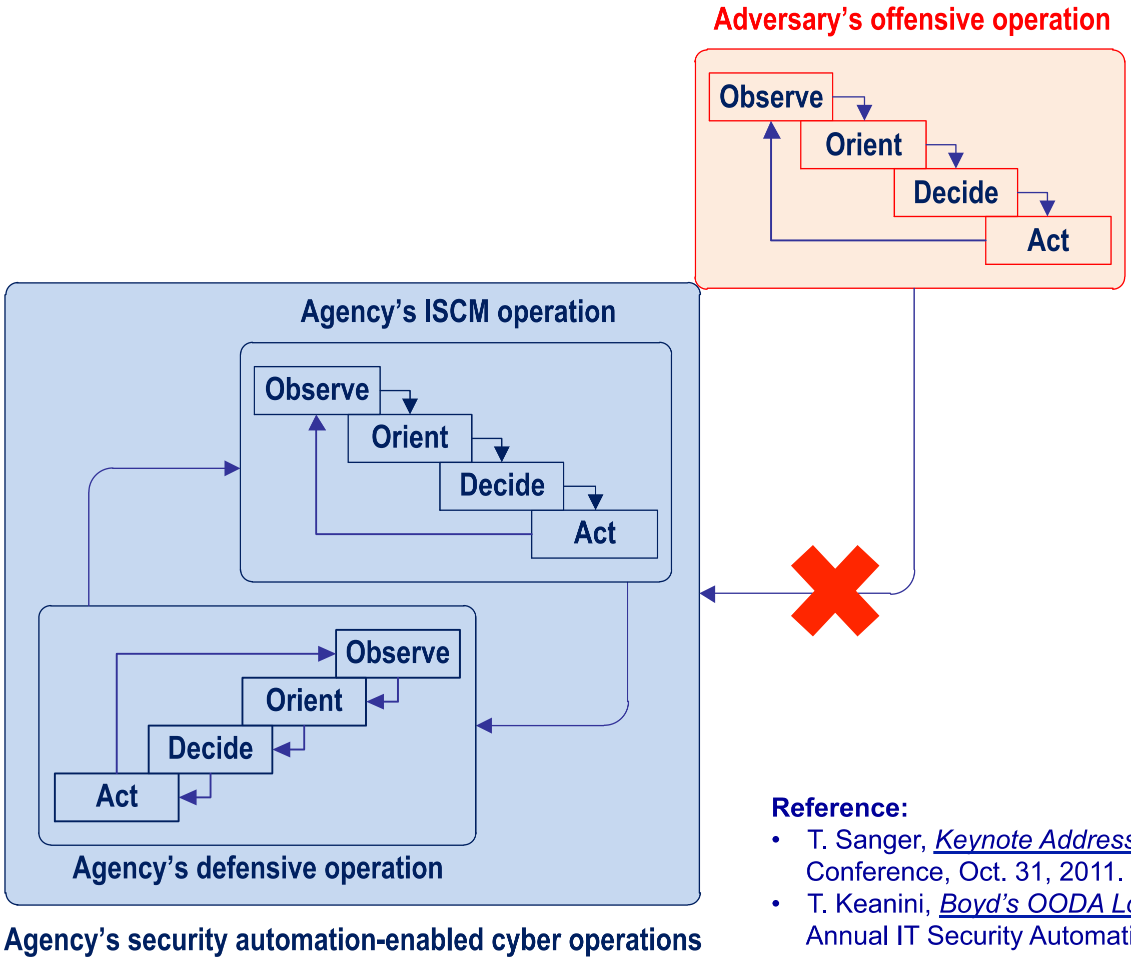


Reference:
* US-CERT.

(cc) BY-NC-SA

The "Future State" of Cyber Defense Operating Model – Information Security Continuous Monitoring (ISCM)

- Knowing and fixing problems before our adversaries discover them – proactive...


Adversary's offensive operation
Observe
Orient
Decide
Act
Agency's ISCM operation
Observe
Orient
Decide
Act
Observe
Orient
Decide
Act
Agency's defensive operation
Agency's security automation-enabled cyber operations

Reference:

- T. Sanger, *Keynote Address*, 7th Annual IT Security Automation Conference, Oct. 31, 2011.
- T. Keanini, *Boyd's OODA Loop and Continuous Monitoring*, 7th Annual IT Security Automation Conference, Oct. 31, 2011.

BY-NC-SA

Questions:

- When should risk assessment be performed in a typical system life cycle?
  –

- What are the three actions, a designated approving authority may take to address risk?
  –
  –
  –

(cc) BY-NC-SA

Answers:

- When should risk assessment be performed in a typical system life cycle?
  - Risk management is a life cycle activity. Risk assessment should be performed periodically throughout the system life cycle
- What are the three actions, a designated approving authority may take to address risk?
  - Accept Risk
  - Mitigate Risk
  - Transfer Risk

(cc) BY-NC-SA

Questions:

- In qualitative risk assessment method, what are the two variables for determining risks?
  -

- In quantitative risk assessment method, what are the variables that determines the annual lost expectance (ALE)?
  -
  - Hint: What is the term used to describe the monetary lost for each occurrence of a threatened event?
  - Hint: What is the term used to describe the frequency which a threat is expected to occur on an annualized basis?

(cc) BY-NC-SA

Answers:

- In qualitative risk assessment method, what are the two variables for determining risks?
  - Likelihood and Impact.

- In quantitative risk assessment method, what are the variables that determines the annual lost expectance (ALE)?
  - ALE = SLE X ARO.
  - Hint: What is the term used to describe the monetary lost for each occurrence of a threatened event?
  - Hint: What is the term used to describe the frequency which a threat is expected to occur on an annualized basis?

(cc) BY-NC-SA

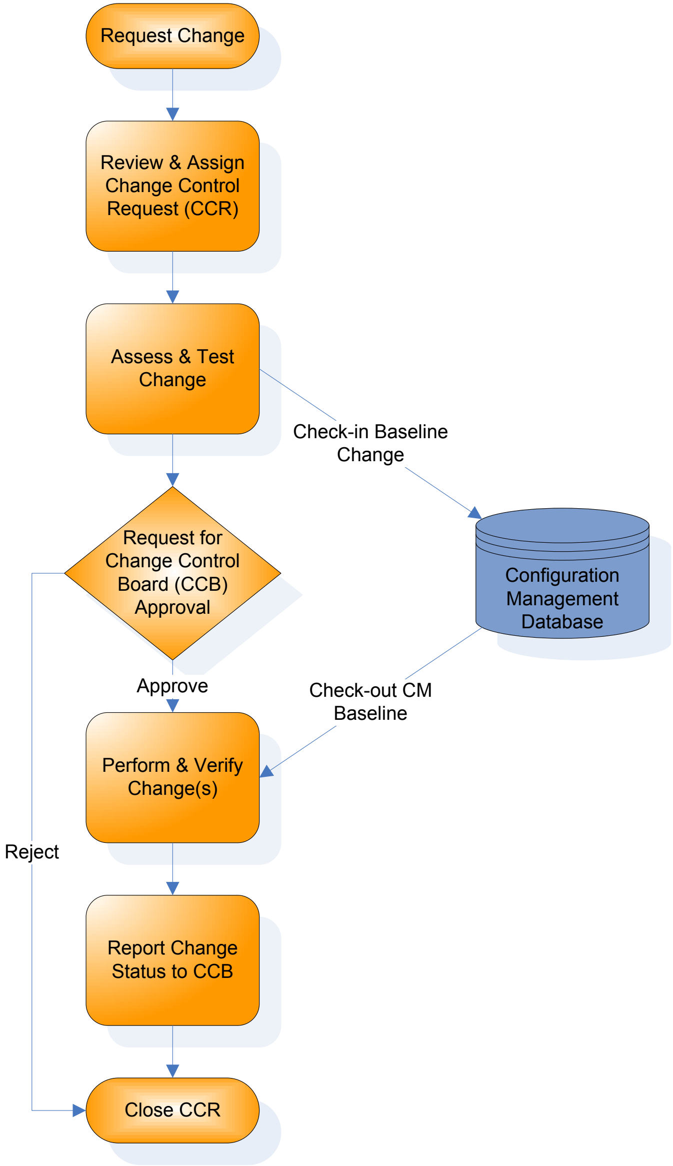
Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- ➡ Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Change Control & Configuration Management

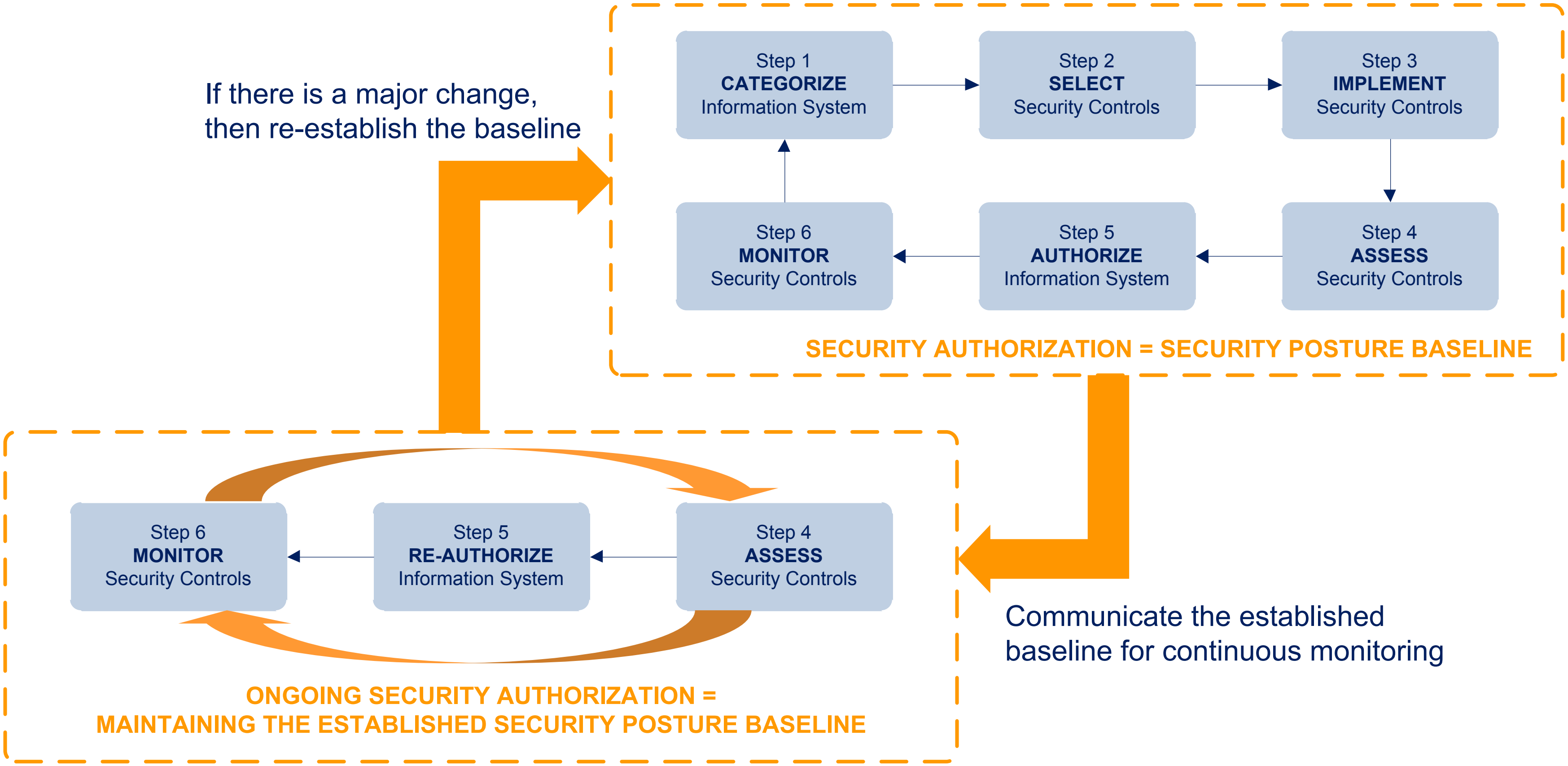

Request Change
Review & Assign Change Control Request (CCR)
Assess & Test Change
Check-in Baseline Change
Configuration Management Database
Request for Change Control Board (CCB) Approval
Approve
Check-out CM Baseline
Perform & Verify Change(s)
Reject
Report Change Status to CCB
Close CCR

- Change control (or Change Management) is a organizational business process.
- Configuration Management (CM) is a organizational practice that manages and maintains records of system baseline, configuration changes, and supports the change control process.

Note: Example of change control process according to ITIL

(cc) BY-NC-SA

Configuration Management and Security Posture Baseline



If there is a major change, then re-establish the baseline

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

SECURITY AUTHORIZATION = SECURITY POSTURE BASELINE

Step 4
ASSESS
Security Controls

Step 5
RE-AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

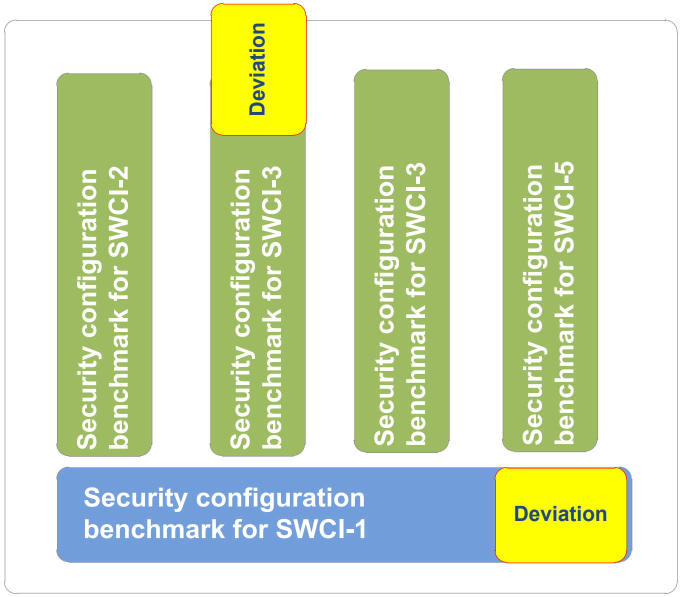
ONGOING SECURITY AUTHORIZATION =
MAINTAINING THE ESTABLISHED SECURITY POSTURE BASELINE

Communicate the established baseline for continuous monitoring

(cc) BY-NC-SA

Configuration Management and Information Security

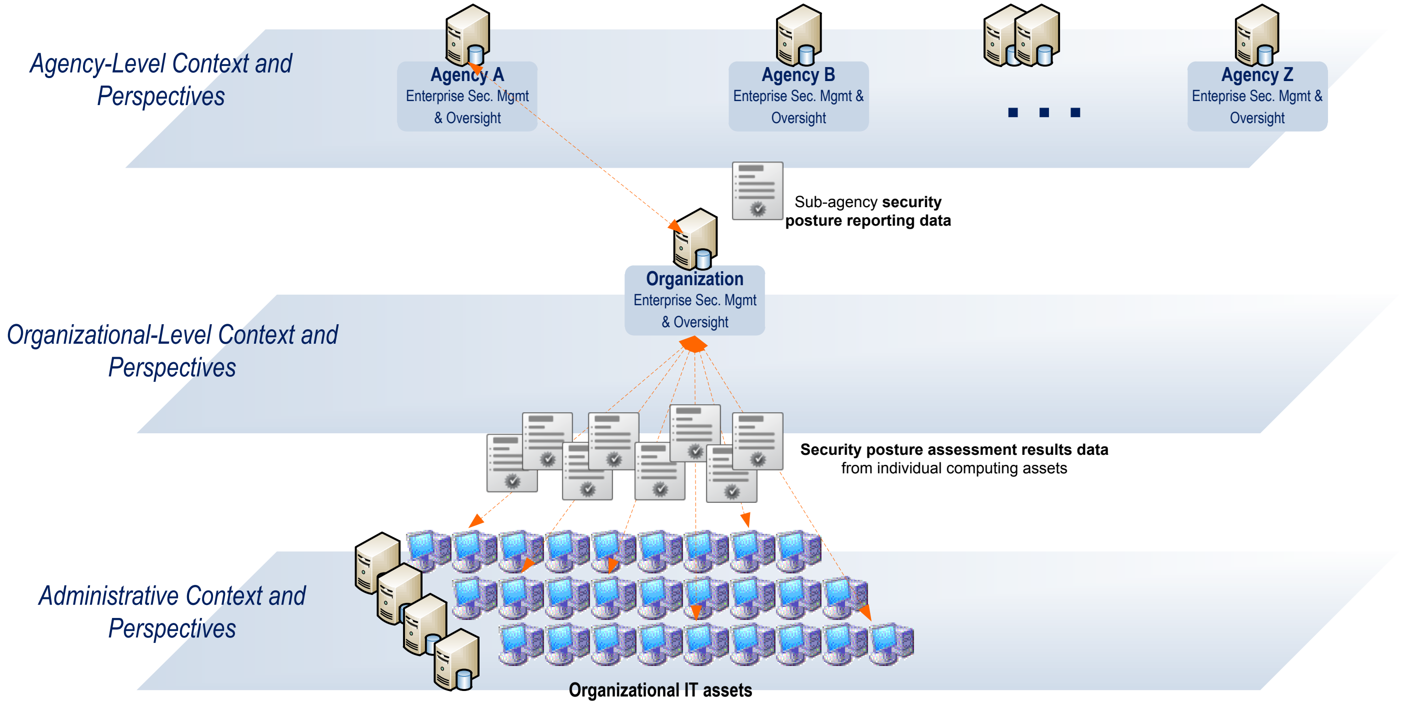
- We know that 80-90% of known vulnerabilities can be attributed to misconfigurations and missing patches, so …
  - Asset inventory data (to know what agencies have?)
  - Configuration (to know how are they configured?)


Security configuration benchmark for SWCI-2
Deviation
Security configuration benchmark for SWCI-3
Security configuration benchmark for SWCI-3
Security configuration benchmark for SWCI-5
Security configuration benchmark for SWCI-1
Deviation

An IT asset

(cc) BY-NC-SA

Configuration Management and Information Security


Agency-Level Context and Perspectives
Agency A
Enterprise Sec. Mgmt & Oversight
Agency B
Entepprise Sec. Mgmt & Oversight
. . .
Agency Z
Entepprise Sec. Mgmt & Oversight
Sub-agency security posture reporting data
Organization
Enterprise Sec. Mgmt & Oversight
Organizational-Level Context and Perspectives
Security posture assessment results data from individual computing assets
Administrative Context and Perspectives
Organizational IT assets

- The effort started with Federal Desktop Core Configuration (FDCC, OMB M-07-18)
- Provided implementation guidance on FDCC (OMB M-08-22)
- Attempted using FISMA to drive change (OMB M-09-29, M-10-15 to CyberScope, then M-11-33)

(cc) BY-NC-SA

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- ➡ Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Personnel Security Best Practice

- Hiring…
  - Personnel security interviews.
  - Background investigation.
  - Adjudication.
  - Non-disclosure agreement.
- Operating…
  - Separation of duties.
  - Rotation of jobs.
  - Security awareness briefing.
- Exiting…
  - Debriefing / exit interview.
  - Inventory & close accounts.
  - Escort.

Soap box:

- Personnel security is critical to information security.
- DIA reported 80% of security incidents are originated from internal threat agents.
  - Navy, the Walkers.
  - FBI, the Hanssen.
- Security Awareness
  - Protect against social engineering, dumpster diving, transmission of virus.
  - Kevin Mitnick

References:

- E.O. 13467, *Reforming Process to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008.
- DCID 6/4, *Personnel Security Standards and Procedure Governing Eligibility for Access to Sensitive Compartmented Information*
- DoD 5200.2-R, *Personnel Security Program*

(cc) BY-NC-SA

Insider Threats... (1/2)

- Employees, former employees, and business partners may be the biggest information security threat to an enterprise...

Source of Incidents*	2007	2008
Unknown	**N/A**	42%
Employees	**48%**	**34%**
Hackers	41%	28%
Former employees	**21%**	**16%**
Business partners	**19%**	**15%**
Customer	9%	8%
Other	20%	8%
Terrorist/ foreign government	6%	4%

References:

* *The Global State of Information Security 2008*, CSO Online (http://www.csoonline.com/article/print/454939)

(cc) BY-NC-SA

Insider Threats... (2/2)

- Software Engineering Institute (SEI) CERT Program's insider threat studies also found that…
  - 68% of the insider attack occurred at the workplace
  - 73% of crimes were committed during working hours
  - Over three-quarters of the insider had authorized access to information assets
  - None of the insider had privileged access (i.e. system/ database administrator.)
  - 20% involved in theft of physical properties (e.g., document, laptops, PC, etc.)

References: *Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model, CERT Program*, Software Engineering Institute and CyLab at Carnegie Mellon University, June 2009.

(cc) BY-NC-SA

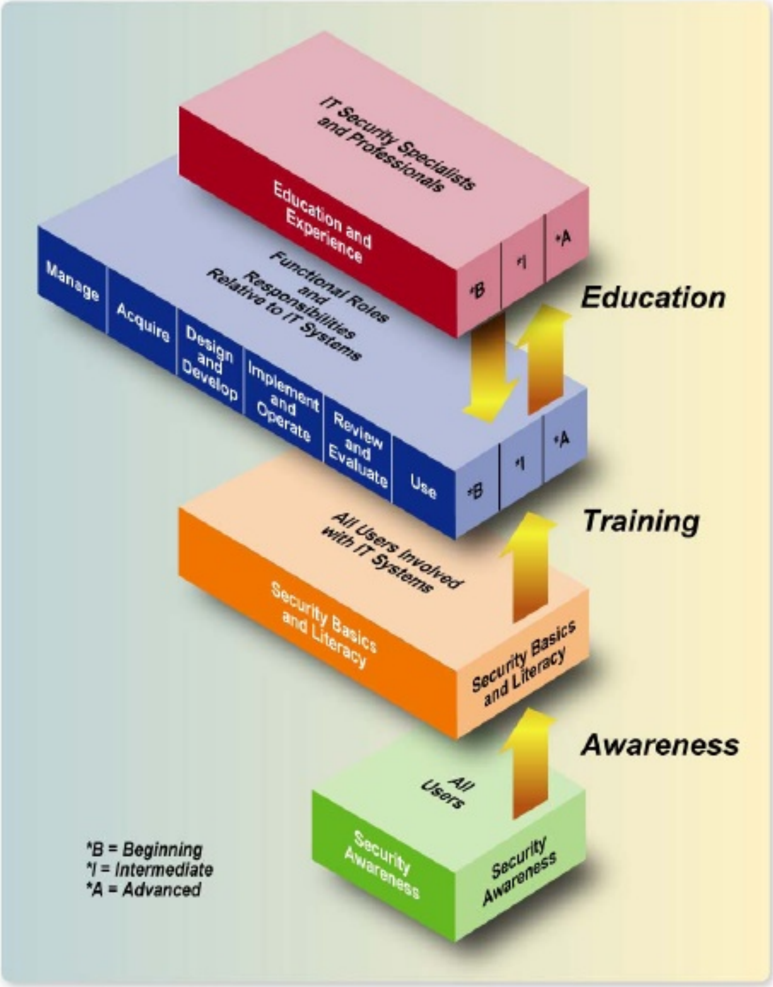
Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Security Education, Training and Awareness (SETA)

- Awareness
  - Orientation briefs and materials to inform and remind employees of their security responsibilities and management's expectation.
- Training
  - Course and materials to provide employees the necessary skills to perform their job functions.
- Education
  - Course and materials to provide employees the necessary decision-making and management skills to improve their promotional ability and mobility.

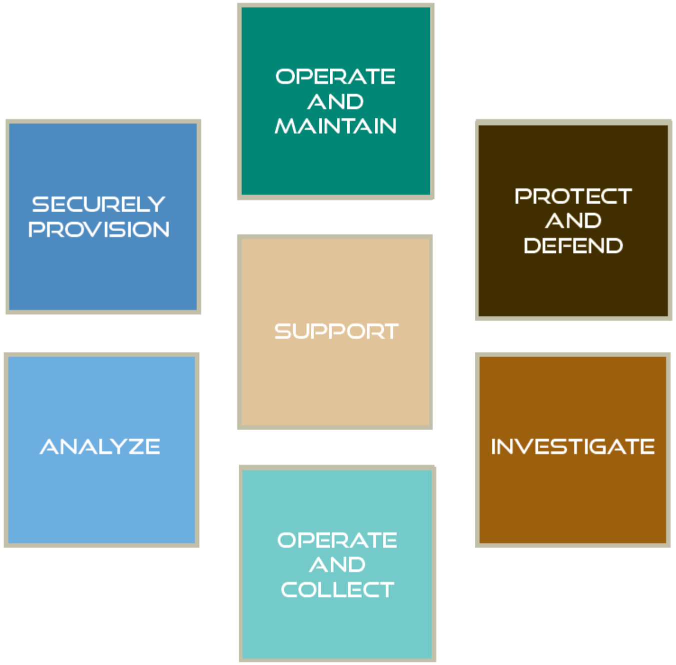


Reference: NIST SP800-50, *Building an IT Security Awareness and Training Program*.

(cc) BY-NC-SA

National Initiative for Cybersecurity Education (NICE) (1/2)

- NICE is a part of Comprehensive National Cybersecurity Initiative (CNCI) where government and industry collaborated to create a training & educational framework for cybersecurity workforce.

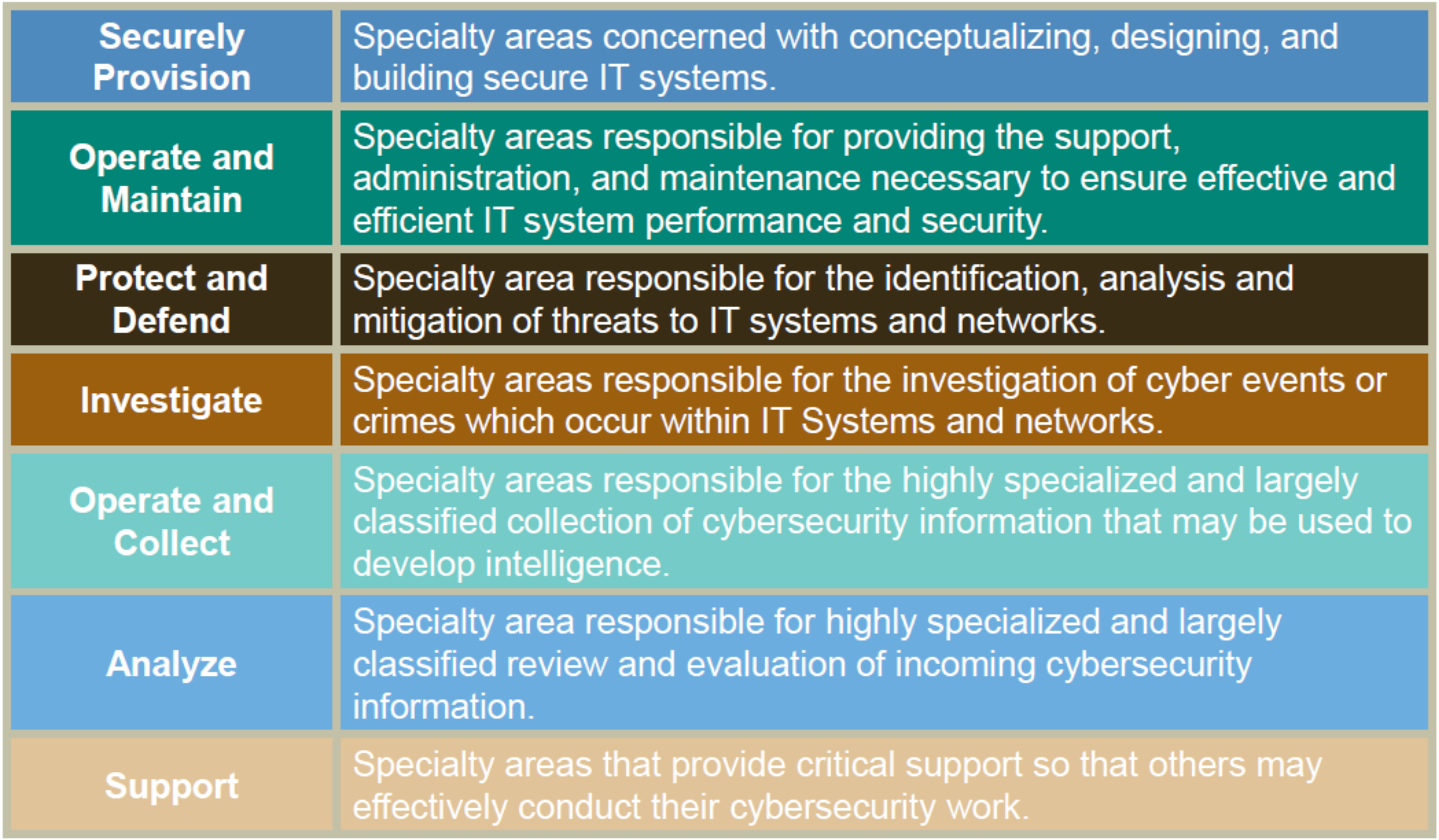


CYBERSECURITY WORKFORCE FRAMEWORK

(cc) BY-NC-SA

Reference: http://csrc.nist.gov/nice/

National Initiative for Cybersecurity Education (NICE) (2/2)



Securely Provision	Specialty areas concerned with conceptualizing, designing, and building secure IT systems.
Operate and Maintain	Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
Protect and Defend	Specialty area responsible for the identification, analysis and mitigation of threats to IT systems and networks.
Investigate	Specialty areas responsible for the investigation of cyber events or crimes which occur within IT Systems and networks.
Operate and Collect	Specialty areas responsible for the highly specialized and largely classified collection of cybersecurity information that may be used to develop intelligence.
Analyze	Specialty area responsible for highly specialized and largely classified review and evaluation of incoming cybersecurity information.
Support	Specialty areas that provide critical support so that others may effectively conduct their cybersecurity work.

(cc) BY-NC-SA

Reference: http://csrc.nist.gov/nice/

Learning Objectives

Information Security Management Domain

- Information Security Concepts
- Information Security Management
- Information Security Governance
- Information Classification
- System Life Cycle (SLC) and System Development Life Cycle (SDLC)
- Risk Management
- Certification & Accreditation
- Security Assessment
- Configuration Management
- Personnel Security
- Security Education, Training, and Awareness
- Project Management

(cc) BY-NC-SA

Terms & Definitions… 1/2

- Project: A planned undertaking to accomplish a specific business goal/objectives.
- Program: A collection of integrated, networked projects to accomplish a set of business/mission goals/objectives.
- Integrated Master Plan (IMP): An "event-based" plan consists of a hierarchical program events (/tasks) supported by specific accomplishments.
- Integrated Master Schedule (IMS): An integrated, networked schedule that contains the detailed discrete tasks or activities (defined in IMP).

(cc) BY-NC-SA

Terms & Definitions... 2/3

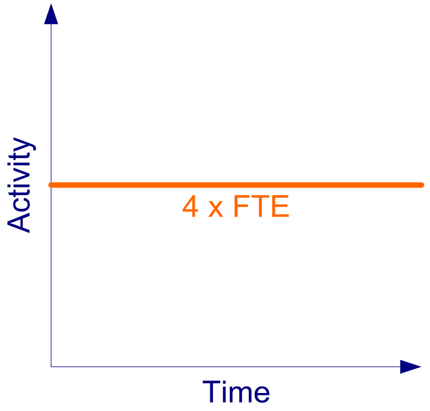
- Task (/ Activity): An element of work performed during the course of a project.
- Resources: Budget, people, time, material and tools, etc.

(cc) BY-NC-SA

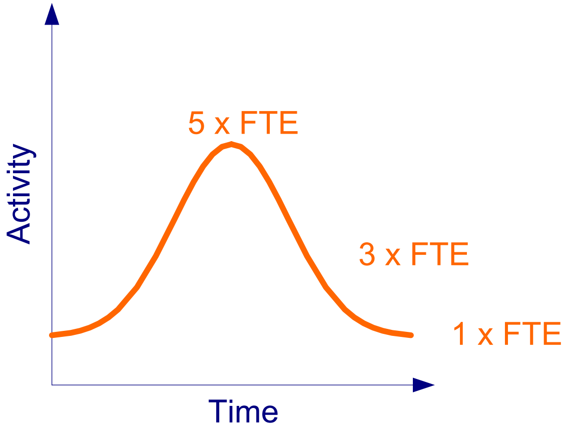
Terms & Definitions... 3/3

Types of Projects:

- Level-of-Effort (LOE): General / supportive activities typically measured through time (e.g. PM, CM, Operations, etc.)



- Discrete Effort (a.k.a. Activities-based Costing (ABC)): Purposeful activities related to completion of a specific product or service that can be measured in Cost/Schedule (e.g. development of a functional module, software code, etc.)



BY-NC-SA

Project Management Methodologies & Framework

- Project Management Methodologies
  - Critical Path Method (CPM).
  - Program Evaluation & Review Technique (PERT).
  - Earned-Value Management System (EVMS) / Earned-Value Technique (EVT).
- Project Management Framework
  - Project Management Institute’s (PMI) Project Management Body of Knowledge (ANSI/PMI 99-001-2004).

BY-NC-SA

“Scientific” Project Management Methodologies

- The concept of “Scientific Management” started by Frederick Winslow Taylor in 1911.

- Critical Path Method (CPM):
  - Started by DuPont Corporation as a scientific management method standard for managing projects/product production.

- Program Evaluation & Review Technique (PERT):
  - Started by USN in 1958, as a scientific management method for the Polaris Missile Program.
  - In 1958, USA also used PERT for their Minuteman Missile Program.

Reference:

- *The Principle of Scientific Management*, by Frederick Winslow Taylor, 1911.
- http://en.wikipedia.org/wiki/Critical_path_method
- http://en.wikipedia.org/wiki/PERT

(cc) BY-NC-SA

“Scientific” Project Management Methodologies

- Earned-Value Management System (EVMS):
  - A systematic integration and measurement of cost, schedule, and accomplishments of an investment that enables organizations to evaluate project performance during execution.
  - Incorporate CPM, PERT and EVT.
- The use of EVMS is required by the *Clinger-Cohen Act* of 1996.

Section 5113 Performance-based and Result-based Management.

(a) IN GENERAL – The Director shall encourage the use of performance-based and results-based management in fulfilling the responsibilities assigned under section 3504(h), of title 44, United States Code.

(b)(1) REQUIREMENT – The Director shall evaluate the information resources to the performance and results of the investment made by the executive agencies in information technology.

(cc) BY-NC-SA

Critical Paths Method (CPM)

- Critical Path Method (CPM) provides you insights to sequence of project tasks/activities.

Statement of Work (SOW)

+ Work Breakdown Structure (WBS)

+ Critical Path Method (CPM)

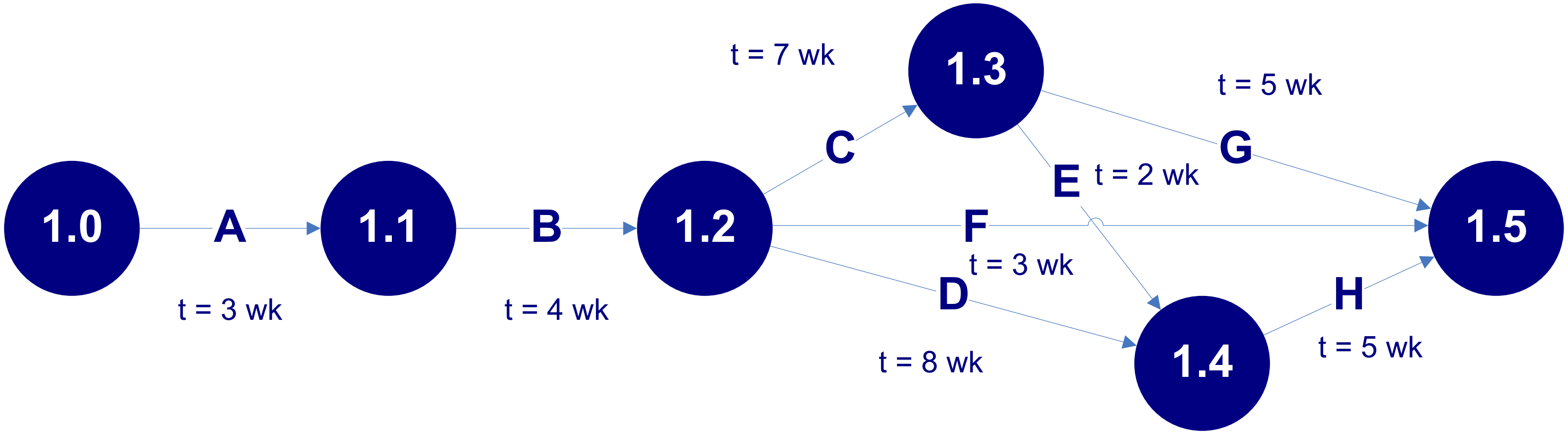
= Integrated Master Plan (IMP)

- However, CPM does not show you: Time, Entry/Exit Criteria and Resources required.

(cc) BY-NC-SA

Program Evaluation & Review Technique (PERT)

- PERT is CPM with “time vector.”
- Time vector contains: Start time and Finish time.
  - Earliest Start time (ES), Latest Start time (LS).
  - Earliest Finish time (EF), Latest Finish time (LF).



BY-NC-SA

Program Evaluation & Review Technique (PERT)

- PERT provides you insights to sequence of tasks/ activities in terms of schedule.

Work Breakdown Structure (WBS)

+ Program Evaluation & Review Technique (PERT)

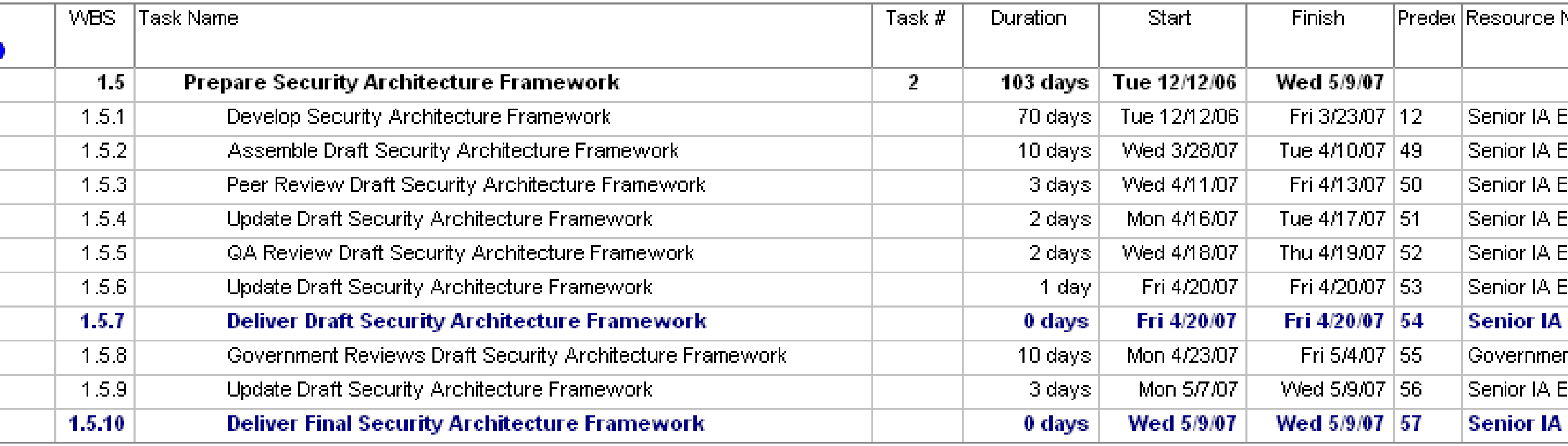
= Integrated Master Schedule (IMS)

- However, PERT does not show you: Entry/exit criteria and resources required.

(cc) BY-NC-SA

Program Evaluation & Review Technique (PERT)

- This is an actual example!



WBS	Task Name	Task #	Duration	Start	Finish	Predec	Resource N
1.5	**Prepare Security Architecture Framework**	**2**	**103 days**	**Tue 12/12/06**	**Wed 5/9/07**		
1.5.1	Develop Security Architecture Framework		70 days	Tue 12/12/06	Fri 3/23/07	12	Senior IA E
1.5.2	Assemble Draft Security Architecture Framework		10 days	Wed 3/28/07	Tue 4/10/07	49	Senior IA E
1.5.3	Peer Review Draft Security Architecture Framework		3 days	Wed 4/11/07	Fri 4/13/07	50	Senior IA E
1.5.4	Update Draft Security Architecture Framework		2 days	Mon 4/16/07	Tue 4/17/07	51	Senior IA E
1.5.5	QA Review Draft Security Architecture Framework		2 days	Wed 4/18/07	Thu 4/19/07	52	Senior IA E
1.5.6	Update Draft Security Architecture Framework		1 day	Fri 4/20/07	Fri 4/20/07	53	Senior IA E
1.5.7	**Deliver Draft Security Architecture Framework**		**0 days**	**Fri 4/20/07**	**Fri 4/20/07**	**54**	**Senior IA**
1.5.8	Government Reviews Draft Security Architecture Framework		10 days	Mon 4/23/07	Fri 5/4/07	55	Governmen
1.5.9	Update Draft Security Architecture Framework		3 days	Mon 5/7/07	Wed 5/9/07	56	Senior IA E
1.5.10	**Deliver Final Security Architecture Framework**		**0 days**	**Wed 5/9/07**	**Wed 5/9/07**	**57**	**Senior IA**

- What is wrong with this project?
- This PM has never build an system architecture.

(cc) BY-NC-SA

Some serious facts about the current state of federal IT projects

- Government Accountability Office (GAO) reported:
  - "… for fiscal year 2006, nearly 25% of the funds (IT budget) requested, totaling about $15 billion, were considered by OMB to be at risk."
  - "In the case of risk assessment, supporting documentation for about 75% of the investments did not address OMB's required risk categories."
- Government Computer News (GCN) reported a survey from 104 Federal IT executives:
  - Reasons for program over-run are…
    - 65+%: Poor program management.
    - 54%: Scope creep.
  - Key to reduce number of failed agency IT projects is…
    - Training.

Resource:

- GAO-06-250 *Information Technology: Agencies Need to Improve the Accuracy and Reliability of Investment Information*.
- http://www.gcn.com/online/vol1_no1/42733-1.html

(cc) BY-NC-SA

Earned-Value Management System (EVMS)

- DoD EVMS is based on ANSI/EIA-748-A-1998, *Earned Value Management Systems Standard.*

- Implementation of EVMS (i.e. DoD EVMIG) consists of 32 Guidelines in 5 Categories:
  - Organization.
  - Planning, Scheduling & Budgeting.
  - Accounting Considerations.
  - Analysis and Management Reports.
  - Revisions and Data Maintenance.

Reference:

- http://www.acq.osd.mil/pm/historical/ansi/ansi_announce.html
- http://www.ndia.org/Content/ContentGroups/Divisions1/Procurement/NDIA_PMSC_EVMS_IntentGuide_Jan2006U1.pdf

(cc) BY-NC-SA

Earned-Value Management System (EVMS)

- Key attributes in EVMS:
  - Statement of Work (SOW).
  - Work Breakdown Structure (WBS).
  - Entry Criteria (i.e. task dependencies, work authorization, etc.)
  - Exit Criteria (i.e. deliverables, PMR, closure, etc.)
  - Resources: Time, costs & budget.

(cc) BY-NC-SA

Earned-Value Management System (EVMS)

- Project performance value is “earned” through:
  - Work performed.
  - Product delivery (i.e. milestones).

- Project performance can be analyzed and projected using Earned-Value Technique (EVT) (a.k.a. Performance Measurement Analysis).

cc BY-NC-SA

EVMS – Earned-Value Technique (EVT)

- Earned Value (EV): Actual work performed.
- Planned Value (PV): Budgeted cost for work scheduled at a given time.
- Actual Cost (AC): Costs incurred in actual work performed.
- BCWP: Budgeted cost for work performed.
- BCWS: Budgeted cost for work scheduled.
- ACWP: Actual cost for work performed.

(cc) BY-NC-SA

Reference: PMI *Project Management Body of Knowledge* (ANSI/PMI 99-001-2004)

EVMS – Earned-Value Technique (EVT)

- Cost Variance: CV = BCWP – ACWP
- Schedule Variance: SV = BCWP – BCWS
- Cost Performance Index: CPI = BCWP ÷ ACWP
- Schedule Performance Index: SPI = BCWP ÷ BCWS

Reference: PMI *Project Management Body of Knowledge* (ANSI/PMI 99-001-2004)

(cc) BY-NC-SA

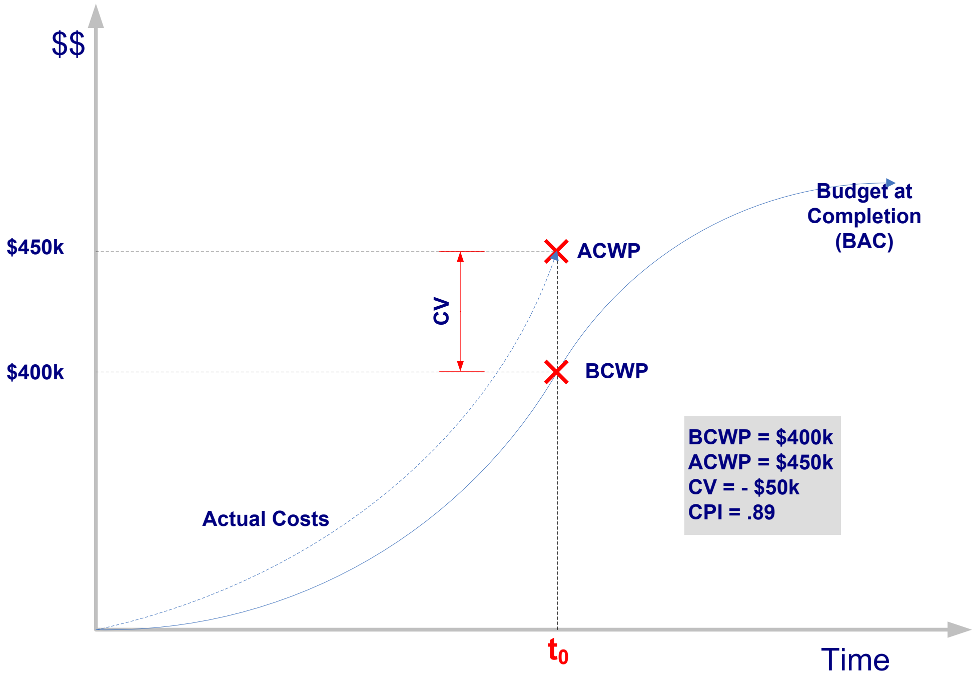
EVMS – Earned-Value Technique (EVT)

Calculating the Cost Variance…

   BCWP ($400k)

– ACWP ($450k)

= CV (-$50k)



BCWP = $400k
ACWP = $450k
CV = - $50k
CPI = .89

(cc) BY-NC-SA

Project Management

EVMS – Earned-Value Technique (EVT)

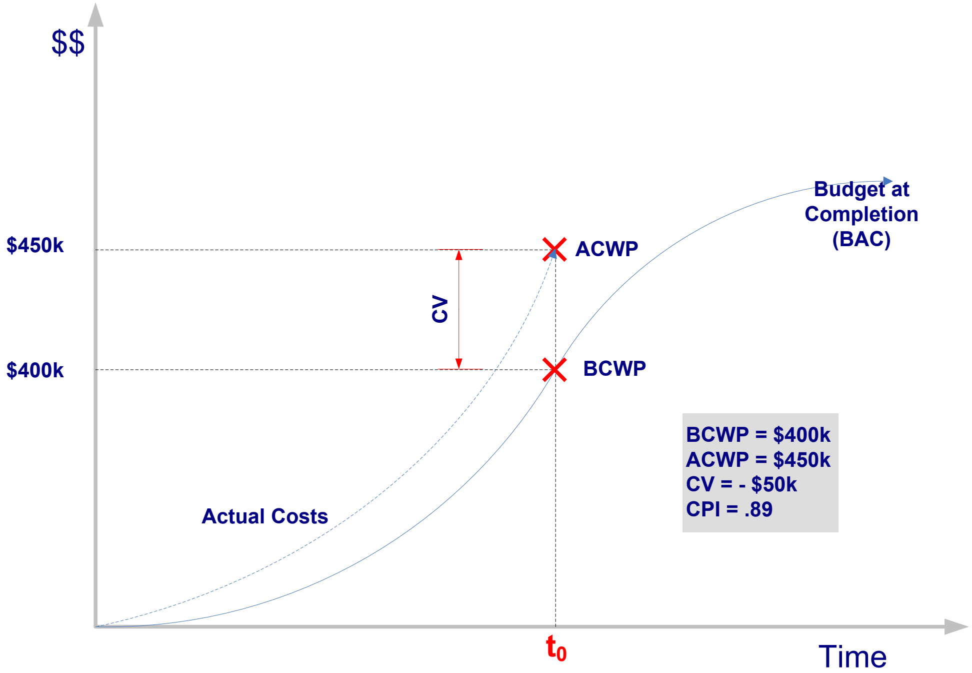
Calculating the Cost Performance Index (CPI)…

BCWP ($400k)

÷ ACWP ($450k)

= CPI (.89)

Question:
If CPI < 1 then how is this project doing?



BCWP = $400k
ACWP = $450k
CV = - $50k
CPI = .89

Answer:
Project is not as productive as planned.

(cc) BY-NC-SA

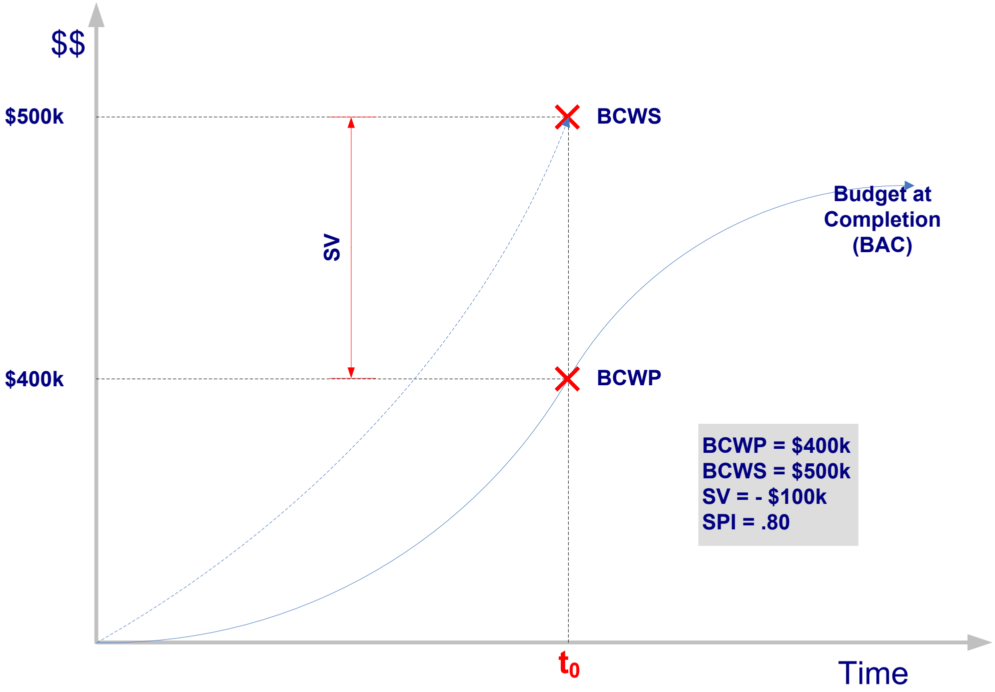
EVMS – Earned-Value Technique (EVT)

Calculating the Schedule Variance…

BCWP ($400k)

– BCWS ($500k)

= SV (- $100k)



(cc) BY-NC-SA

EVMS – Earned-Value Technique (EVT)

Calculating the Cost Performance Index (CPI)…

BCWP ($400k)

÷ BCWS ($500k)

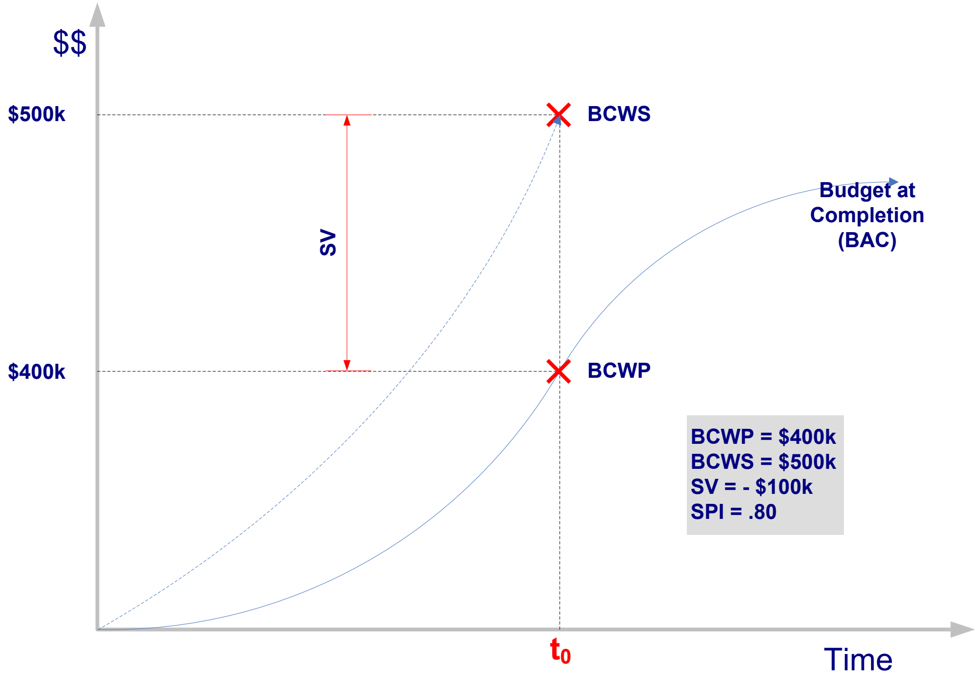
= SPI (.80)

Question:

If SPI < 1 then how is this project doing?

Answer:

It’s is behind schedule.

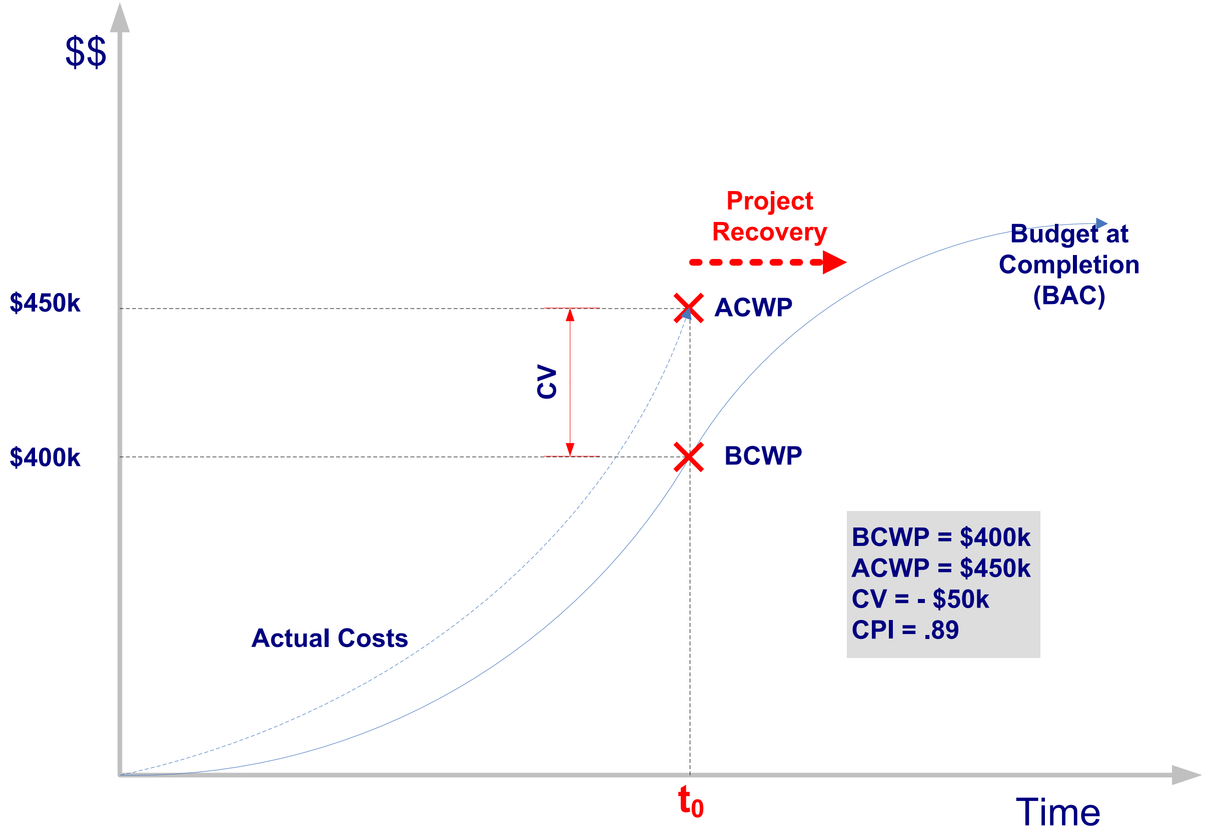


BCWP = $400k
BCWS = $500k
SV = - $100k
SPI = .80

BY-NC-SA

Project Recovery

So, project is not doing well… What do you do?

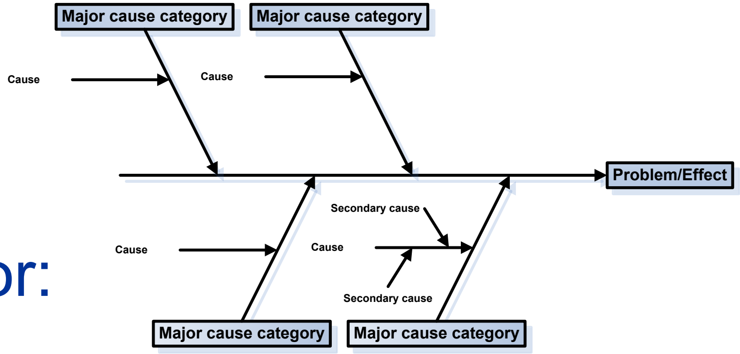


BCWP = $400k
ACWP = $450k
CV = - $50k
CPI = .89

(cc) BY-NC-SA

Project Recovery

- Use CPM to find task dependencies.
- Use PERT to locate effect(s) on schedule.
- Use Cause-Effect (Fishbone) to locate problem.



- Re-negotiate project goals or milestone (via change-order).
- Increase resources, but watch for:
  - Impact of resource re-allocation to other dependent tasks.
  - The “Mythical Man-Month” problem.
- De-scope tasks, but watch for:
  - Effects on quality & program dependencies.

(cc) BY-NC-SA

Validation Time… ☺

1. Classroom Exercise

2. Review Answers

(cc) BY-NC-SA

Exercise #1: Build Security In

- A civilian agency is planning an acquisition of an information system…
  - Please identify key security engineering tasks required.

BY-NC-SA

Exercise #2: Risk Management Process

- A civilian agency is planning an acquisition of an information system that will assess the security configuration settings of IT assets in a Secret-System High operating enclave.
  - Please identify the attributes required to enable you to determine the information protection needs.

- Google is planning to offer its Google Apps service to biotech research company.
  - What is the annual loss expectancy from a service outage?
    - Estimated asset value: $14.6B (total revenues in 2009)
    - Exposure factor: 0.01%
    - Google’s annual rate of service outage occurrence: 1.2%

(cc) BY-NC-SA