CISSP® Common Body of Knowledge Review:

Security Architecture & Design Domain

Version: 5.10

Security Architecture and Design Domain

The Security Architecture & Design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, network, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

Information security architecture and design covers the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that these practices and processes align with the organization's core goals and strategic direction.

The candidate is expected to understand security models in terms of confidentiality, integrity, data flow diagrams; Common Criteria (CC) protection profiles; technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

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

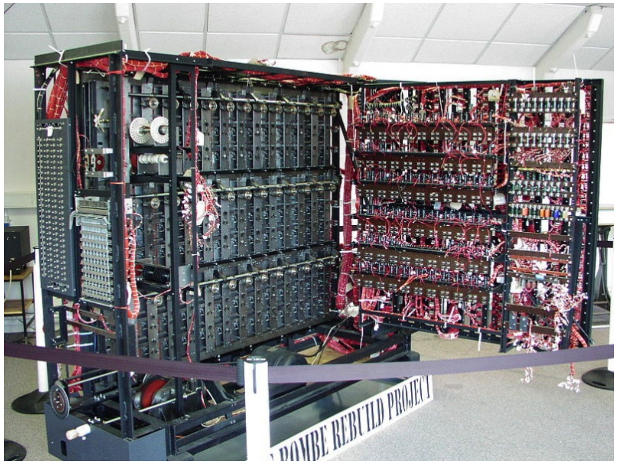
Security Architecture & Models Domain

- Computing Platforms
- Security Models
  - Information Security Models
- Evaluation & Certification
- Security Architecture
  - Modes of Operation
  - Architecture Concepts
  - Implementation Models

Electro-mechanical Computational Machines

- In 1930-1940s, Dr. Alan Turing invented concept of “Turing machine” that given us the electro-mechanical computational machines (e.g., ACE and Bombe.)
- Bombe was used by British cryptologists to decrypt German Nazi’s Enigma machine.

Enigma Cipher Machine

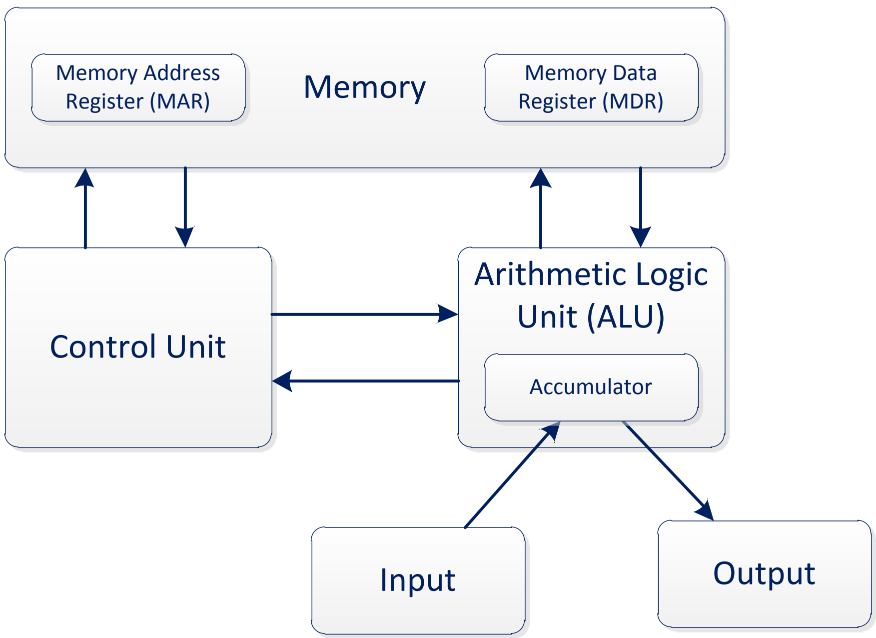


British Bombe machine in Bletchley Park

Reference: http://www.mathcomp.leeds.ac.uk/turing2012/

Von Neumann Model

- In 1950s, Dr. John von Neumann wrote *The Computer and the Brains* that described a system architecture for the modern micro-processor computing machine.



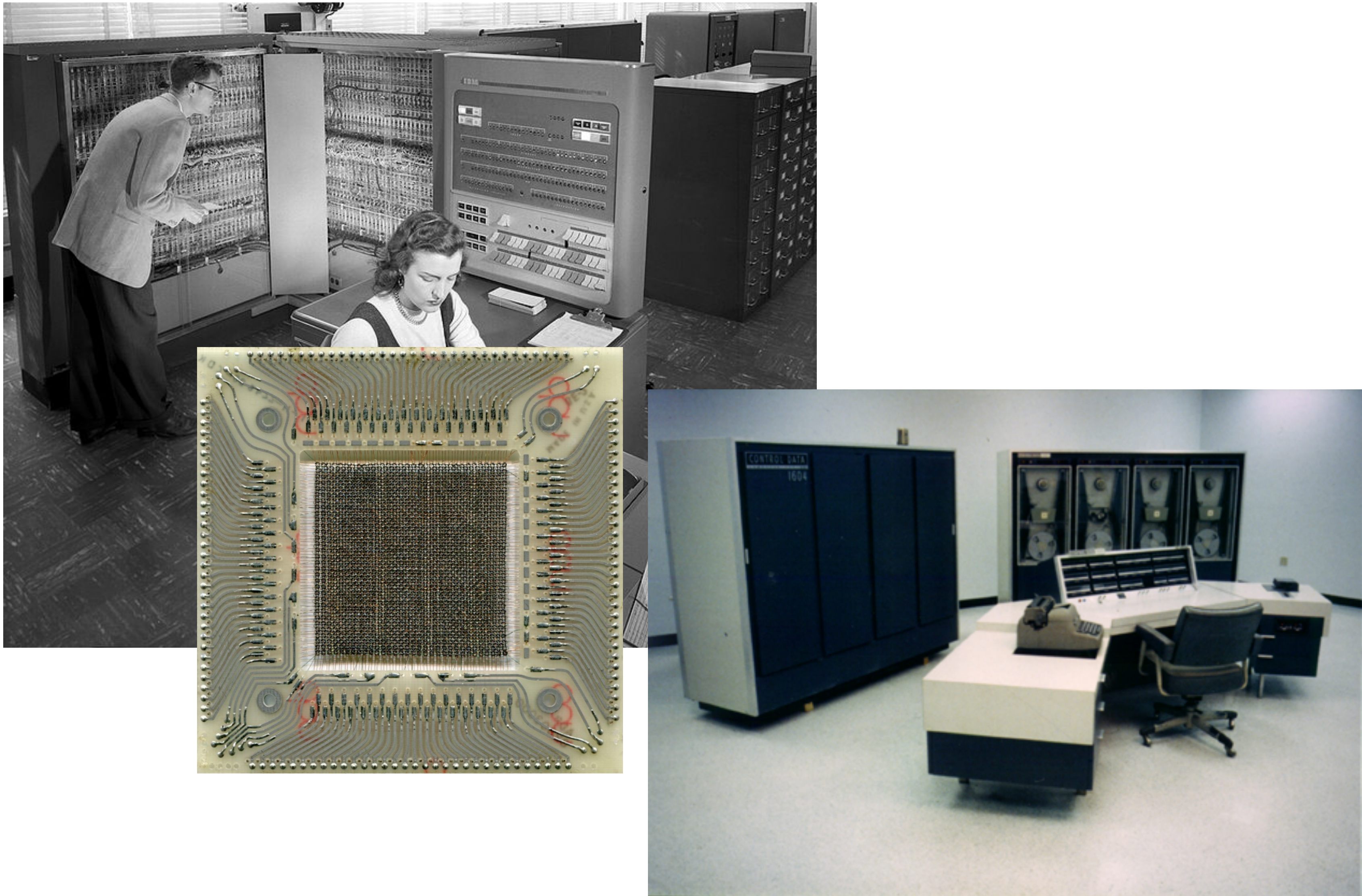
Reference:
- http://en.wikipedia.org/wiki/Von_Neumann_architecture
- Daybreak of the Digital Age (http://paw.princeton.edu/issues/2012/04/04/pages/5444/index.xml?page=3&)

MITRE's SAGE System

- Semi-Automatic Ground Environment (SAGE)

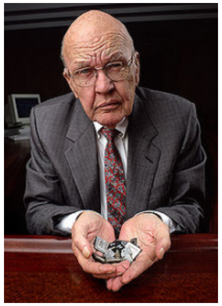
Reference: http://en.wikipedia.org/wiki/Semi-Automatic_Ground_Environment

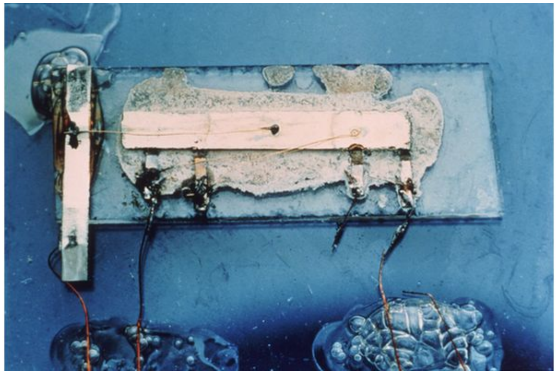
Transistorized Computers – IBM 7000 Series, CDC 1604



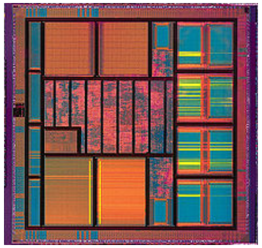
Integrated Circuit (IC) / Micro-processor

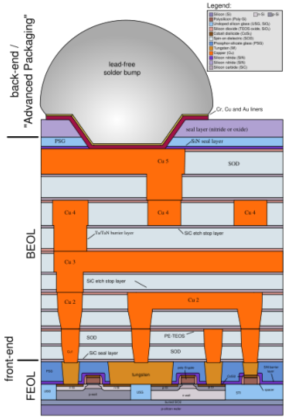
- In late 1950s, the integrated circuit (IC) invented by:
  - Jack Kilby of Texas Instruments, and
  - Robert Noyce of Fairchild Semiconductor

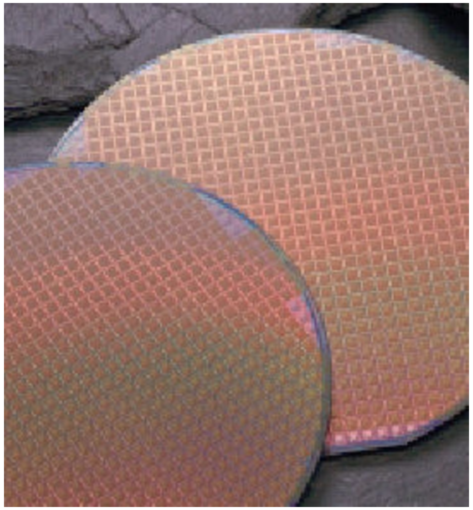




- Electro-mechanical computing machines → Micro-processor computing machines







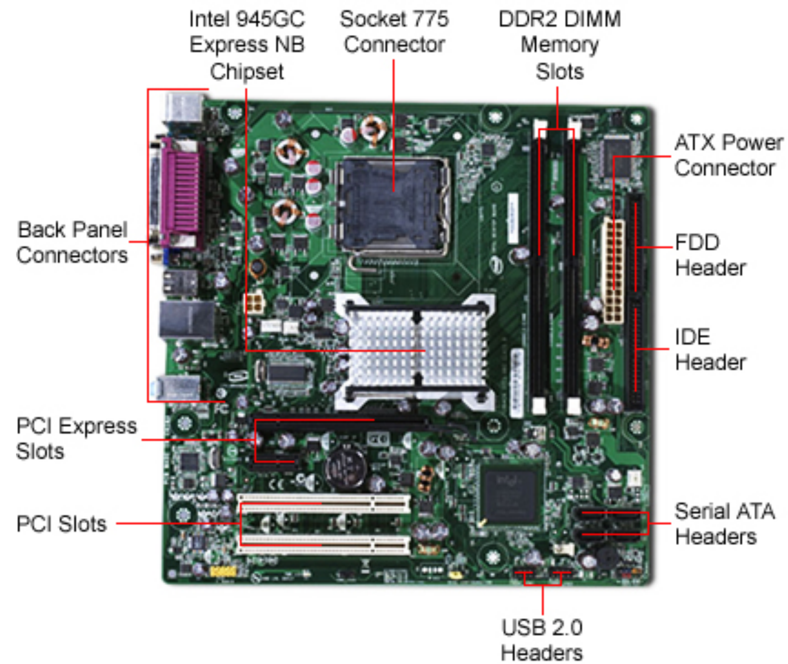
Reference: *Google image search.*

Integrated Circuit (IC)/Large Scale Integration (LSI) Computers – IBM System/360 and PDP-11

Reference:
- IBM Archives: System/360 Model 50 (http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_PP2050.html)
- PDP-11 (http://en.wikipedia.org/wiki/PDP-11)

Hardware Components

- Central Processing Unit (CPU)
  - Registers (General-purpose, Dedicated)
  - Arithmetic Logical Unit (ALU)
- Memory
  - Primary + Secondary Cache
  - Read Only Memory (ROM)
  - Random Access Memory (RAM)
  - Flash Memory
  - Virtual Memory (via Storage)
- Input/Output (I/O) Devices
  - System Bus & Channels
  - Serial, Parallel, USB, SCSI, PCMCIA, etc.
  - Network Interface Card (NIC)
- Storage
  - Disk, Tape, Flash (USB Jump Drive + PCMCIA)

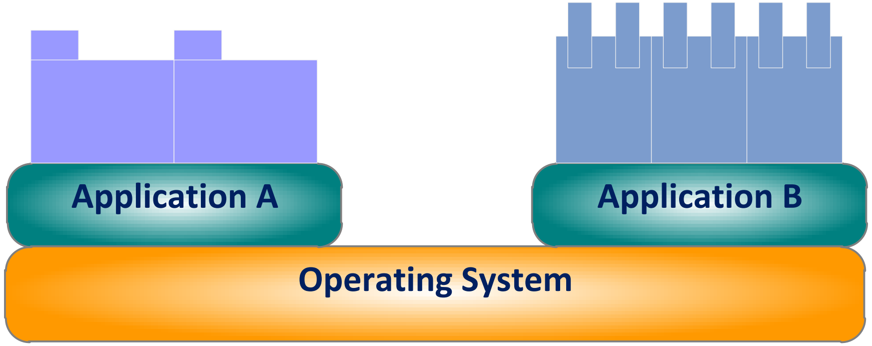


Hardware Components

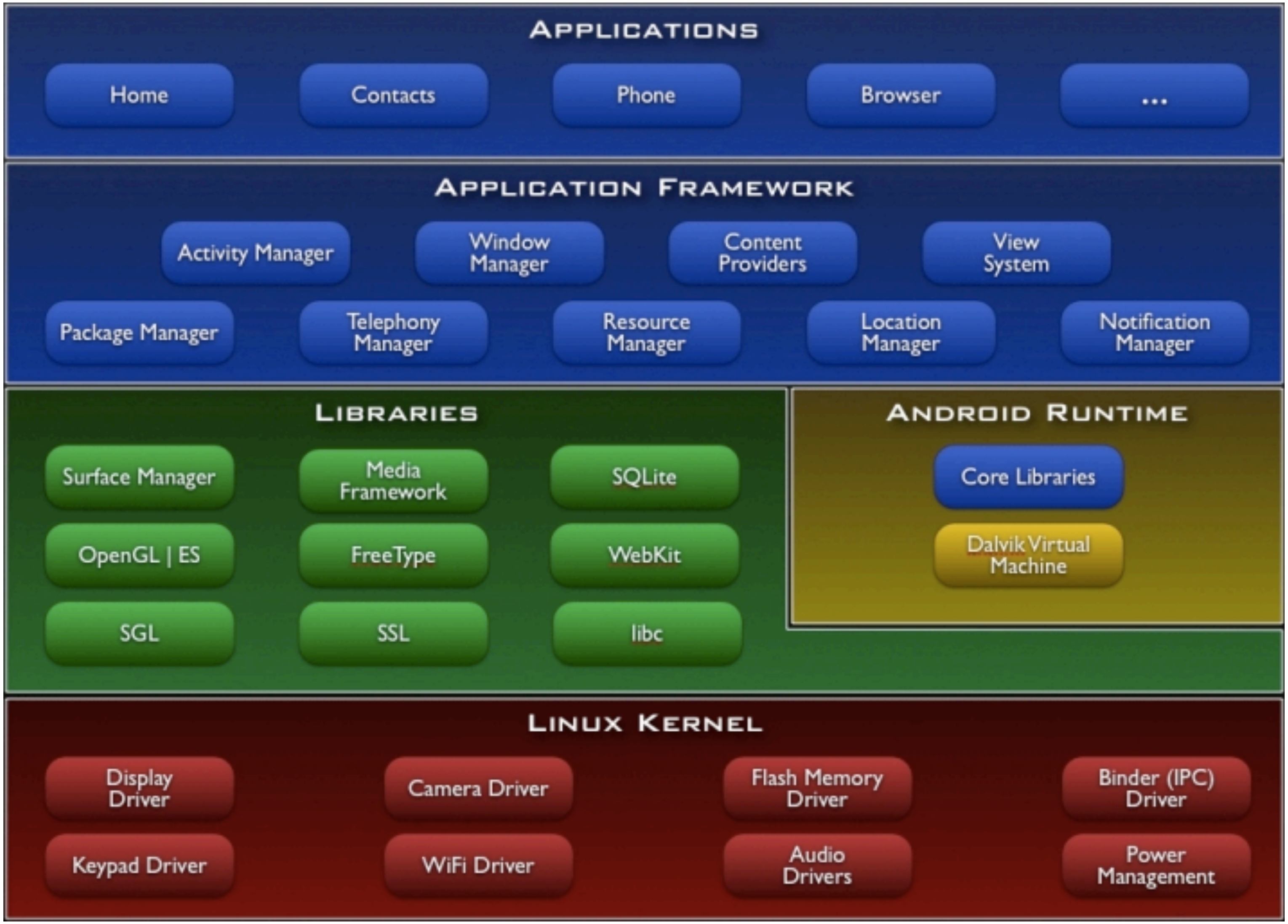
Source:
- AppleInsider (http://appleinsider.com/articles/10/10/30/review_apples_new_11_6_inch_and_13_3_inch_macbook_air_late_2010/page/3)

Software Components

- Operating System (OS)
- Firmware (stored in ROM/EPROM/EEPROM)
  - BIOS
  - Device Firmware
- Input/Output (I/O) Controllers
  - Device Drivers
- System Programs & Applications
  - File Management Systems
  - Network Management
  - Process Management
- Mobile Code
  - Java Virtual Machine (JVM)
  - Active X
  - Application Macro
- Data / Memory Addressing
  - Register, Direct, Absolute, Indexed, Implied.
  - Memory Protection



Software Components

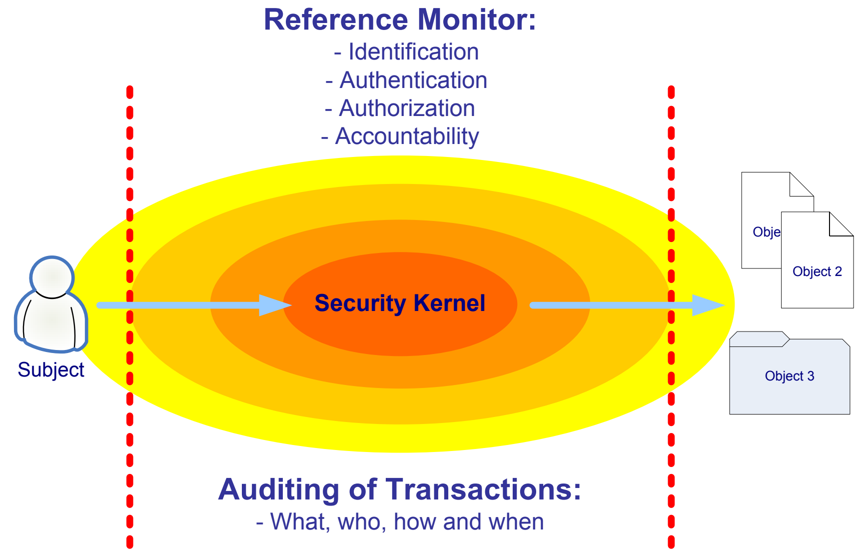


Source:

- Android Architecture (http://elinux.org/Android_Architecture)

Operating System (OS)

- User identification and authentication.
- Discretionary access control (DAC).
- Mandatory access control (MAC).
- Mediate transactions.
- Object reuse protection.
  - Prevent leakage.
- Accountability.
  - Audit security events.
  - Protection of audit logs.
- Trusted path.
  - Protection of critical operations.
- Intrusion detection.
  - Patterns, analysis, and recognition.

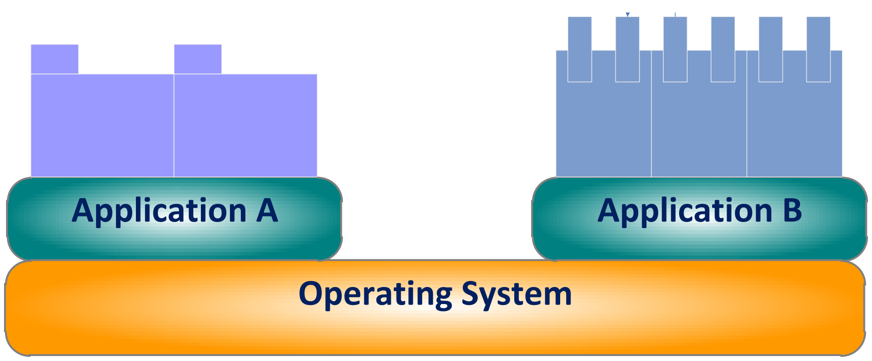


OS Process Scheduling

- Multi-programming
  - Managing and coordinating the process operations to multiple sets of programmed instructions e.g. VMS (Mainframe)
- Multi-tasking
  - Allows user to run multiple programs (tasks) e.g. Windows 2000, LINUX
- Multi-threading
  - Managing the process operations by work/execution threads (a series of tasks) using the same programmed instructions. Which allows multiple users and service requests e.g. Mach Kernel (BSD UNIX: Solaris, MacOS X, etc.)
- Multi-processing
  - Managing and coordinating the process operations to multiple sets of programmed instructions and multiple user requests using multiple CPUs e.g. Windows 2000, LINUX, UNIX

CPU Processing Threads

- Most of today's programs are comprised of many individual modules, programs or processes that are separately written and work together to fulfill the overall objective of the application
- These may be called modules or processing threads
- The security problems lie in the fact that these independent sections may be written by someone else then they may link dynamically and not be controlled by the Operating System (OS)



Operating Modes and Processing States

- Modes of operation
  - Kernel mode (privileged)
    - Program can access entire system
    - Both privileged and non-privileged instructions
  - User mode (non-privileged)
    - Only non-privileged instruction executed
    - Intended for application programs

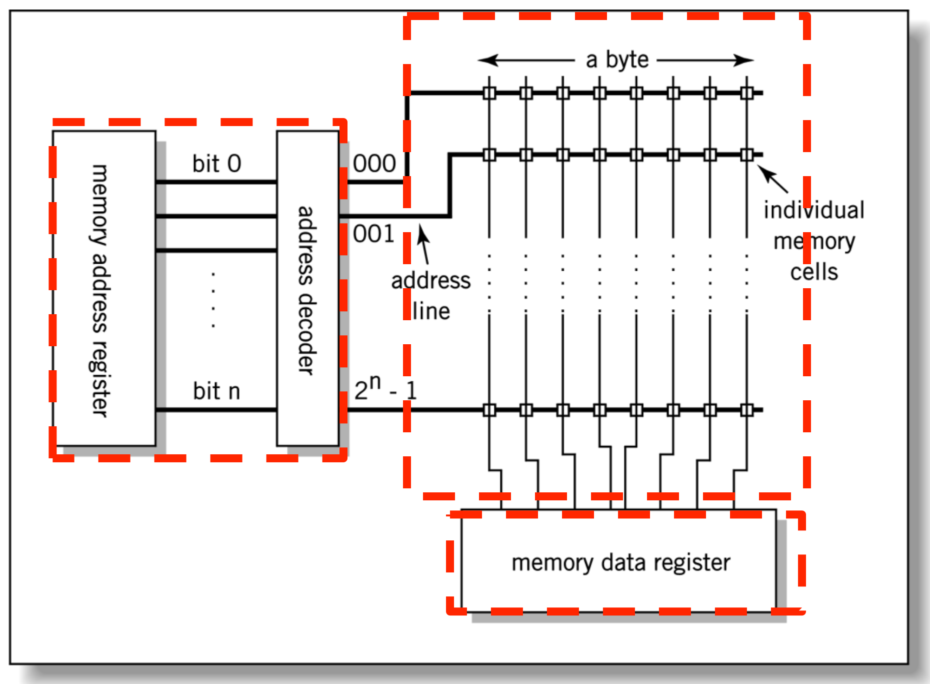
- Processing states
  - Stopped vs. Run state
  - Wait vs. Sleep state
  - Masked/interruptible state
    - E.g. if masked bit not set, interrupts are disabled (masked off) – known as IRQs in systems.

Memory Management – Functional Requirements

- There are five functional requirements for memory management:
  1. Physical Organization (Physical)
     - Provide management of data in physical memory space (e.g., CPU registers, cache, main memory (RAM), disk storage (secondary storage))
  2. Logical Organization (Logical)
     - Provide management of data in logical segments (virtual memory)
  3. Relocation (Relative)
     - Provide pointers to the actual location in memory
  4. Protection
     - Provide access control to protect integrity of memory segments
  5. Sharing
     - Allowing access to memory segment

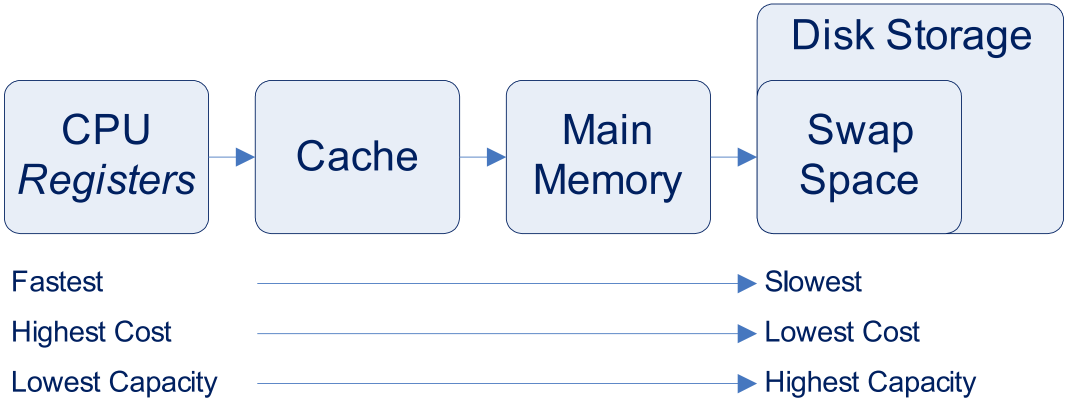
Memory Management – Type of memory addressing

- Three types of memory addresses:
  - Physical – the absolute address or actual location
  - Logical – reference to a memory location that is independent of the current assignment of data to memory. (Requires a translation to the physical address.)
  - Relative – address expressed as a location relative to a known point



Memory Management – Storage

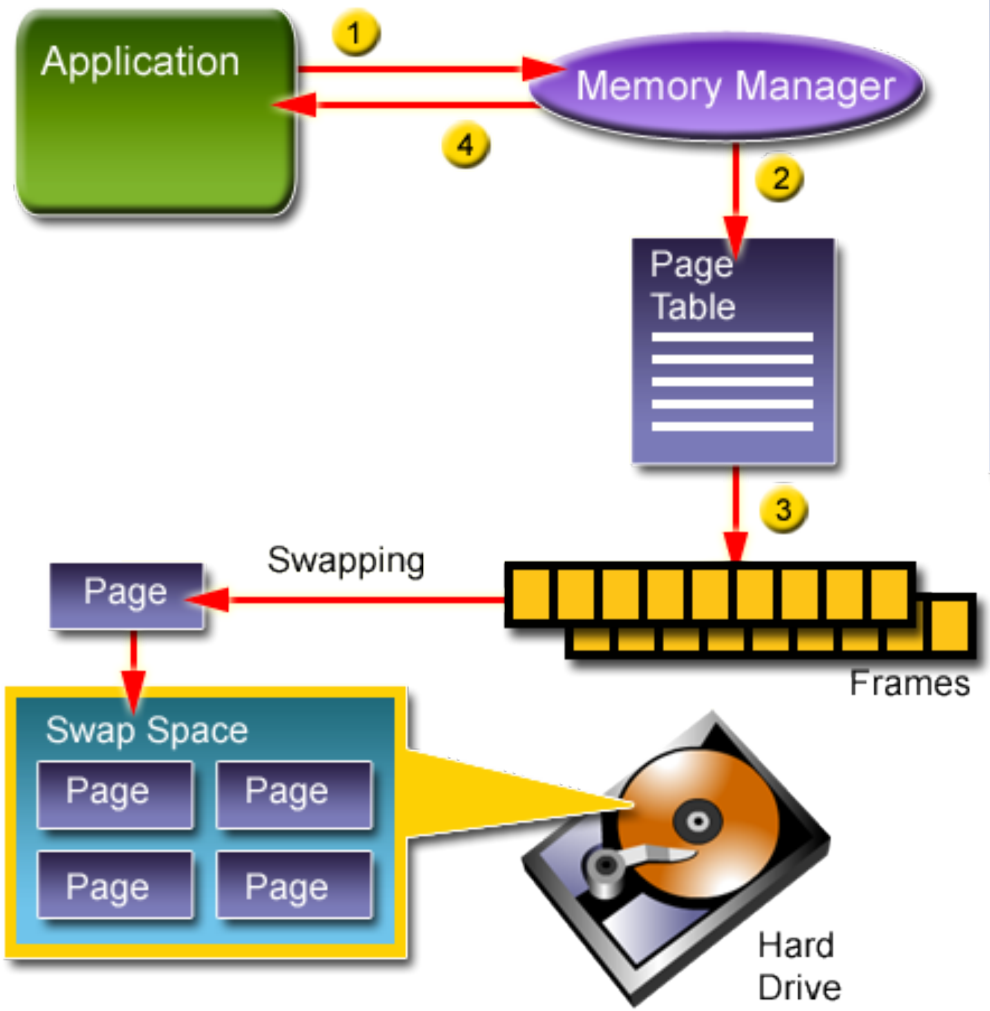
- Types of memory:
  - Real (A program or application defined storage location in memory and direct access to peripheral devices e.g. Comm. buffer)
  - Virtual (Extended primary memory to secondary storage medium)
- Types of storage:
  - Primary (Memory direct accessible to CPU e.g. Cache and RAM)
  - Secondary (Non-volatile storage medium e.g. Disk Drives)



Memory Management – Paging & Swapping

- Virtual Memory is a memory management technique that extends memory by using secondary storage for program pages not being executed.
- Paging involves:
  - Splitting memory into equal sized small chunks that are called page frames.
  - Splitting programs (processes) into equal sized small chunks are called pages.
  - OS maintains a list of free frames
  - Pages are fixed blocks of memory usually 4K or 8K bytes
  - A page-fault is when a program accesses a page that is not mapped in physical memory.
- Swapping is the act of transferring pages between physical memory and the swap space on a disk.

Memory Management: Paging & Swapping



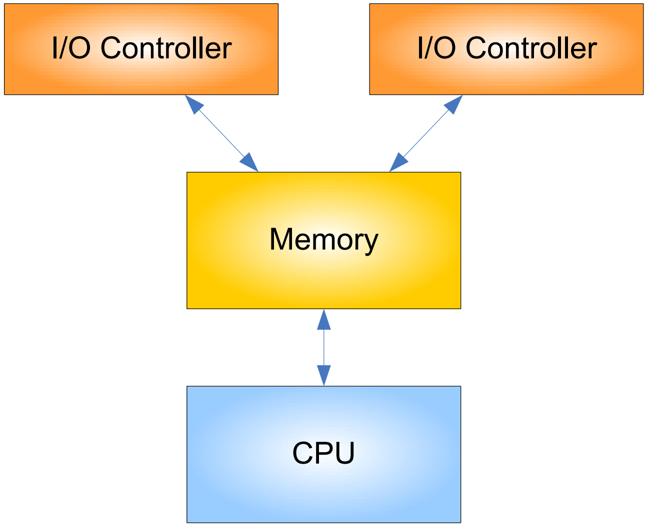
Main Memory

1. Application requests to access memory
2. Manager looks up which segments are allocated to that process
3. Access memory frame for process
4. Returns data held in memory

Reference: ISSA-Alamo CISSP Training Course.

Input/Output Devices

- The I/O controller is responsible for moving data in and out of memory.
- An element of managing the I/O devices and thus managing memory is through swapping or paging files.



Input/Output Devices – Storage

- Storage devices for secondary memory:
  - Hard disk drives

  - Write-Once Read Memory (WORM) (Storage medium such as CD-ROM, DVD-ROM)

  - USB flash drives

  - SD, Micro-SD memory cards

  - PCMCIA memory cards

  - Floppy disk drives

Security Architecture & Models Domain

- Computing Platforms
- Security Models
  - Information Security Models
- Evaluation & Certification
- Security Architecture
  - Modes of Operation
  - Architecture Concepts
  - Implementation Models

Information Security Models

- Security model specifies the operational and functional behavior of a “system” for security.
- There are many security models:
  - Graham-Denning Model – formal system of protection rules.
  - Information-Flow Model – demonstrates the data flows, communications channels, and security controls.
  - State-Machine Model – abstract math model where state variable represent the system state. The transition functions define system moves between states.
  - Non-Interference Model – a subset of information-flow model that prevents subjects operating in one domain from affecting each other in violation of security policy. (i.e. Compartmentalized.)
- Others are combination of above and generalized access control models.

Terms and Definition … (1/2)

- A subject requests service
  - A subject can be user, program, process, device, etc.
- An object provides the requested service
  - An object can be file, database, program, process, devices, etc.

- A security model specifies the rules of behavior for a “system” (/ system of systems) in meeting the security objectives, where:
  - Security objective: confidentiality, integrity
  - Implementation rules: least-privilege, separation-of-duties

Terms and Definition ... (2/2)

- Access is the flow of information between a subject and an object(s).
- Access capability is what a subject can do to an object(s).
- Access control governs the information flow.
  – Discretionary access control (DAC) is where the information owner determines the access capabilities of a subject to what object(s).
  – Mandatory access control (MAC) is where the access capabilities are pre-determined by the security classification of a subject and the sensitivity of an object(s).

Graham-Denning Security Model

Graham-Denning is an information access model operates on a set of subjects, objects, rights.

- Levels of Protection
  1. No sharing at all
  2. Sharing copies of programs/ data files
  3. Sharing originals of programs/ data files
  4. Sharing programming systems/ subsystems
  5. Permitting the cooperation of mutually suspicious subsystems, e.g., debugging/ proprietary subsystems
  6. Providing memory-less subsystems
  7. Providing “certified” subsystems

- Operations
  - How to securely create an object/ subject.
  - How to securely delete an object/ subject.
  - How to securely provide the read access right.
  - How to securely provide the grant access right.
  - How to securely provide the delete access right.
  - How to securely provide the transfer access right.

References: G.S.Graham and P.J. Denning, *Protection – Principles and Practice*, AFIPS Conf. Proc., 1972.

Harrison-Ruzzo-Ullman (HRU) Security Model

- Access capability matrix specifying types of access
  - Subject-object
  - One row per subject. One column per object
  - It is a version of Graham-Denning

		Objects									
		S_1	S_2	S_3	S_4	S_5	O_1	O_2	O_3	O_4	O_5
Subjects	S_1	Cntrl	---	---			rwx	rw-	---	---	---
	S_2	---	Cntrl	---			---	---	--x	---	---
	S_3	---	---	Cntrl	r-x		---	---	---	---	---
	S_4	---	---	---	Cntrl		---	r-x	---	---	r-x
	S_5	---	---	---		Cntrl	---	r-x	---	---	---

References: M. Harrison, W. Ruzzo, and J.D. Ullman, *Protection in Operating Systems*, Communications of the ACM, August 1976

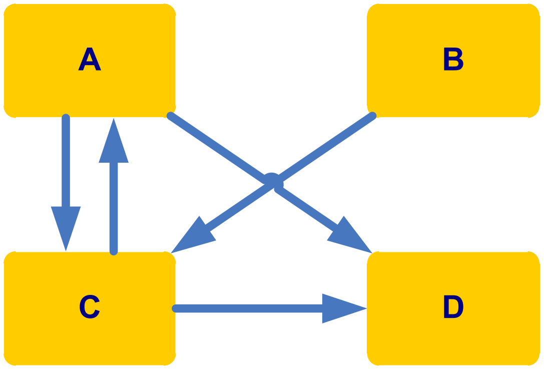
Information Flow Model

Information flow model illustrates the direction of data flow between objects

- Based on object security levels
- Information flow is constrained in accordance with object's security attributes
- Covert channel analysis is simplified

Note: Covert channel is moving of information to and from unauthorized transport

	A	B	C	D
A	N/A		X	X
B		N/A	X	
C	X		N/A	X
D				N/A



Bell-LaPadula Security Model ...(1/3)

Bell-LaPadula is a state-machine model for information flow and access control.

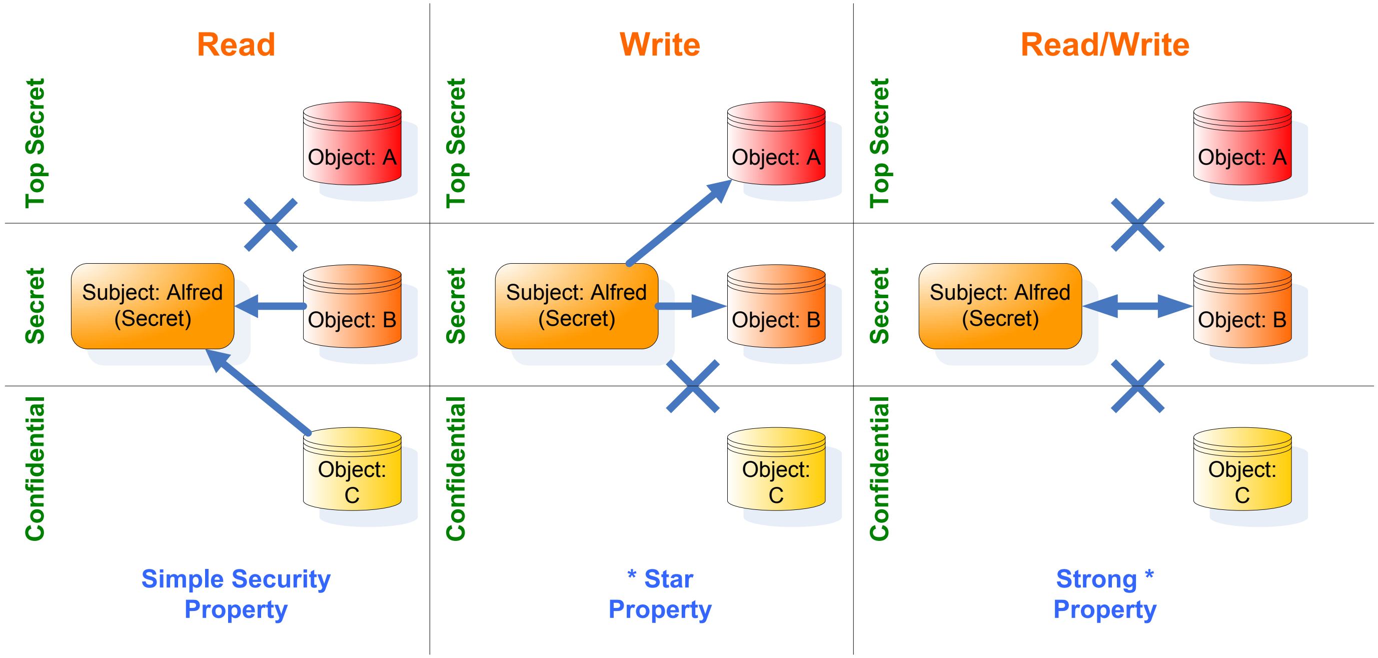
- Confidentiality only!
- Secure state-access is only permitted in accordance with specific security policy
- Secure state is when rules are security-preserving
- Fundamental modes of access:
  - Read only, Write only, or Read & Write.
- Discretionary Security: Specific subject authorized for particular capability of access.

Reference: D. Bell, L. LaPadula , MTR-2997, *Secure Computer System: Unified Exposition and Multics Interpretation*, March 1976.

Bell-LaPadula Security Model …(2/3)

Bell-LaPadula confidentiality policy:

- Simple security property
  - Subject cannot read object of higher sensitivity.
- Star property (* property)
  - Subject cannot write to object of lower sensitivity.
- Strong Star property (Strong * property)
  - Subject cannot read/write to object of higher/lower sensitivity.



Bell-LaPadula Security Model …(3/3)

Bell-LaPadula security model has two major limitations:

- Confidentiality only
- No method for management of classifications
  - It assumes all data are assigned with a classification
  - It assumes the data classification will never change
- Hence the need for…
  - E.O. 13526 (updates E.O. 13292, E.O. 12958), *Classified National Security Information*, Dec. 29, 2009
  - E.O. 13467(updates E.O. 12968), *Reforming Process Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified Information*, July 2, 2008
  - DoD 5200.01-M, *Information Security Program*, Vol. 1-4, March 2012

Reference: *Secrets & Lies – Digital Security in a Networked World*, Bruce Schneier, 2004

Biba Security Model ...(1/2)

Biba Security Model is a state-machine model for information flow and integrity control

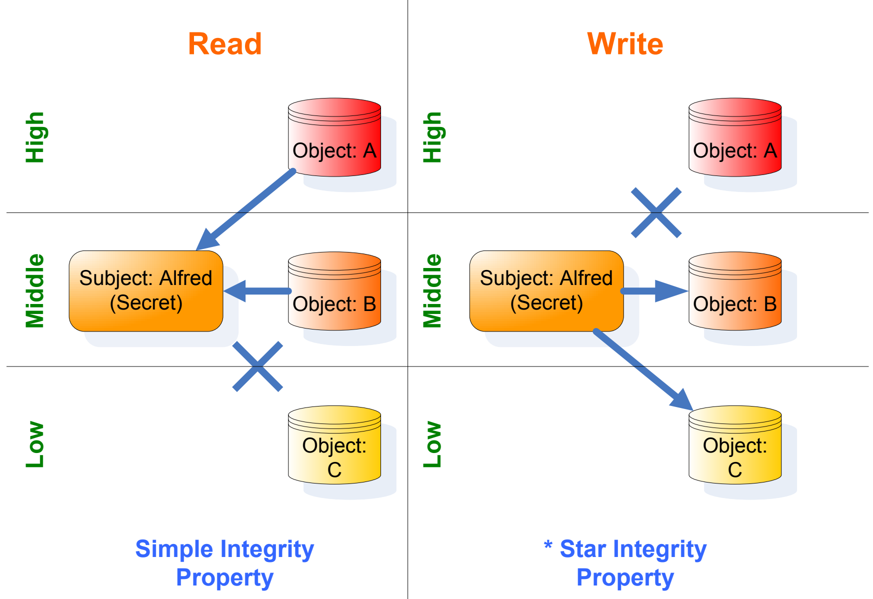
- Addresses integrity in information systems.
- Based on hierarchical lattice of integrity levels
- Elements
  - Set of subjects (Active, information processing)
  - Set of objects (Passive, information repository)
- Integrity: Prevent unauthorized subjects from modifying objects.
- Mathematical dual of access control policy
  - Access Tuple: subject & object.

Reference: K. Biba, MTR-3153, *Integrity Consideration for Secure Computing System*, 1975

Biba Security Model …(2/2)

Biba security policy:

- Simple integrity condition
  - Subject cannot read objects of lesser integrity.
- Integrity star * property
  - Subject cannot write to objects of higher integrity.
- Invocation property
  - Subject cannot send messages (logical request for service) to object of higher integrity.

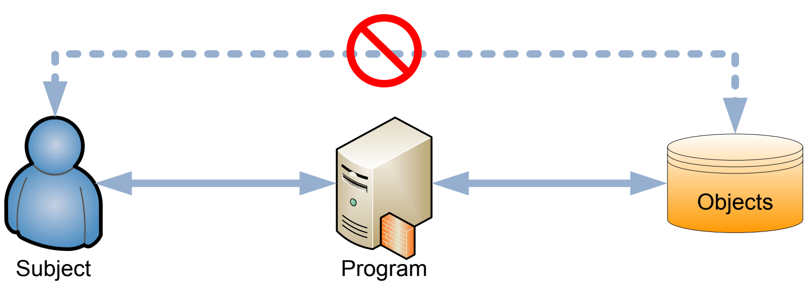


Clark-Wilson Security Model ...(1/3)

Clark-Wilson is a state-machine security model addresses information flow and the integrity goals of:

- Preventing unauthorized subjects from modifying objects
- Preventing authorized subjects from making improper modification of objects
- Maintaining internal and external consistency

- Well-formed transaction
  - Preserve/ensure internal consistency
  - Subject can manipulate objects (i.e. data) only in ways that ensure internal consistency.
- Access Triple: Subject-Program-Object
  - Subject-to-Program and Program-to-Object.
  - Separation-of-Duties



Reference: D. Clark, D. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, IEEE Symposium on Security and Privacy, 1987

Clark-Wilson Security Model …(2/3)

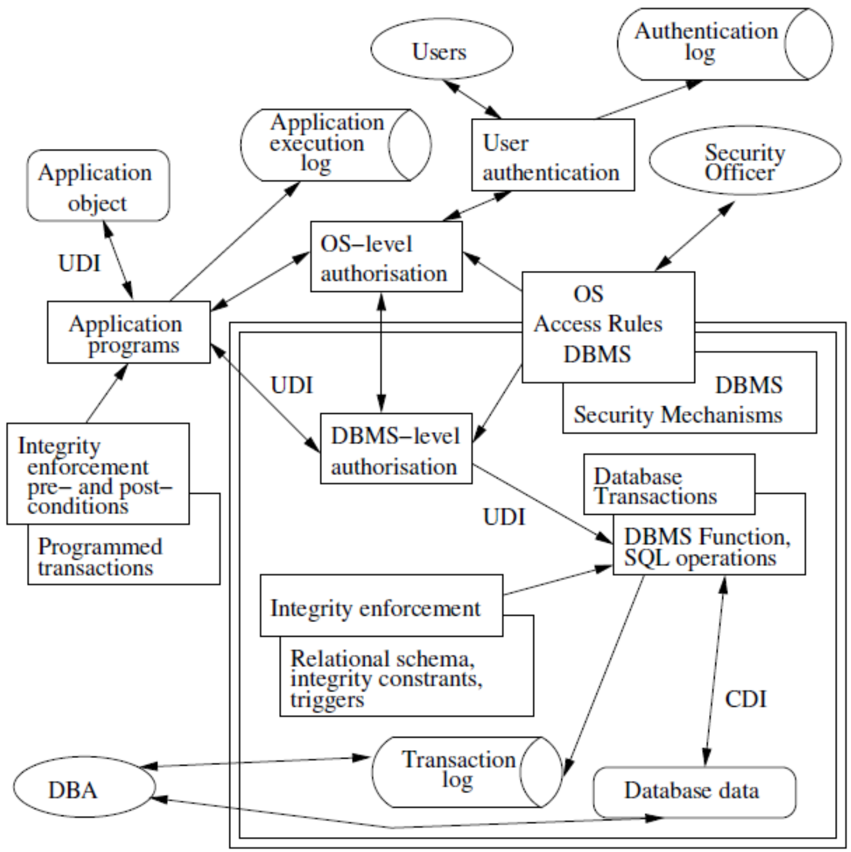
- Certification rules:
  - C1: When an integrity verification procedure (IVP) is run, it must ensure that all constrained data items (CDIs) are in a valid state.
  - C2: For some associated set of CDIs, a transformation procedure (TP) must transform those CDIs in a valid stat into a (possibly different) valid state.
  - C3: The allowed relations must meet the requirements imposed by separation-of-duties principle.
  - C4: All TP must append sufficient information to reconstruct the operation to an append-only CDI.
  - C5: Any TP that takes a un-constrained data item (UDI) as input may perform only valid transformations, or none at all, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.

- Enforcement rules:
  - E1: The system must maintain the certified relations, and must ensure that only transformation processes (TPs) certified to run on a constrained data item (CDI) manipulate that CDI.
  - E2: The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user.
  - E3: The system must authenticate each user attempting to execute a TP.
  - E4: Only the certifier of a TP may change the list of entities associated with a TP. No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.

Reference: D. Clark, D. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, IEEE Symposium on Security and Privacy, 1987

Clark-Wilson Security Model ...(3/3)

- Clark-Wilson security model is often implemented in modern database management systems (DBMS) such as: Oracle, DB2, MS SQL, and MySQL.

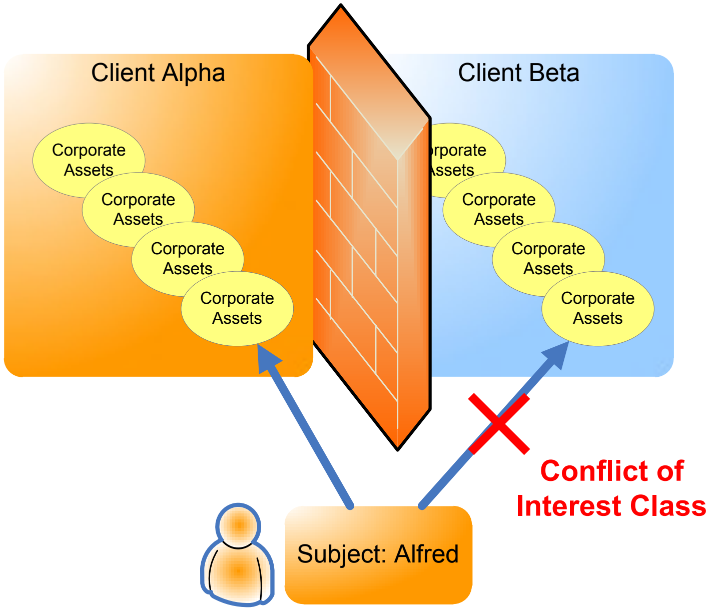


Reference: *Secure Database Development and the Clark-Wilson Security Model*, X.Ge, F.Polack, R.Laleau, University of York, UK.

Brewer-Nash Security Model (a.k.a. Chinese Wall)

Brewer-Nash security model is an information flow model used to implement dynamically changing access permissions.

- A "wall" is defined by a set of rules that ensures no subject from one side of the wall can access objects on the other side of the wall.

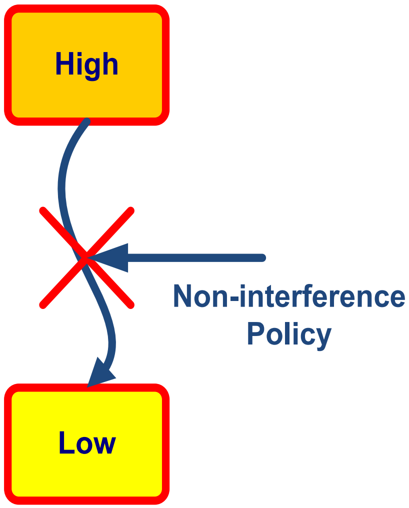


Reference: *The Chinese Wall Security Policy*, D.F.C. Brewer, M. Nash, Gama Secure Systems, UK.

Non-interference Model ...(1/2)

Non-interference model (a.k.a. Goguen-Meseguer security model) is loosely based on the information flow model; however, it focuses on:

- How the actions of a subject at a higher sensitivity level affect the system state or actions of a subject at a lower sensitivity level. (i.e., interference)
  - Users (subjects) are in their own compartments so information does not flow or contaminate other compartments
  - With assertion of non-interference security policy, the non-interference model can express multi-level security (MLS), capability passing, confinement, compartmentation, discretionary access, multi-user/multi key access, automatic distribution and authorization chains, and downgrading.

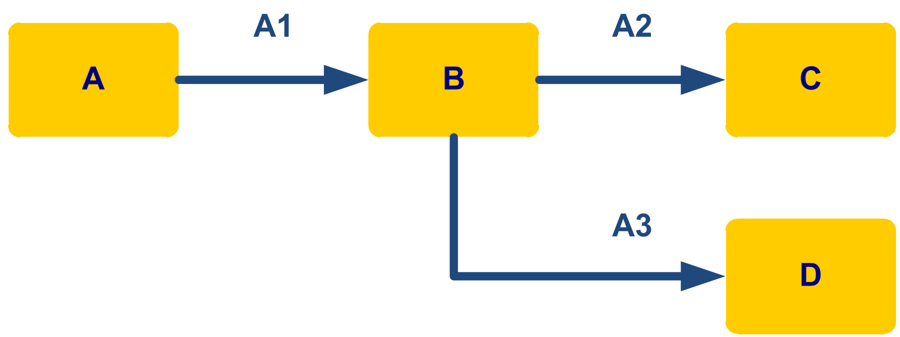


Reference: *Security Policies and Security Models*, J.A. Goguen, J. Meseguer, IEEE, 1982.

Non-interference Model ...(2/2)

- Information flow is controlled by the security policy, where security policy is a set of non-interference assertions (i.e., "capabilities".) For example:
  - A, B, C, and D are compartmentalized subjects.

  - A1, A2, and A3 are non-interference assertions that defines the "capabilities" of what subjects can do.

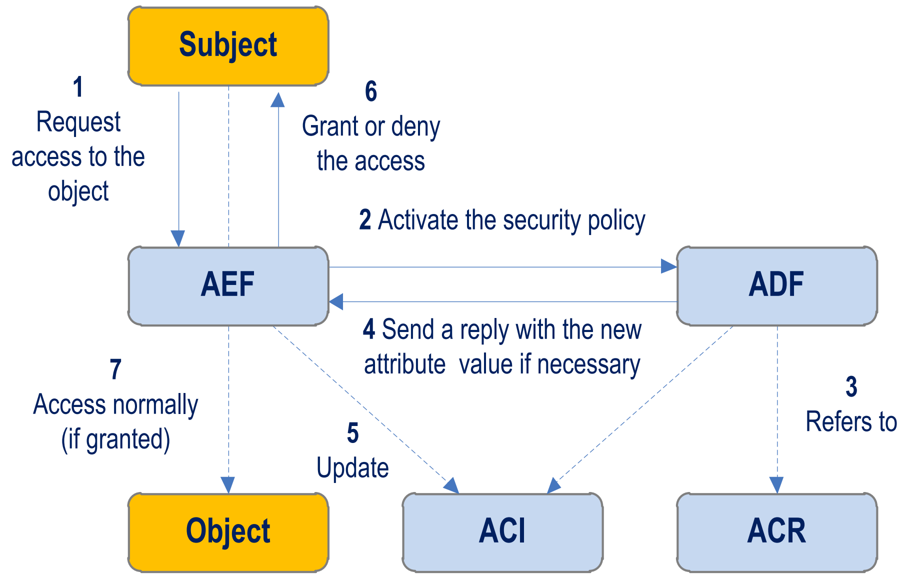


- Non-interference is to address covert channels and inference attacks.
- Note: Bell-LaPadula (BLP) is about information flow between objects.

Reference: *Security Policies and Security Models*, J.A. Goguen, J. Meseguer, IEEE, 1982.

Rule-set Based Access Control Model

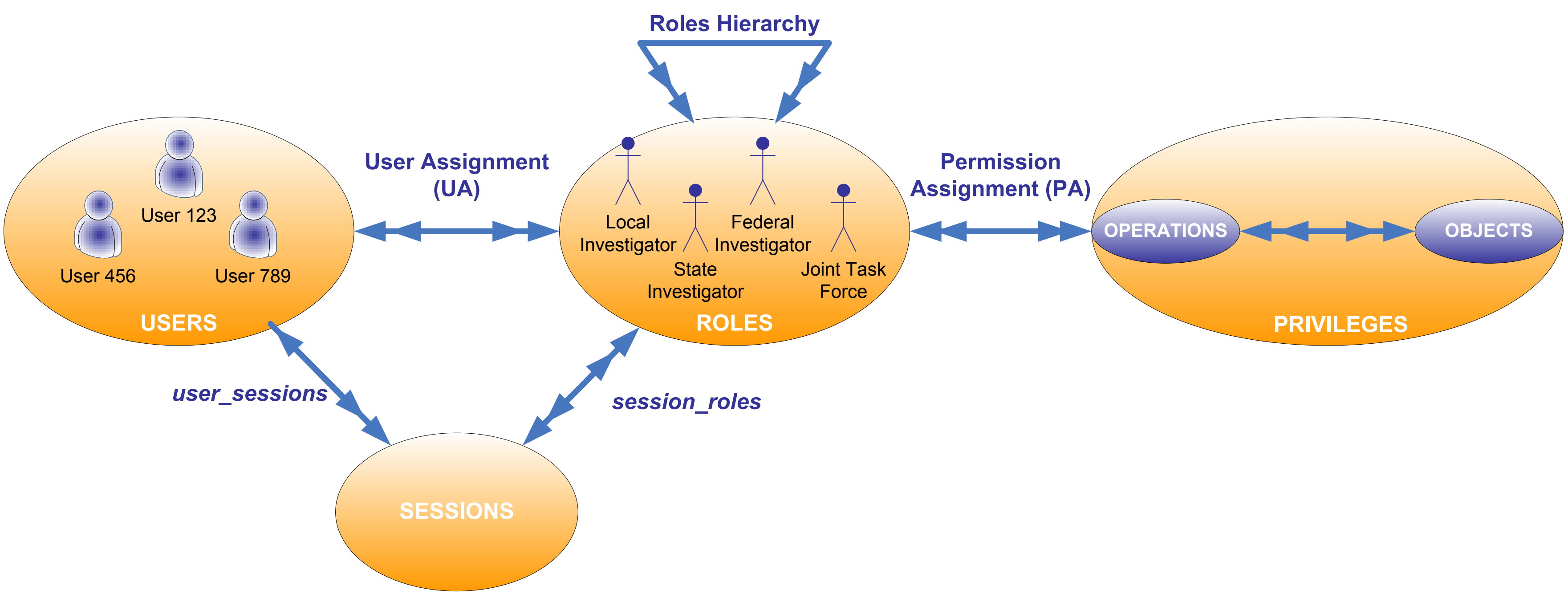
- Access is based on a set of rules that determines capabilities.
- The model consists of:
  - Access enforcement function (AEF)
  - Access decision function (ADF)
  - Access control rules (ACR)
  - Access control information (ACI)



Reference: M.D. Abrams, K.W. Eggers, L.J. LaPadula, I.M. Olson, *Generalized Framework for Access Control: An Informal Description*, October, 1990.

Example of Rule-set Based Access Control: Role-based Access Control (RBAC)

- Limited hierarchical RBAC-based authorization for web services.
  - User Assignment: Identity-to-roles.
  - Permission Assignment: Roles-to-privileges.

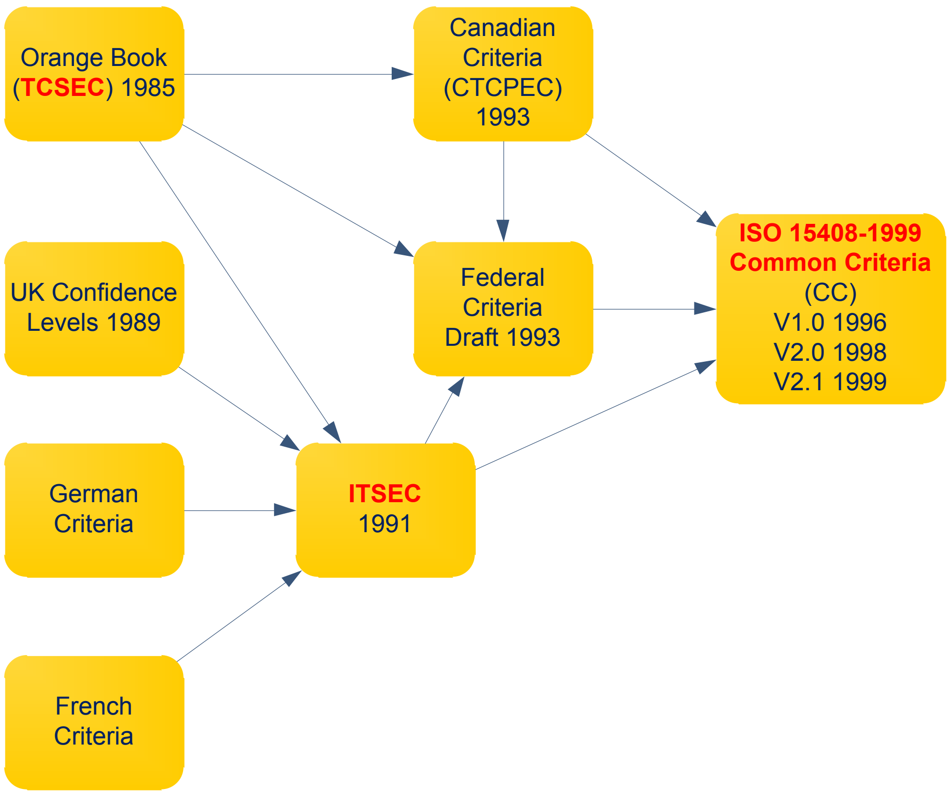


Reference: *Role Based Access Control (RBAC) and Role Based Security*, NIST. (http://csrc.nist.gov/groups/SNS/rbac/)

Security Architecture & Models Domain

- Computing Platforms
- Security Models
  - Information Security Models
- Evaluation & Certification
- Security Architecture
  - Modes of Operation
  - Architecture Concepts
  - Implementation Models

Evaluation Criteria



- 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)

Trusted Computer Security Evaluation Criteria (TCSEC) (DoD 5200.28-STD)

Based on meeting the following 6 requirements…

1. Security policy – DAC or MAC.
2. Marking of objects – Sensitivity labels.
3. Identification of subjects – Identification & authorization of users (subjects).
4. Accountability – Audit logs
5. Assurance – Operational security requirements.
   - Assurance in meeting the policy, marking, identification, and accountability requirements
   - Documentation – Security features user's guide (SFUG), trusted facility manual (TFM), test & design document
6. Continuous protection – Anti-tamper provision.

Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria* (TCSEC), December 26, 1985.

TCSEC Divisions

- Division D: Minimal Protection
- Division C: Discretionary Protection (DAC)
  - C1: Discretionary Security Protection
  - C2: Controlled Access Protection
- Division B: Mandatory Protection (MAC)
  - B1: Labeled Security Protection
  - B2: Structured Protection
  - B3: Security Domains
- Division A: Verified Protection
  - A1: Verified Design

Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria* (TCSEC), December 26, 1985.

TCSEC Division C: Discretionary Protection

- C1: Discretionary Security Protection.
  - Security policy: discretionary access control
  - Accountability: identification and authentication
  - Assurance:
    - Operational assurance: system architecture, system integrity
    - Life-cycle assurance: security testing
  - Documentation: security features user's guide (SFUG), trusted facility manual (TFM), test document, design document
- C2: Controlled Access Protection.
  - C1 +
  - Security policy: object reuse
  - Accountability: audit

Reference: DoD 5200.28-STD, _Trusted Computer System Evaluation Criteria_ (TCSEC), December 26, 1985.

TCSEC Division B: Mandatory Protection

- B1: Labeled Security Protection
  - Security policy: DAC, object reuse, labels, MAC
  - Accountability: identification and authentication, audit
  - Assurance:
    - Operational assurance: system architecture, system integrity
    - Life-cycle assurance: security testing, design specification and verification
  - Documentation: security feature user's guide (SFUG), trusted facility manual (TFM), test and design documentation

Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria* (TCSEC), December 26, 1985.

TCSEC Division B: Mandatory Protection

- B2: Structured Protection
  - Security policy: B1 + subject sensitivity labels, device labels
  - Accountability: B1 + trusted path
  - Assurance:
    - Operational assurance: B1 + covert channel analysis, trusted facility management
    - Life-cycle assurance: B1 + configuration management
  - Documentation: B1
- B3: Security Domains
  - Security policy: B2
  - Accountability: B2
  - Assurance:
    - Operational assurance: B2 + trusted recovery
    - Life-cycle assurance: B2
  - Documentation: B2

Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria* (TCSEC), December 26, 1985.

TCSEC Division A: Verified Protection

- A1: Verified Design
  - Functionally equivalent as class: B3
  - Requires design verification
    - Security policy must be identified and documented (including a mathematical proof of the security model)
    - Must provide a formal top-level specification (FTLS) that identifies all the components that constitutes trusted computing base (TCB)
    - The FTLS of the TCB must be shown to be consistent with the documented security policy model (FTLS ≈ security policy)
    - The TCB must be shown to be consistent with the documented FTLS (TCB ≈ FTLS)
    - Formal analysis techniques must be used to identify and analyze covert channels

Reference: DoD 5200.28-STD, _Trusted Computer System Evaluation Criteria_ (TCSEC), December 26, 1985.

Information Technology Security Evaluation Criteria (ITSEC)

- Security objectives: Why is the functionality wanted?
  - Statements about the system environment.
  - Assumption about the target of evaluation (TOE) environment.
- Security functions (F): What is actually done?
  - Rational for security functions.
  - Required security mechanisms.
  - Required evaluation level.
- Security assurance (E): How is it done?
  - The level of assurance required in the TOE.

Reference: *Information Technology Security Evaluation Criteria (ITSEC)*, version 1.2, June 28, 1991.

ITSEC – Functional + Assurance Ratings

- Functional (F)
  - F-C1 – F-B3 Mirror the functionality aspects of TCSEC (Orange Book) classes.
  - F6 High integrity req. for data and programs.
  - F7 High availability req. for system.
  - F8 High integrity req. for data communications.
  - F9 High confidentiality req. for data communications.
  - F10 High confidentiality + integrity req. for data communications.
- Assurance (E)
  - E0 Inadequate assurance.
  - E1 System in development.
  - E2 Informal system tests.
  - E3 Informal system + unit tests.
  - E4 Semi-formal system + unit tests.
  - E5 Semi-formal system + unit tests and source code review.
  - E6 Formal end-to-end security tests + source code reviews.

Reference: *Information Technology Security Evaluation Criteria (ITSEC)*, version 1.2, June 28, 1991.

ITSEC vs. TCSEC

ITSEC Rating	TCSEC Rating
E0	D - Minimal Security
F-C1, E1	C1 - Discretionary Security Protection
F-C2, E2	C2 - Controlled Access Protection
F-B1, E3	B1 - Labeled Security
F-B2, E4	B2 - Structured Protection
F-B3, E5	B3 - Security Domains
F-B3, E6	A1 - Verified Design
F6 - High integrity	N/A
F7 - High availability	N/A
F8 - Data integrity during communications	N/A
F9 - High confidentiality (encryption)	N/A
F10 - Networks w/high demands on confidentiality and integrity	N/A

Reference: *Information Technology Security Evaluation Criteria (ITSEC)*, version 1.2, June 28, 1991.

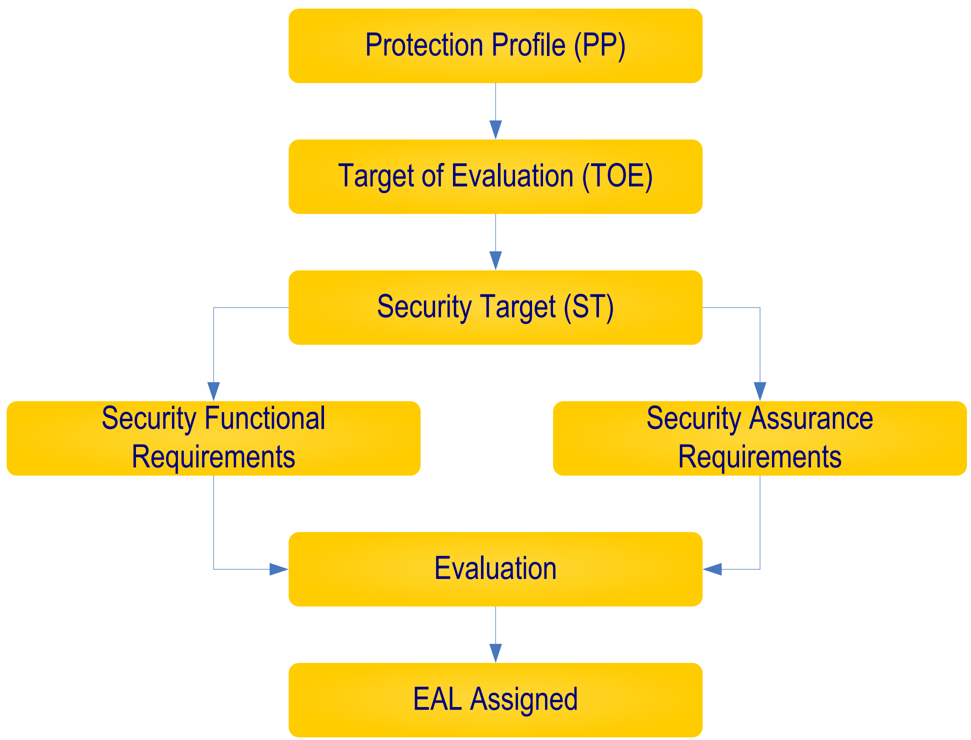
Common Criteria (ISO 15408)

- Protection Profile (PP)
  - Specific functional and assurance requirements
  - Applies to a category of products, not just a single one
- Target of Evaluation (TOE)
  - The specific product or system that is being evaluated
- Security Target (ST)
  - Written by vendor or developer to explain functional and assurance specifications of product, and how they meet CC or PP requirements
- Evaluation Assurance Level (EAL)
  - Combined rating of functional and assurance evaluation

Reference: *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

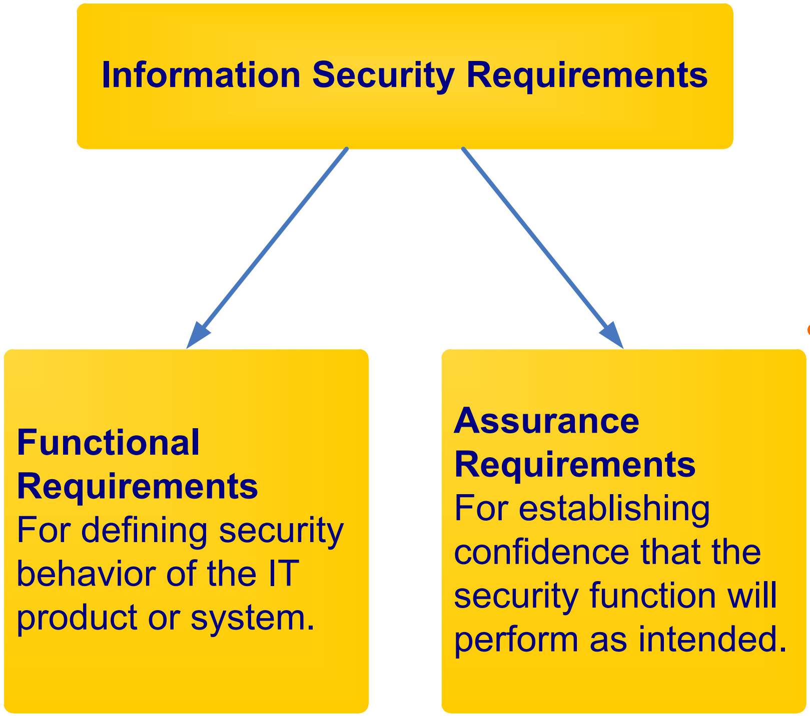
Common Criteria (ISO 15408)

- Part One: Introduction and General Model.
- Part Two: Security Functional Requirements.
- Part Three: Security Assurance Requirements (establishes a set of assurance components – Evaluation Assurance Levels (EAL)).



Reference: *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

Common Criteria Security Requirements

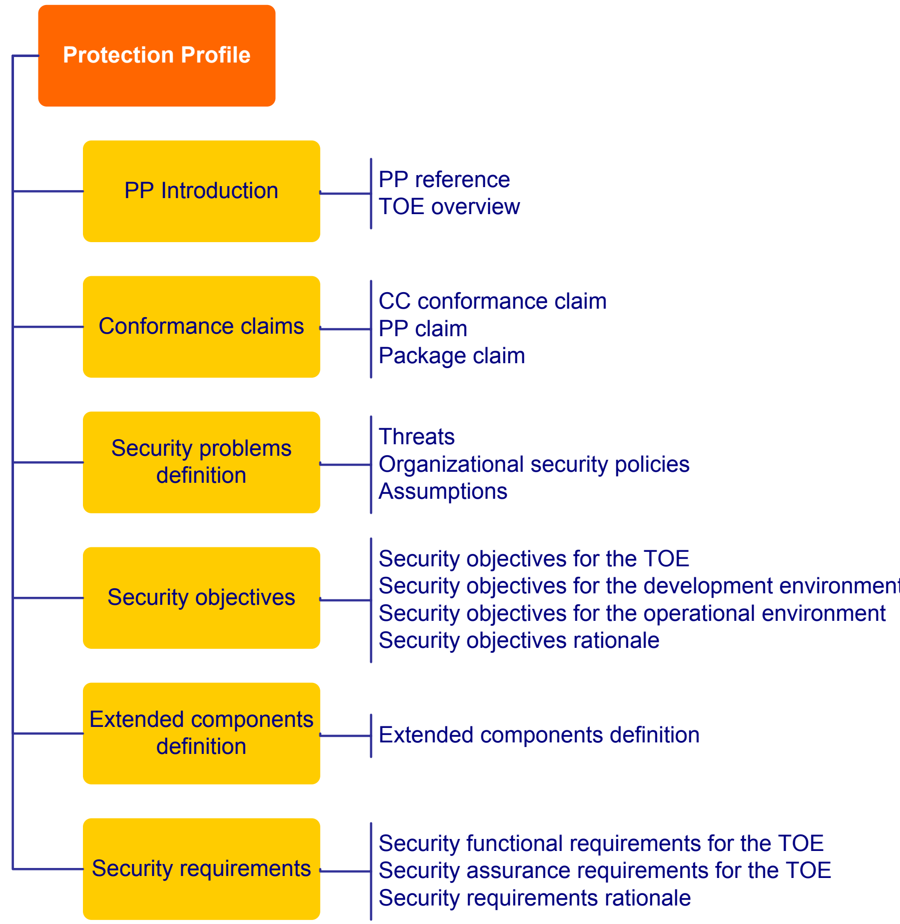


- Assurance Requirements define the security attributes (or countermeasures) that in information system shall provide so the system owner can have a measurable level of assurance that the risks have been sufficiently addressed (or mitigated.)

- Functional Requirements explain the operational functions which an information system shall perform in support of subjects access the objects.

Common Criteria – Protection Profile (PP)

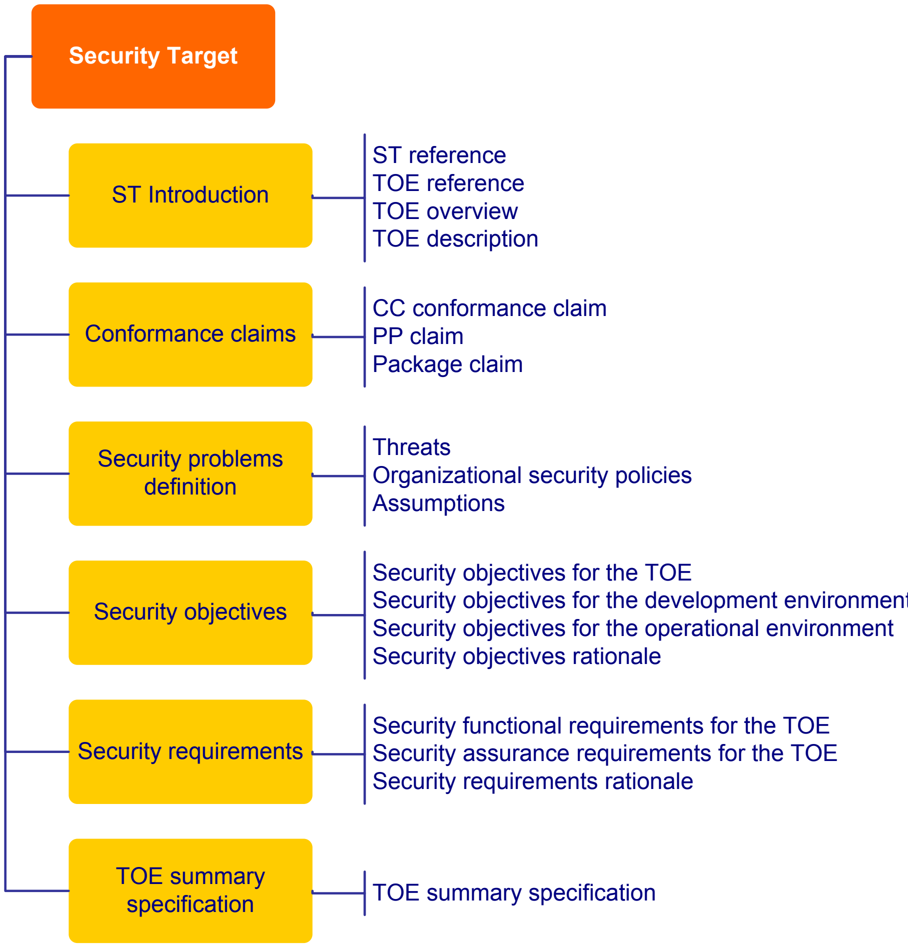
- Protection Profile (PP) is an implementation-independent specification of information security requirements.
  - Security objectives
  - Security functional requirements
  - Information assurance requirements
  - Assumption and rationale



Reference: *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

Common Criteria – Security Target (ST) & Target of Evaluation (TOE)

- Security Target (ST) is similar to PP. It is a vendor response to PP that contains implementation-specific information to demonstrate how the Target of Evaluation (TOE) addresses PP.
- Target of Evaluation (TOE) is the specific product or system that is being evaluated.



Reference: *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

Common Criteria (CC) (ISO 15408)

- Evaluation Assurance Level (EAL) is the combined rating of functional and assurance evaluation
  - EAL 1: Functionally tested
  - EAL 2: Structurally tested
  - EAL 3: Methodically tested and checked
  - EAL 4: Methodically designed, tested, and reviewed
  - EAL 5: Semi formally designed and tested
  - EAL 6: Semi formally verified, designed, and tested
  - EAL 7: Formally verified, designed, and tested

The U.S. recognizes products that have been evaluated under the sponsorship of other signatories and in accordance with the International Common Criteria for Information Technology Security Evaluation Recognition Arrangement (CCRA) for EALs 1-4 only.

Reference: *Common Criteria Evaluation & Validation Scheme (CCEVS)*, Version 2.3, August 2005.

Security Architecture & Models Domain

- Computing Platforms
- Security Models
  - Information Security Models
- Evaluation & Certification
- Security Architecture
  - Modes of Operation
  - Architecture Concepts
  - Implementation Models

Modes of Operation... (1/2)

- Dedicated
  - System is specifically & exclusively dedicated to and controlled for the processing of one type or classification of information.
- System-high
  - Entire system is operated at the highest security classification level, and trusted to provide “need-to-know” to a specific user or role (DAC)
- Multi-Level Security (MLS)
  - A system which allows to operate and process information at multiple classification levels.
  - Controlled mode.
    - The mode of operation that is a type of MLS in which a more limited amount of trust is placed in the HW/SW base of the system, with resultant restrictions on the classification levels and clearance level that can be supported.
- Compartmentalized
  - A system which allows to operate and process information at multiple compartmented information. Not all user have the “need-to-know” on all information.

Modes of Operation... (2/2)

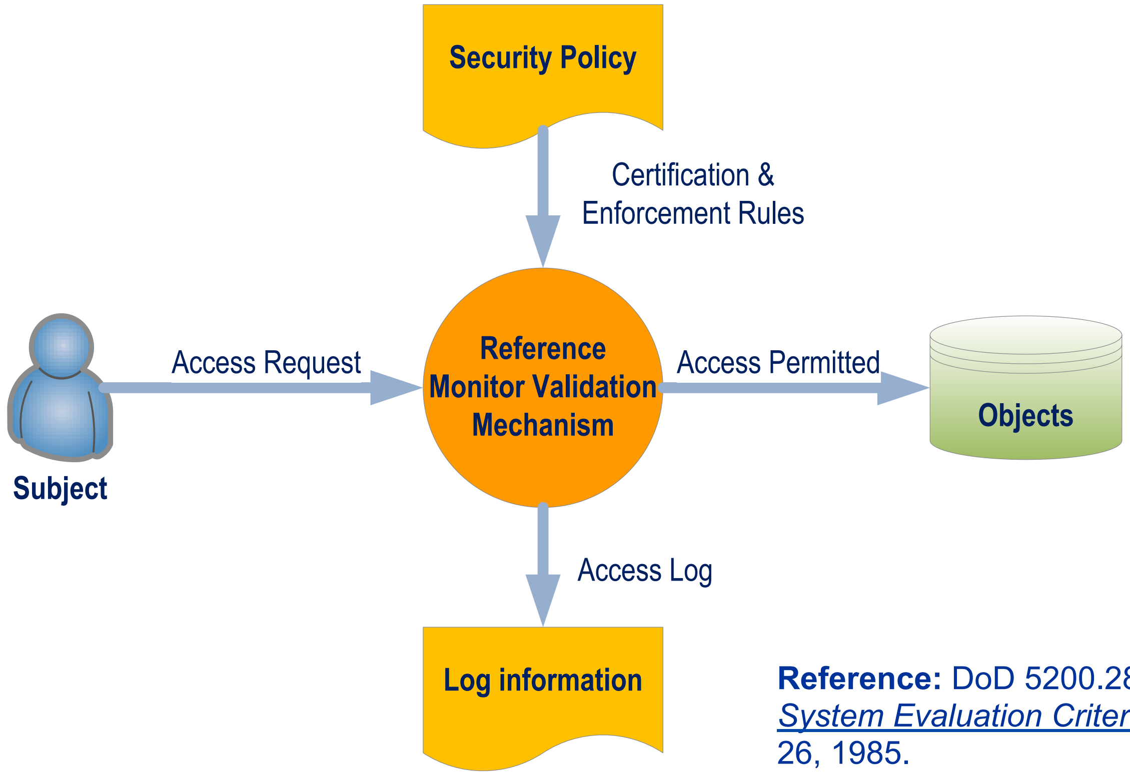
Mode	Clearance Level	Access Approval	Need-to-Know
Dedicated	Proper clearance for all information on the system	Formal access approval for all information on the system	A valid need-to-know for all information on the system
System-High	Proper clearance for all information on the system	Formal access approval for all information on the system	A valid need-to-know for some of the information on the system
Compartmental	Proper clearance for the highest level of data classification on the system	Formal access approval for all information they will access on the system	A valid need-to-know for some of the information on the system
MLS	Proper clearance for all information they will access on the system	Formal access approval for all information they will access on the system	A valid need-to-know for some of the information on the system

Reference: *DCID 6/3 Protecting Sensitive Compartmented Information Within Information Systems*, 2000.

Reference Monitor

A reference monitor is an abstract machine that mediates all accesses to objects by subjects

- Reference monitor is performed by a reference validation mechanism where it is a system composed of hardware, firmware, and software



Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria* (TCSEC), December 26, 1985.

Reference Monitor

- Design requirements:
  - The reference validation mechanism must always be invoked.
  - The reference validation mechanism must be tamper proof.
  - The reference validation mechanism must be small enough to be subject to analysis and tests to assure that it is correct.

- Reference monitor is “policy neutral”.
  - TCSEC requires Bell-LaPadula
  - But, can be implemented for database security, network security, and other applications, etc.

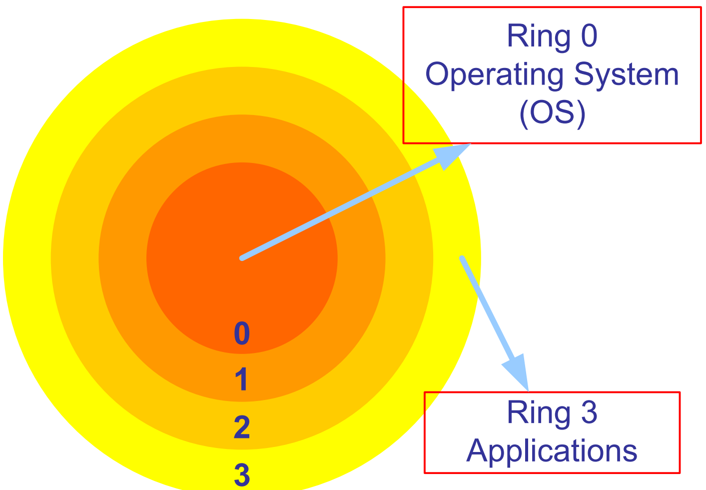
Reference:
• DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria (TCSEC)*, December 26, 1985.
• *The Reference Monitor Concept as a Unifying Principle in Computer Security Education*, C.E. Irvine, Naval Postgraduate School 1999

Trusted Computing Base (TCB)

- The Trusted Computing Base is the totality of protection mechanisms within a computing system – hardware, firmware, software, processes, transports
- The TCB maintains the confidentiality and integrity of each domain and monitors four basic functions:
  - Process activation
  - Execution domain switching
  - Memory protection
  - Input/Output operation

Reference: DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria (TCSEC)*, December 26, 1985.

TCB – 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.

Questions:

- Which information security model is for confidentiality only?
  -
- Which information security model utilizes access triple (i.e. subject-program-object) to enforce “well-formed” transactions?
  -
- Which information security model allows dynamic change of access permission?
  -
- Which information security model defines the direction of the information flow?
  -

Answers:

- Which information security model is for confidentiality only?
  - Bell-LaPadula
- Which information security model utilizes access triple (i.e. subject-program-object) to enforce “well-formed” transactions?
  - Clark-Wilson
- Which information security model allows dynamic change of access permission?
  - Brewer-Nash
- Which information security model defines the direction of the information flow?
  - Information Flow Model

Questions:

- What mediates all accesses to objects by subjects?
  –
- What is the protection mechanism inside a computer that is responsible for enforcing the security policy?
  –
- What is the system (e.g., hardware, firmware, OS, and software applications) that implements the reference monitor concept?
  –

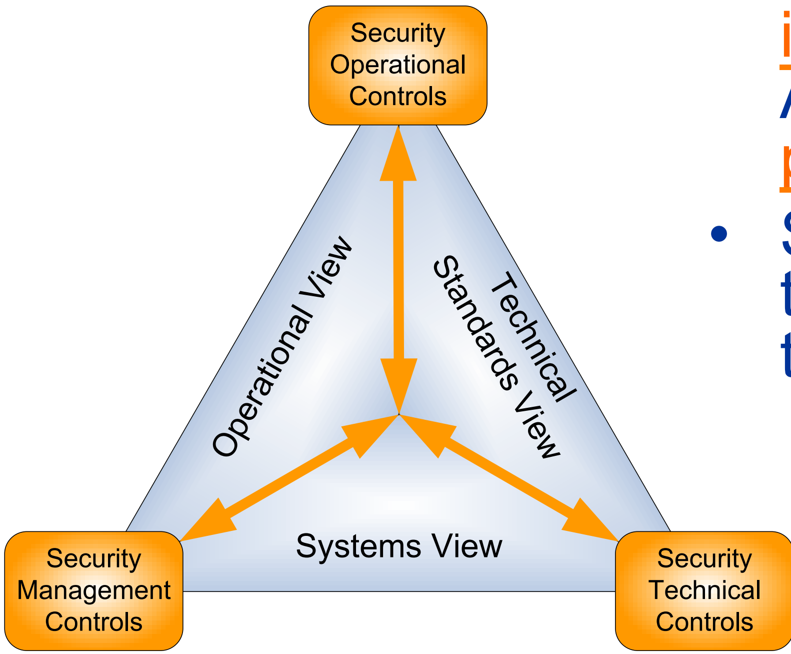
Answers:

- What mediates all accesses to objects by subjects?
  - Reference monitor validation mechanism
- What is the protection mechanism inside a computer that is responsible for enforcing the security policy?
  - Secure kernel (i.e., rings of protection)
- What is the system (e.g., hardware, firmware, OS, and software applications) that implements the reference monitor concept?
  - Trusted computing base (TCB)

Topics
Security Architecture & Models Domain

- Computing Platforms
- Security Models
  - Information Security Models
- Evaluation & Certification
- Security Architecture
  - Modes of Operation
  - Architecture Concepts
  - Implementation Models

Security Architecture & Construction Methodology



Relationship between Enterprise System Architecture and Security Controls

- Security Architecture is an integrated view of System Architecture from a security perspective.
- Security Architecture describes how the system should be implemented to meet the security requirements.
  - **Operational View** = A set of Enterprise Mission/Business Operational Processes that influences the selection of Security Operational, Management and Technical Controls
  - **Systems View** = The Enterprise-wide System of Systems that influences the selection of Security Management, Technical, Operational Controls
  - **Technical Standards View** = The implemented technologies that influence the selection of Security Technical, Operational and Management Controls

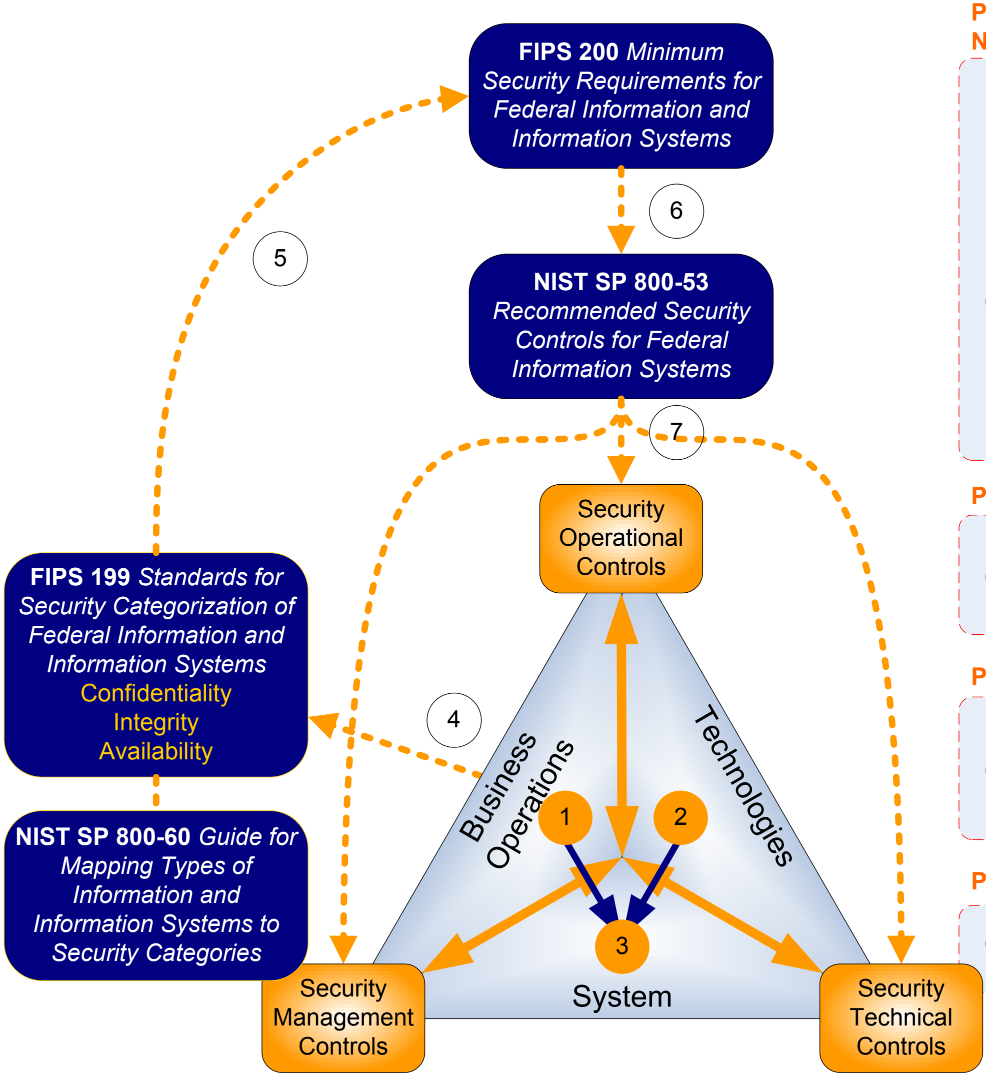
References:

- *DoD Architecture Framework (DoD AF) V1.0*
- FIPS 200, *Minimum Security Controls for Federal Information Systems*

Security Architecture

- Enterprise – A collective of functional organizations / units that is composed of multiple domain and networks.
- Architecture – The highest level concept of a system in its operating environment (Conceptual model)
- Security Architecture – A integrated view of system architecture from a security perspective
- Enterprise Security Architecture – An integrated view of enterprise system architecture from a perspective of meeting the organizational security policy, standards, and processes.

Security Architecture & Construction Methodology – Civil



Phase 1: Discover Information Protection Needs

1 2 3 **Define Mission/Business Needs**
- **System** is designed to meet: **Operational/Business** needs,
- Using the available & cost-effective **Technologies**.

4 **Create Info. Mgmt. Model (IMM)**
- Define the Security Categories of the information types.

Define Info. Protection Policy (IPP).
- Perform Preliminary Risk Assessment

Assemble Info. Mgmt. Plan (IMP)

Phase 2: Define Security Requirements

5 Based on the security category, define the minimum **security requirements** for the system.

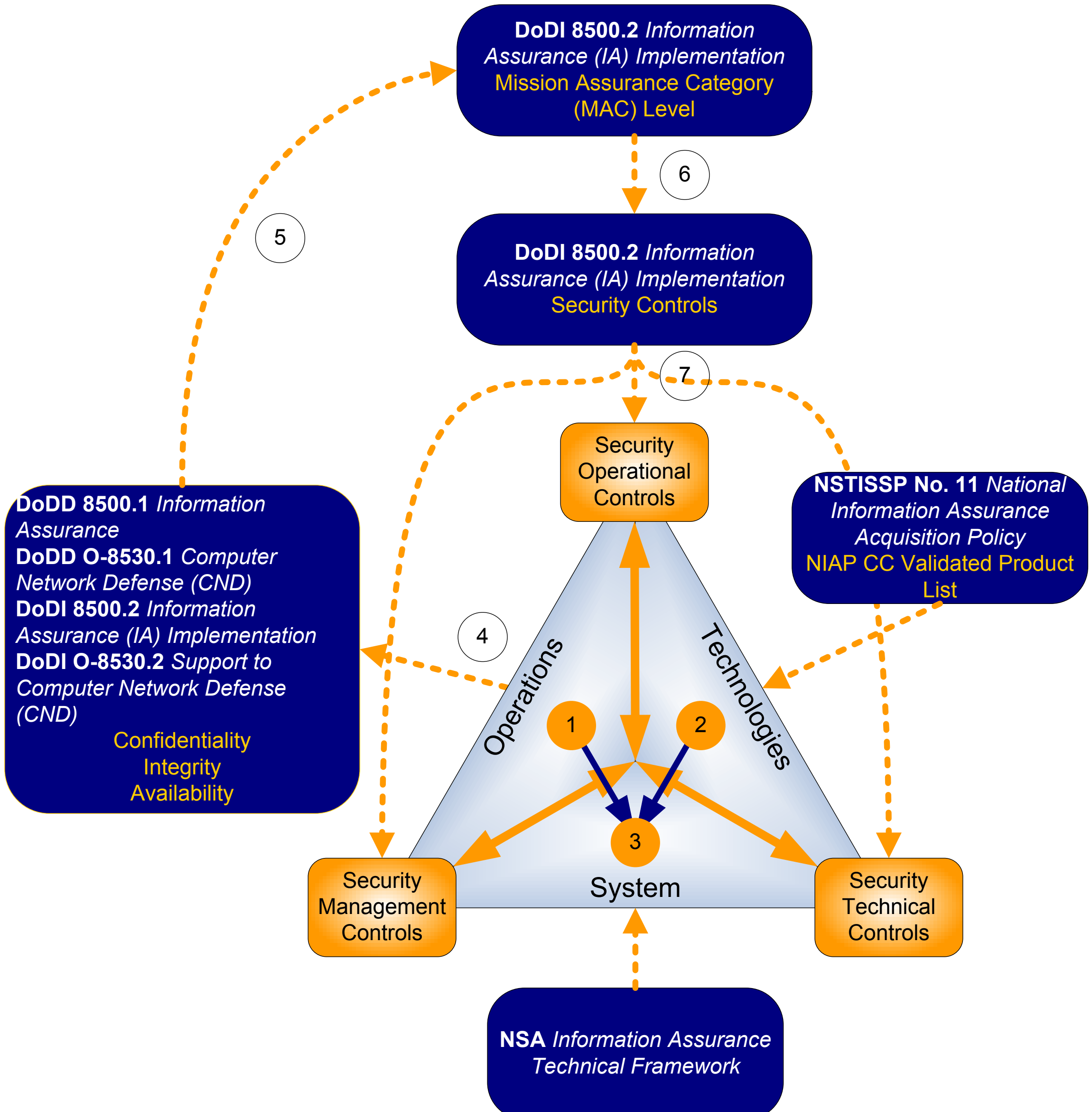
Phase 3: Define System Security Architecture

6 Based on the minimum security requirements and the system architecture, select **security controls** to meet the security needs.

Phase 4: Develop Detailed Security Design

7 Define the **Security Blueprint** for all security implementation standards.

Security Architecture & Construction Methodology – DoD



Phase 1: Discover Information Protection Needs

1 2 3 **Define Mission/Business Needs**

- **System** is designed to meet: **Operational/Business** needs,
- Using the available & cost-effective **Technologies**.

4 **Create Info. Mgmt. Model (IMM)**

- Define the Security Categories of the information types.

Define Info. Protection Policy (IPP).

- Perform Preliminary Risk Assessment

Assemble Info. Mgmt. Plan (IMP)

Phase 2: Define Security Requirements

5 Based on the security categories, select **MAC Level** and define minimum **security requirements** for the system.

Phase 3: Define System Security Architecture

6 Based on the minimum security requirements and the system architecture, select **security controls** to meet the security needs.

Phase 4: Develop Detailed Security Design

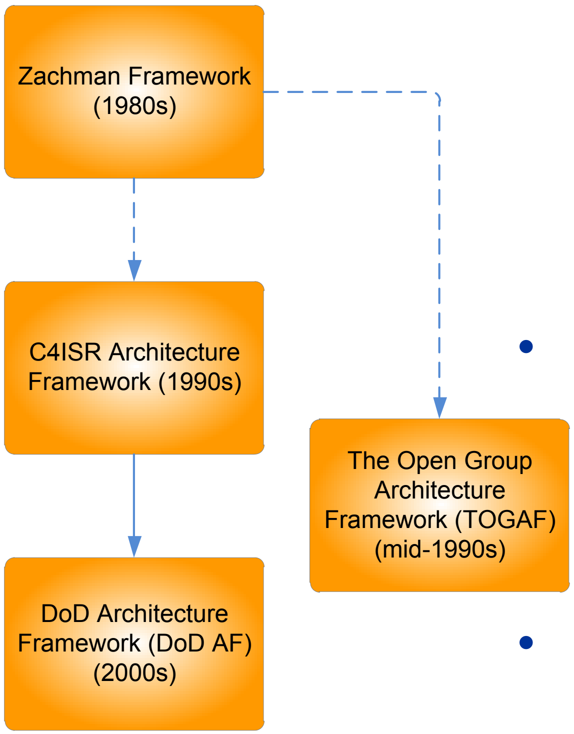
7 Define the **Security Blueprint** for all security implementation standards.

System Architecture – Framework

The purpose of architecture framework is to provide a common standard of terminology, description, and models to facilitate communications between:

- Program Managers and System Designers (Contextual)
- System Designers and System Engineers (Conceptual)
- System Engineers and System Developers (Logical)
- System Developers and System Integrators (Physical)
- System Integrators and System Operators (Component)
- System Users to System Designers, Engineers, Developers, Integrators, and Operators (Concept of Operations)

System Architecture – Historical Perspective



History of Architecture Framework for Information Systems

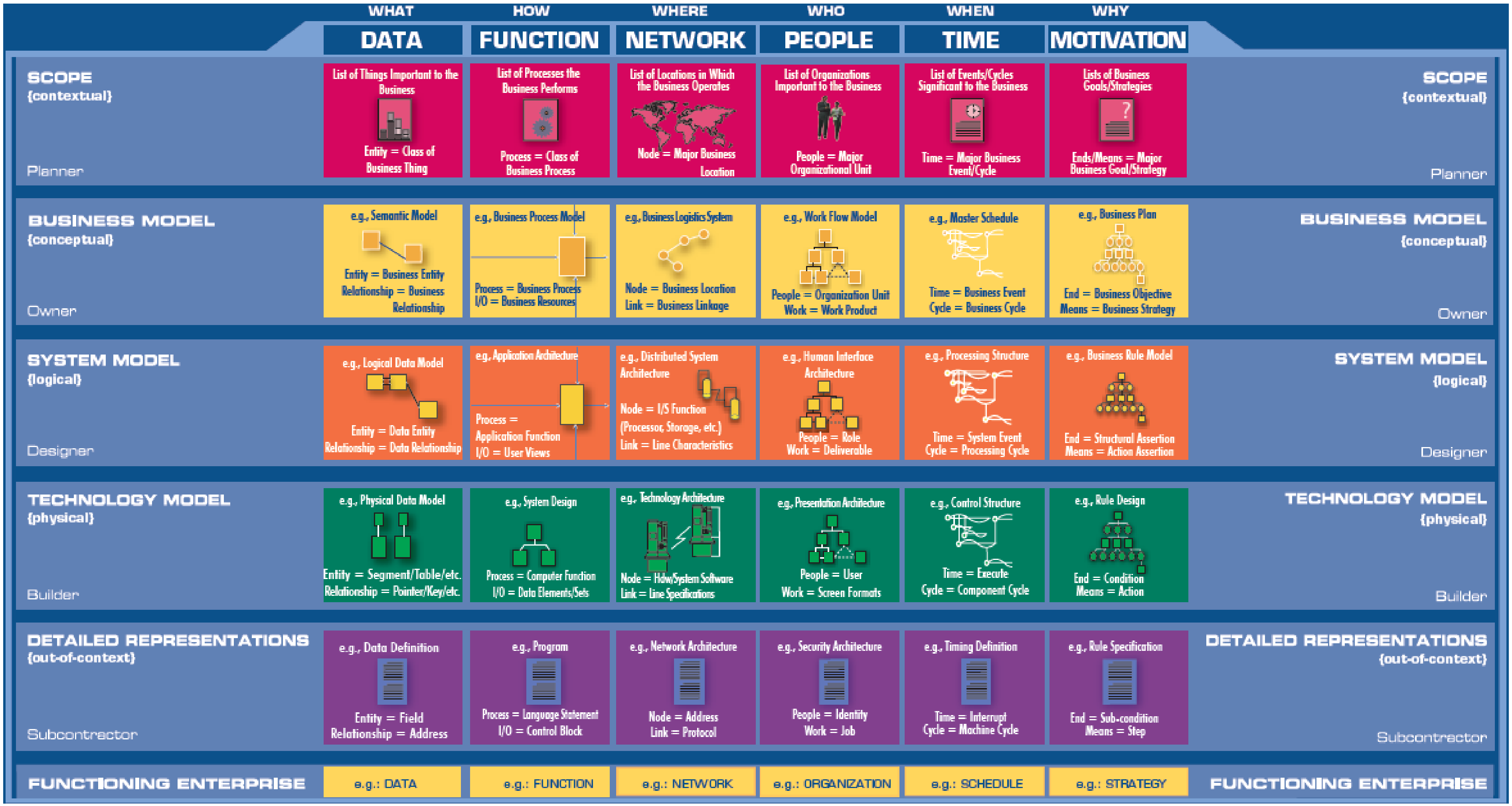
- Zachman Architecture Framework
  - Strategic planner's view
  - System user's view
  - System designer's view
  - System developer's view
  - Subcontractor's view
  - System itself
- The Open Group Architecture Framework (TOGAF)
  - Business Architecture Domain.
  - Application Architecture Domain.
  - Data Architecture Domain.
  - Technology Architecture Domain.
- C4ISR Architecture Framework → DoD AF 1.0 → DoD AF 2.0
  - Operational View
  - Systems View
  - Technical Standards View
  - Service View
  - Capability View

System Architecture – TOGAF Architecture Framework

- The Open Group Architecture Framework (TOGAF) has been developed by the Architecture Forum of The Open Group (TOG) since the mid-90s.
  - Business architecture domain.
  - Application architecture domain.
  - Data architecture domain.
  - Technology architecture domain.

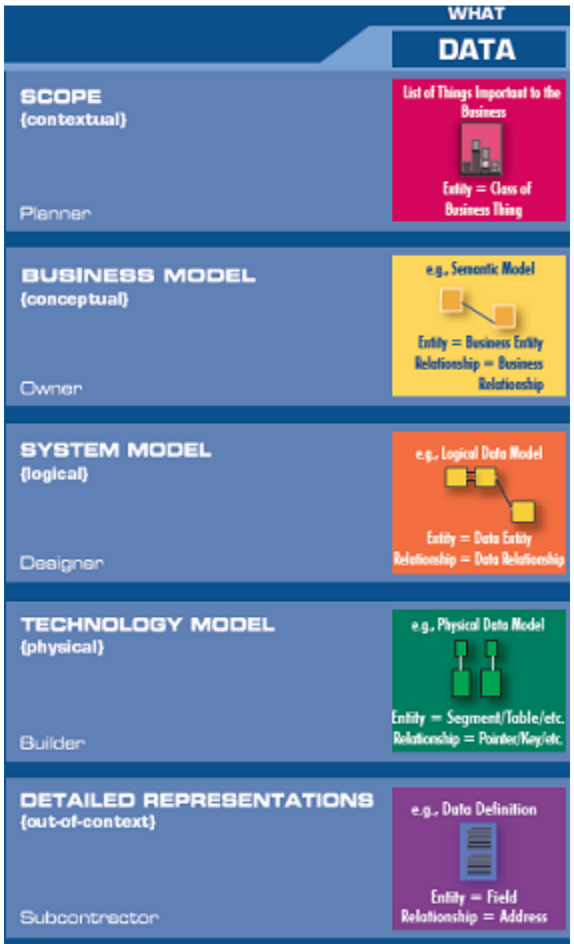
Implementation Architecture

System Architecture – Zachman Architecture Framework



Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of business entities (i.e. Entity Classes.)

Description of relations between business entities (Entity =Business Entity, Relation=Business relations.)

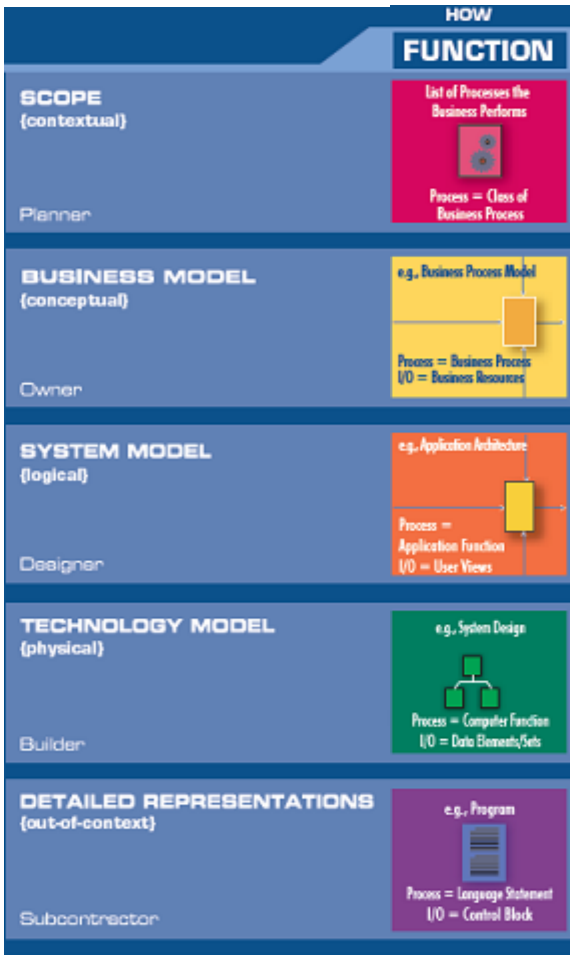
Description of logical data model (Entity=Data Entity, Relation=Data Relations.)

Description of physical data model (Entity=Segment/ Tables/etc., Relation=Pointer/Key/etc.)

Data definition (Entity=Field, Relation=Address.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of business processes (Function=Class of Business Process.)

Description of business process model (Process =Business Process, I/O=Business Resources.)

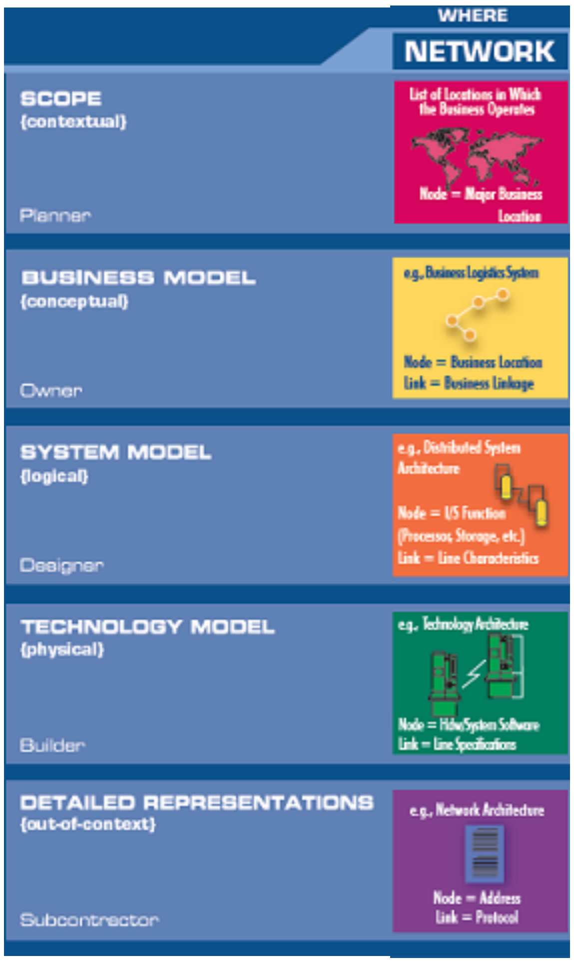
Description of application functions (Process= Application Function, I/O = User Views.)

Description of system design (Process=Computer Function, I/O=Data Elements/Sets.)

Computer program (Process=Language Statement, I/O=Control Block.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of locations (Node=Major Business Location.)

Description of business systems (Node=Business Location, Link=Internetworking Linkage.)

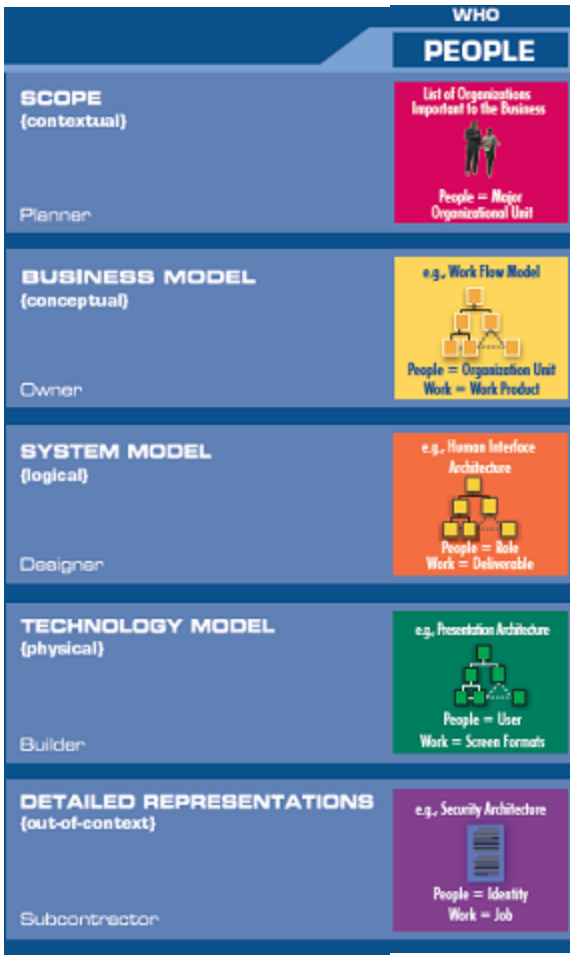
Description of system architecture (Node=InfoSys. Function, Link=Internetworking Characteristics.)

Description of technology architecture (Node=HWCI/ SWCI, Linkage=Internetworking Characteristics.)

Network architecture (Node=Address, Link=Protocols.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of organizations (i.e. Stakeholders)

Description of work-flow model (People= Organization Unit, Work=Work Product.)

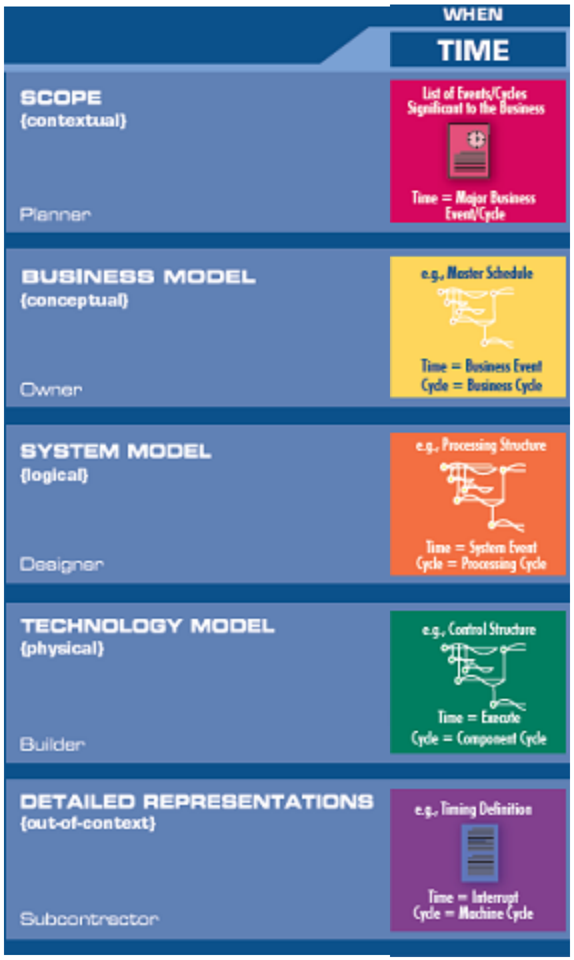
Description of human interface architecture (People= Role, Work=Deliverable.)

Description of presentation architecture (People= User, Work=Screen/User Interface.)

Security architecture (People=Identity, Work=Job Function.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of Events (that is significant to the business.)

Description of master schedule (Time=Business Event, Cycle=Business Cycle.)

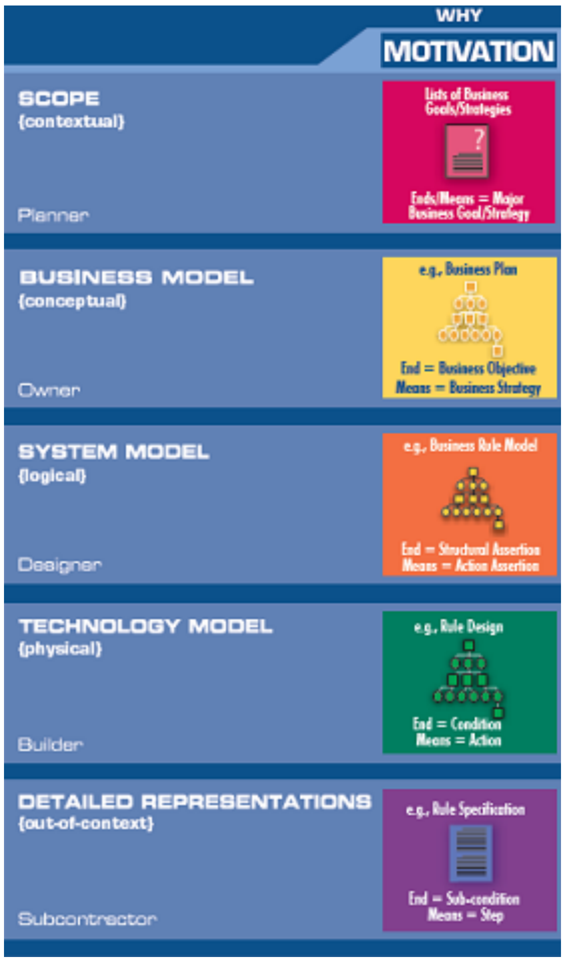
Description of process structure (Time=System Event, Cycle=Processing Cycle.)

Description of control structure (Time=Execute, Cycle=Component Cycle.)

Timing definition (Time=Interrupt, Cycle=Machine Cycle.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – Zachman Architecture Framework



List of business goals/strategy (Ends/Means=Major Business Goal/Success Factor.)

Description of business plan (Ends=Business Objectives, Means=Business Strategy.)

Description of business rule model (End=Structural Assertion, Means=Action Assertion.)

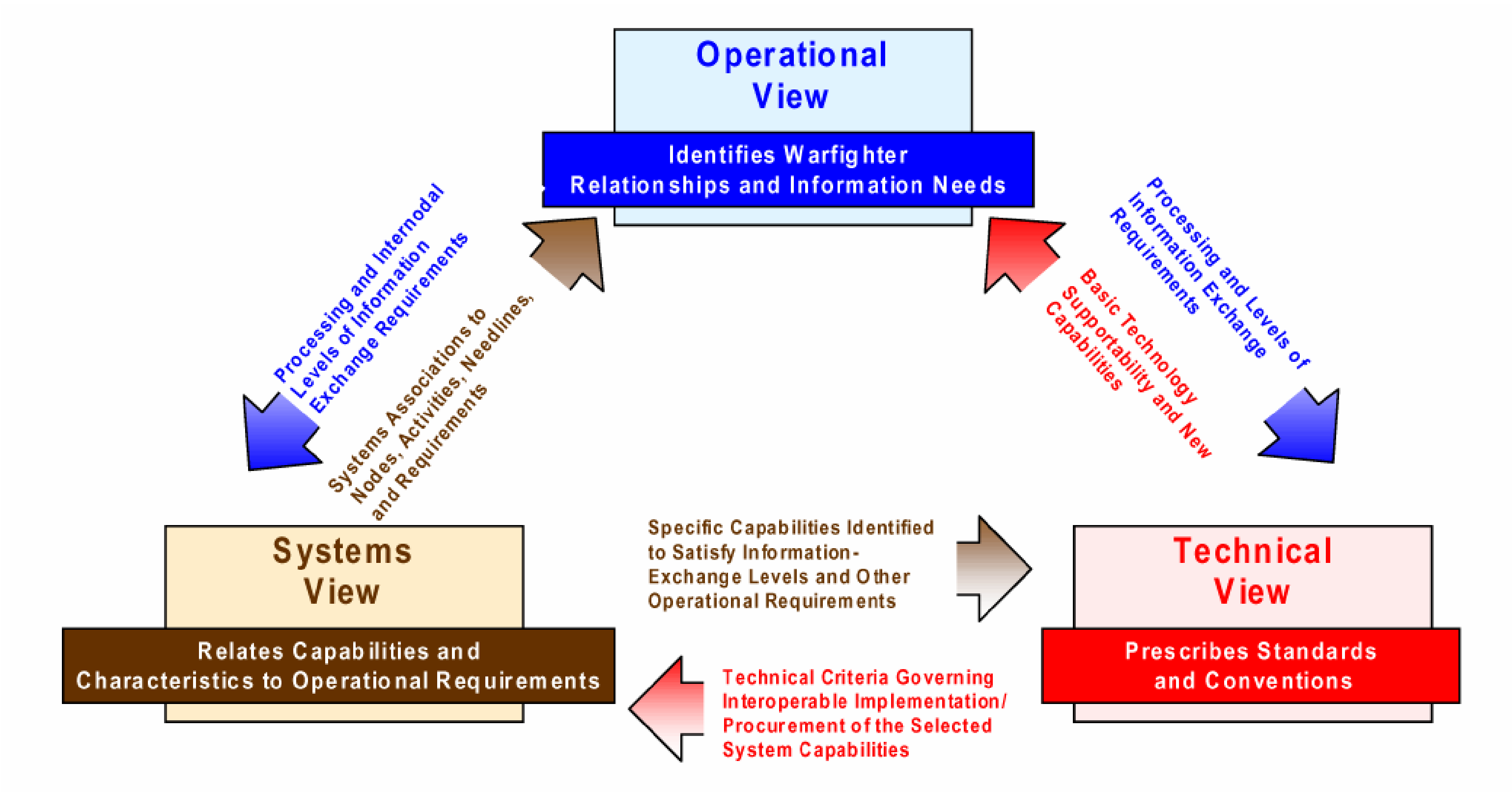
Description of rules design (End=Condition, Means= Action.)

Rule specification (End=Sub-condition, Means=Step.)

Source: *The Zachman Framework for Enterprise Architecture*

System Architecture – DoD Architecture Framework

- DoD Architecture Framework (DoDAF) is based on C4ISR Architecture Framework (C4ISR AF).
- DoDAF 1.0 focuses on SYSTEMS



Reference: *DoD Architecture Framework*, Version 1.0, Volume I

System Architecture – DoDAF 1.0

All View (AV)
- **AV-1** Overview and Summary Information
- **AV-2** Integrated Dictionary

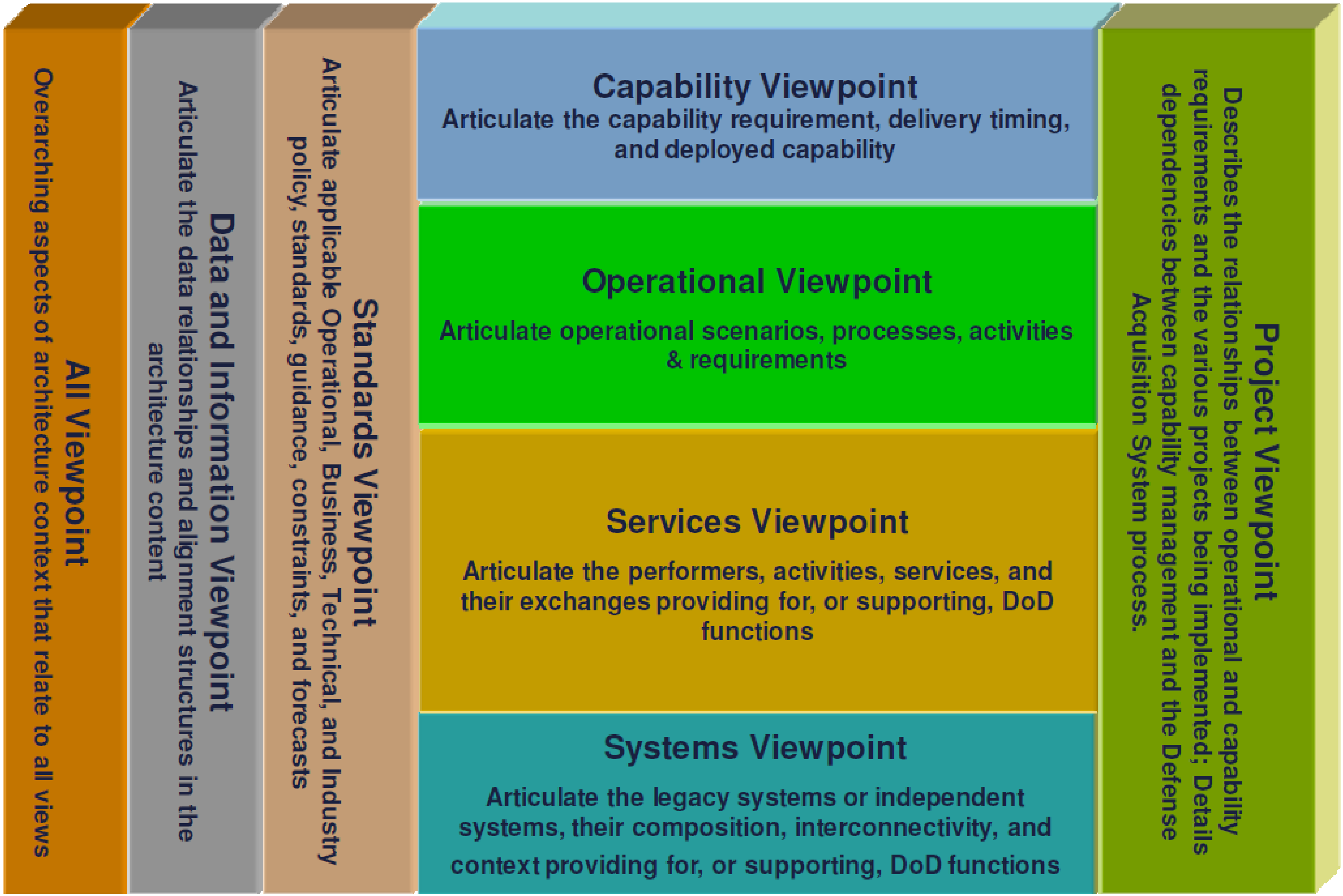
Operational View (OV)
- **OV-1** High Level Operational Concept Graphic
- **OV-2** Operational Node Connectivity Description
- **OV-3** Operational Information Exchange Matrix
- **OV-4** Organizational Relationships Chart
- **OV-5** Operational Activity Model
- **OV-6a** Operational Rules Model
- **OV-6b** Operational State Transition Description
- **OV-6c** Operational Event-Trace Description
- **OV-7** Logical Data Model

Technical Standards View (TV)
- **TV-1** Technical Standards Profile
- **TV-2** Technical Standards Forecast

Systems View (SV)
- **SV-1** System Interface Description
- **SV-2** System Communications Description
- **SV-3** System-System Matrix
- **SV-4** System Functional Description
- **SV-5** Operational Activity to Systems Functionality Traceability Matrix
- **SV-6** System Data Exchange Matrix
- **SV-7** System Performance Parameters Matrix
- **SV-8** System Evolution Description
- **SV-9** System Technology Forecast
- **SV-10a** System Rules Model
- **SV-10b** System State Transition Description
- **SV-10b** System Event-Trace Description
- **SV-11** Physical Schema

Reference: *DoD Architecture* Framework, Version 1.0, Volume I

Enterprise System Architecture – DoDAF 2.0



Reference: DoD Architecture Framework, Version 2.0, Volume I

Enterprise System Architecture – DoDAF 2.0

Project View (PV)

- **PV-1** Project Portfolio Relationships
- **PV-2** Project Timelines
- **PV-3** Project to Capability Mapping

Capability View (CV)

- **CV-1** Vision
- **CV-2** Capability Taxonomy
- **CV-3** Capability Phasing
- **CV-4** Capability Dependencies
- **CV-5** Capability to Organizational Development Mapping
- **CV-6** Capability to Operational Activities Mapping
- **CV-7** Capability to Services Mapping

Data & Information View (DIV)

- **DIV-1** Conceptual Data Model
- **DIV-2** Logical Data Model
- **DIV-3** Physical Data Model

Service View (SvcV)

- **SvcV-1** Services Context Description
- **SvcV-2** Services Resource Flow Description
- **SvcV-3a** Systems-Services Matrix
- **SvcV-3b** Services-Services Matrix
- **SvcV-4** Services Functionality Description
- **SvcV-5** Operational Activity to Services Traceability Matrix
- **SvcV-6** Services Resource Flow Matrix
- **SvcV-7** Services Measures Matrix
- **SvcV-8** Services Evolution Description
- **SvcV-9** Services Technology & Skills Forecast
- **SvcV-10a** Services Rules Model
- **SvcV-10b** Service State Transition Description
- **SvcV-10c** Services Event-Trace Description

Reference: *DoD Architecture* Framework, Version 2.0, Volume I

Enterprise System Architecture – DoDAF 2.0

All View (AV)
- **AV-1** Overview and Summary Information
- **AV-2** Integrated Dictionary

Operational View (OV)
- **OV-1** High Level Operational Concept Graphic
- **OV-2** Operational Resource Flow Description
- **OV-3** Operational Resource Flow Matrix
- **OV-4** Organizational Relationships Chart
- **OV-5a** Operational Activity Decomposition Tree
- **OV-5b** Operational Activity Model
- **OV-6a** Operational Rules Model
- **OV-6b** State Transition Description
- **OV-6c** Event-Trace Description

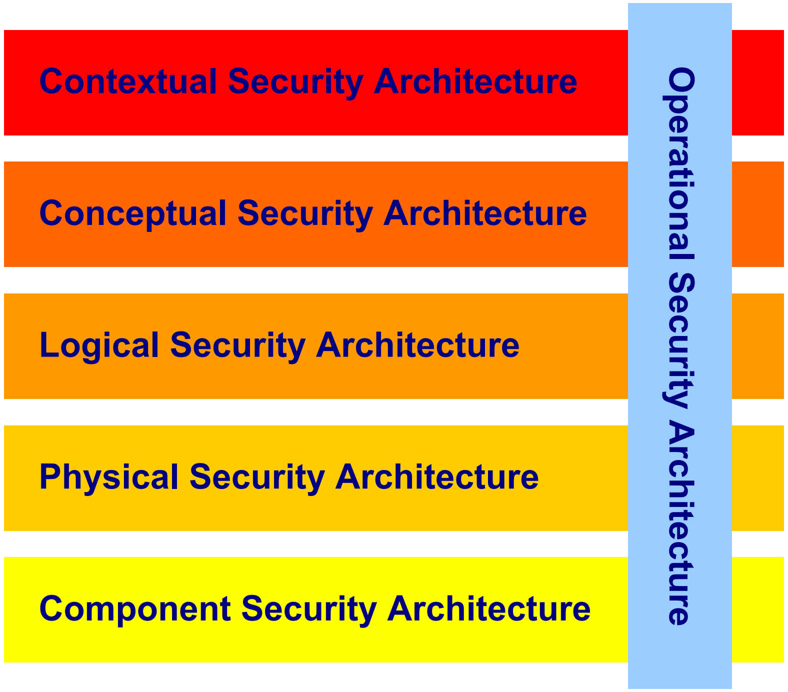
Standards View (StdV)
- **TV-1** Standards Profile
- **TV-2** Standards Forecast

Systems View (SV)
- **SV-1** Systems Interface Description
- **SV-2** Systems Resource Flow Description
- **SV-3** Systems-Systems Matrix
- **SV-4** Systems Functional Description
- **SV-5a** Operational Activity to Systems Function Traceability Matrix
- **SV-5b** Operational Activity to Systems Traceability Matrix
- **SV-6** Systems Resource Flow Matrix
- **SV-7** Systems Measures Matrix
- **SV-8** Systems Evolution Description
- **SV-9** Systems Technology & Skills Forecast
- **SV-10a** Systems Rules Model
- **SV-10b** System State Transition Description
- **SV-10b** System Event-Trace Description

Reference: *DoD Architecture Framework*, Version 2.0, Volume I

Determining the Architecture Model

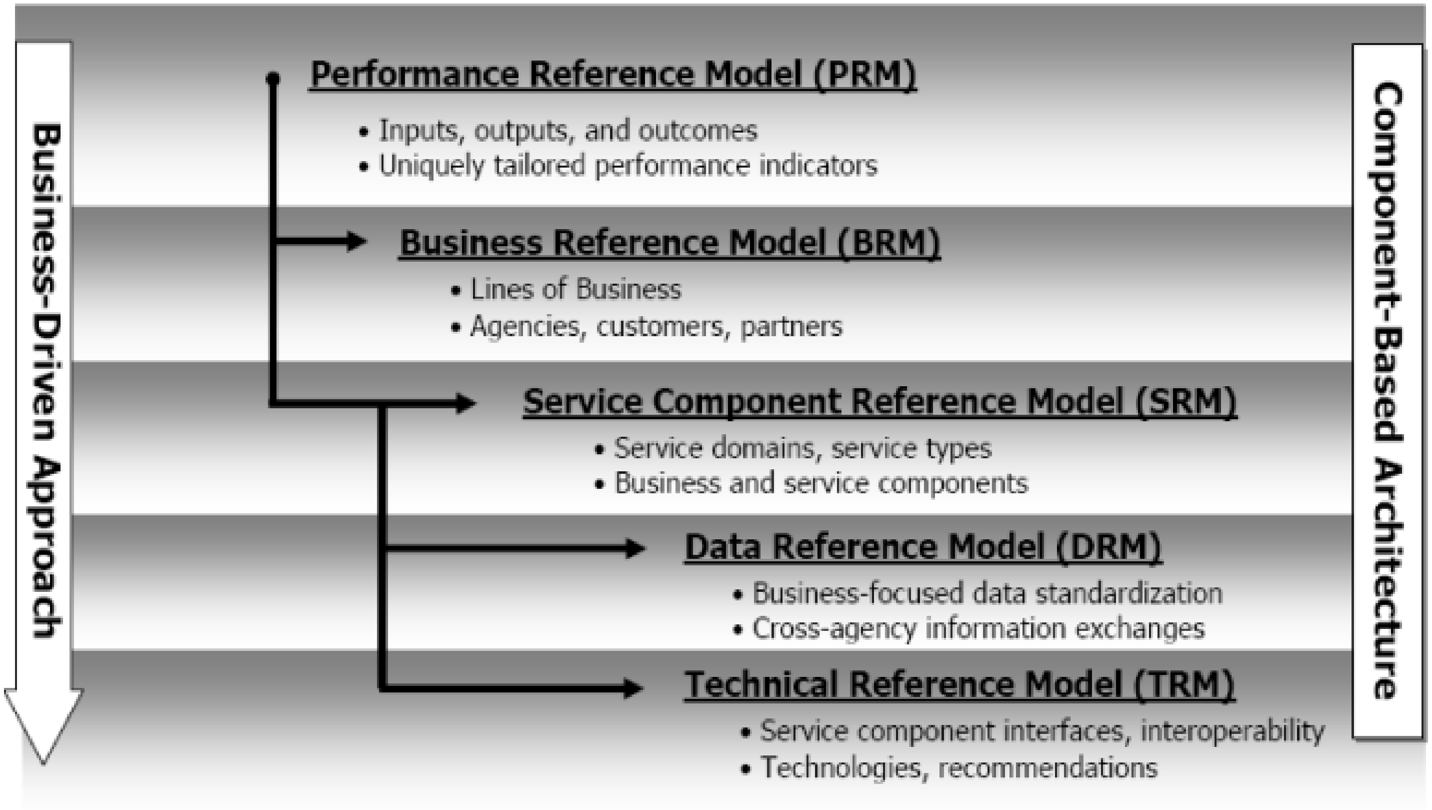
- Architecture is a high-level description of system.
  - Intended use
  - Scope
  - Characteristics to be captured
  - Organization of data for designing a system



Reference: *Enterprise Security Architecture – A Business-Driven Approach*, John Sherwood, 2005

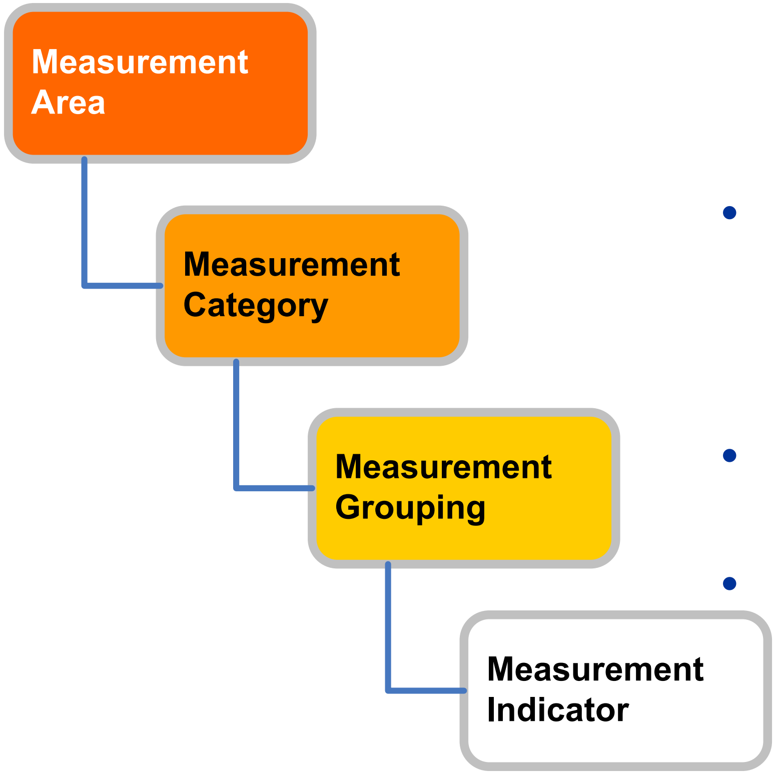
Security Architecture – FEA Framework

- Federal Enterprise Architecture Framework (FEAF) focuses on BUSINESS



Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

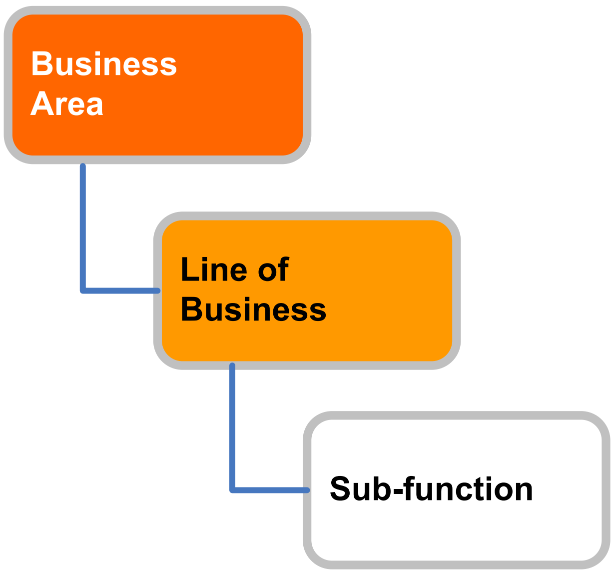
Security Architecture – FEA Framework – Performance Reference Model (PRM)



- Measurement Areas: Mission and Business Results, Customer Results, Processes and Activities, Human Capital, Technology, and Other Fixed Assets.
- Measurement Categories: Collections within each measurement area describing the attribute or characteristic to be measured.
- Measurement Groupings: Specific types of measurement indicators.
- Measurement Indicators: The specific measures, e.g. number and/or % of customers satisfied, tailored for a specific BRM LoB or Sub-function, agency, program, or IT initiative.

Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

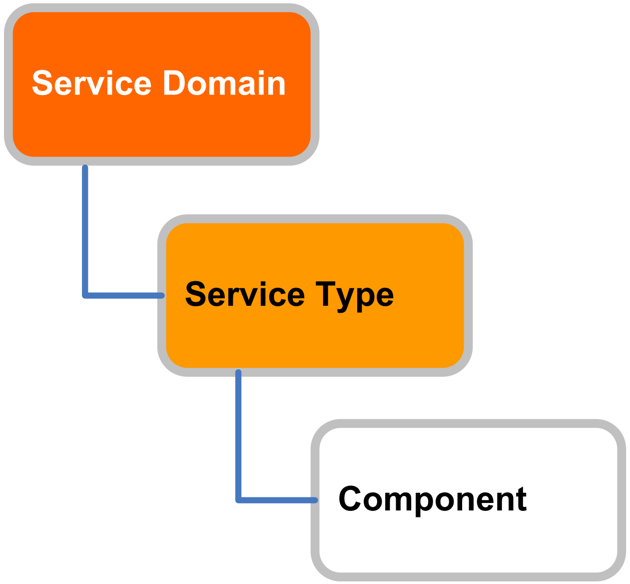
Security Architecture – FEA Framework – Business Reference Model (BRM)



- Business Area: Services for Citizens, Mode of Delivery, Support Delivery of Services, and Management of Government Resources.
- Line of Business (LoB): Each business area (i.e. agency) has a set of LoBs (/ functional organizations) (e.g. IT, Supply Chain, HR, Financial Management, etc.)
- Sub-function: Each LoB has sub-functional organization(s) (e.g. Lifecycle/Change Management, System Development, System Maintenance, Information Systems Security, Information Management, etc.)

Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

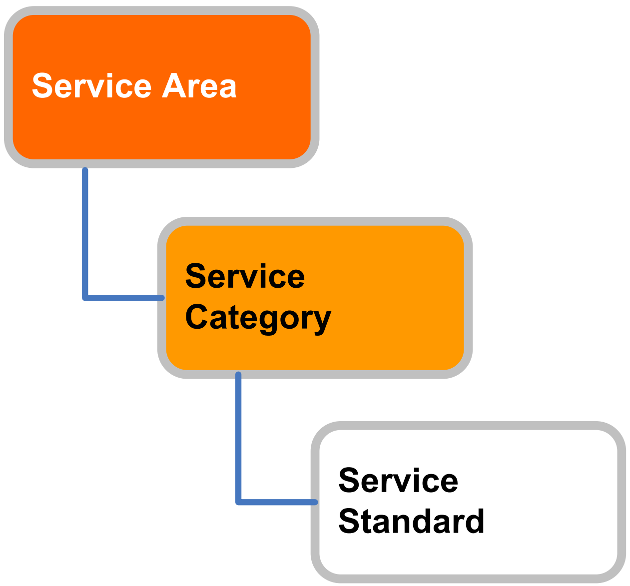
Security Architecture – FEA Framework – Service Component Reference Model (SRM)



- Service Domain: Customer Services, Process Automation, Business Management Services, Digital Asset Services, Business Analytical Services, Back Office Services, Support Services
- Service Type: Each service domain has a set of specified service types (e.g. Management of Process, Organizational Management, Investment Management, Supply Chain Management, etc.)
- Component: Each service type has a set of specified service components (e.g. Procurement.

Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

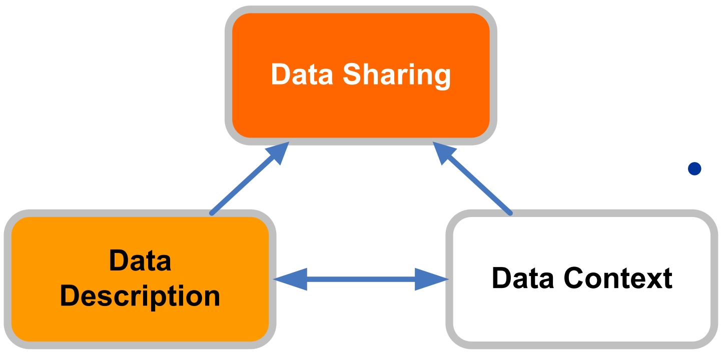
Security Architecture – FEA Framework – Technical Reference Model (TRM)



- Service Areas: Service Access and Delivery, Service Platform and Infrastructure, Component Framework, Service Interface and Integration.
- Service Category: Each service area has several identified service categories (e.g. Access Channels, Delivery Channels, Support Platforms, Delivery Servers, HW/SW, Security, Data Interchange, Management, etc.)
- Service Standard: Technologies that are identified as the Agency standards (e.g. FIPS 140-2, IEEE 802.11n, HTTP, TLS v1.0, etc.)

Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

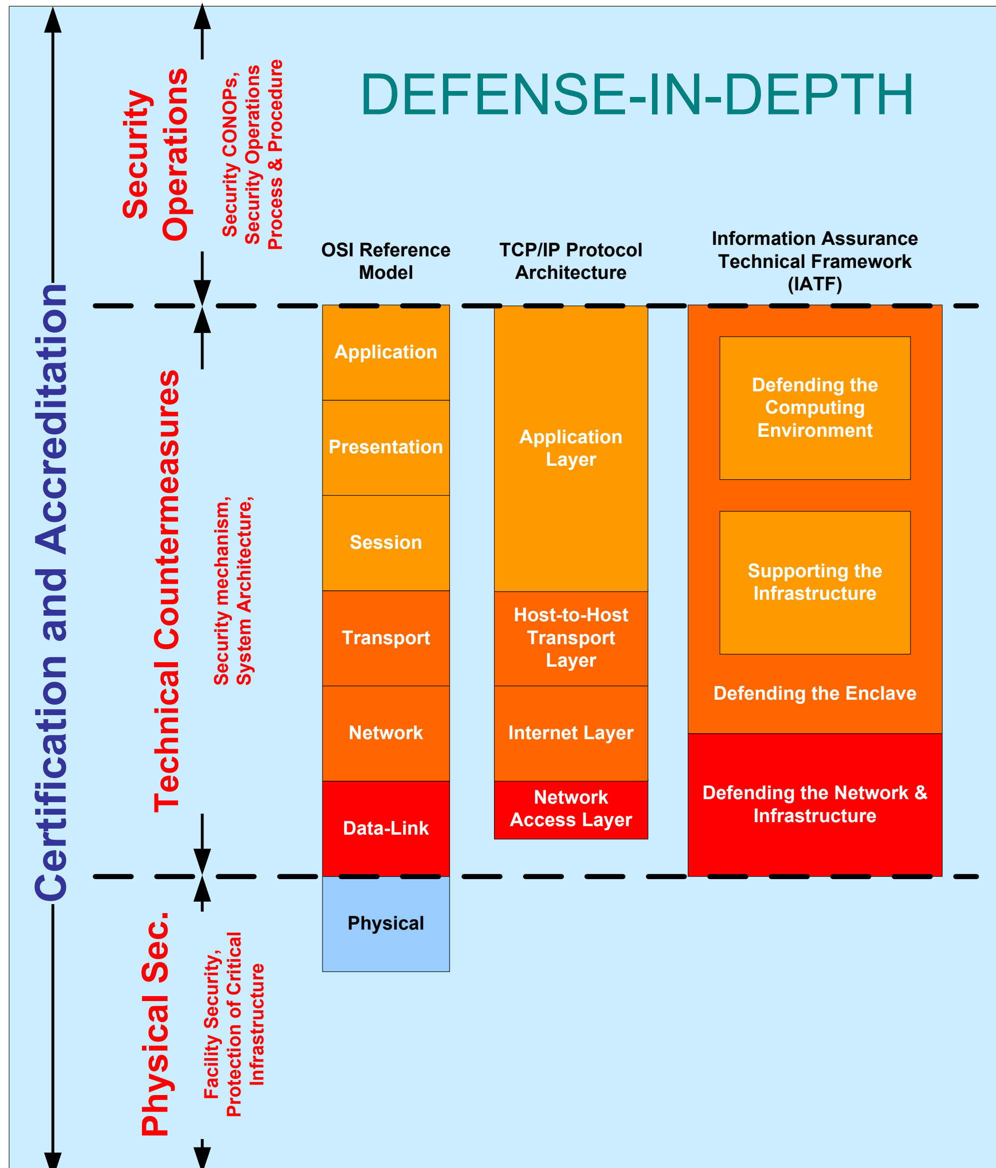
Security Architecture – FEA Framework – Data Reference Model (DRM)



- Data Description: Provides a means to uniformly describe data, thereby supporting its discovery and sharing
- Data Context: Facilitates discovery of data through an approach to the categorization of data according to taxonomies.
- Data Sharing: Supports the access and exchange of data where access consists of ad-hoc requests, and exchange consists of fixed, reoccurring transactions between parties. Enabled by capabilities provided by both the Data Context and Data Description standardization areas.

Reference: *FEA Consolidated Reference Model*, Version 2.3, October 2007

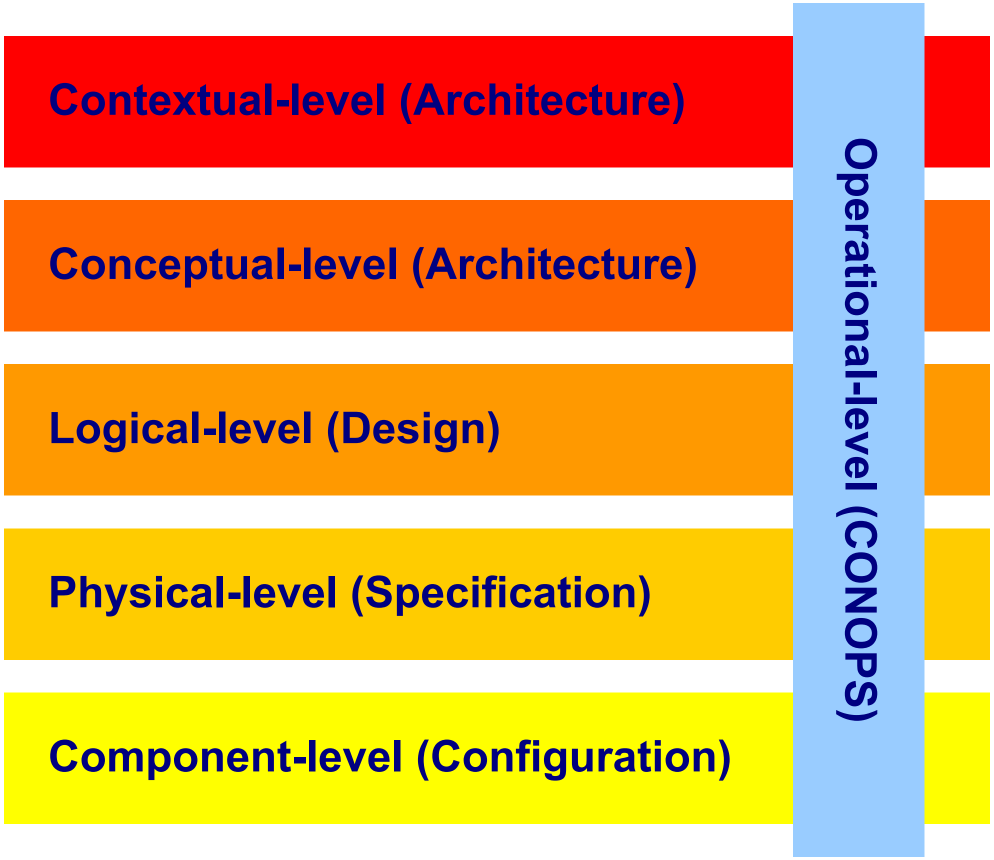
Allocate Security Services – Defense-in-Depth ...(1/2)



Reference: *IATF Release 3.1*

Allocate Security Services – Defense-in-Depth ...(2/2)

- A good Security Architecture should be able to explain security controls at:
  - Operations Layer
  - Contextual-level
  - Conceptual-level
  - Logical-level
  - Physical-level
  - Component-level



System Requirements

System Requirements

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

Performance Requirements
For establishing confidence that the specified function will perform as intended.

- Functional Requirements

  Example:

  The information system shall support the FISMA reporting, mandated by OMB, in the following format :

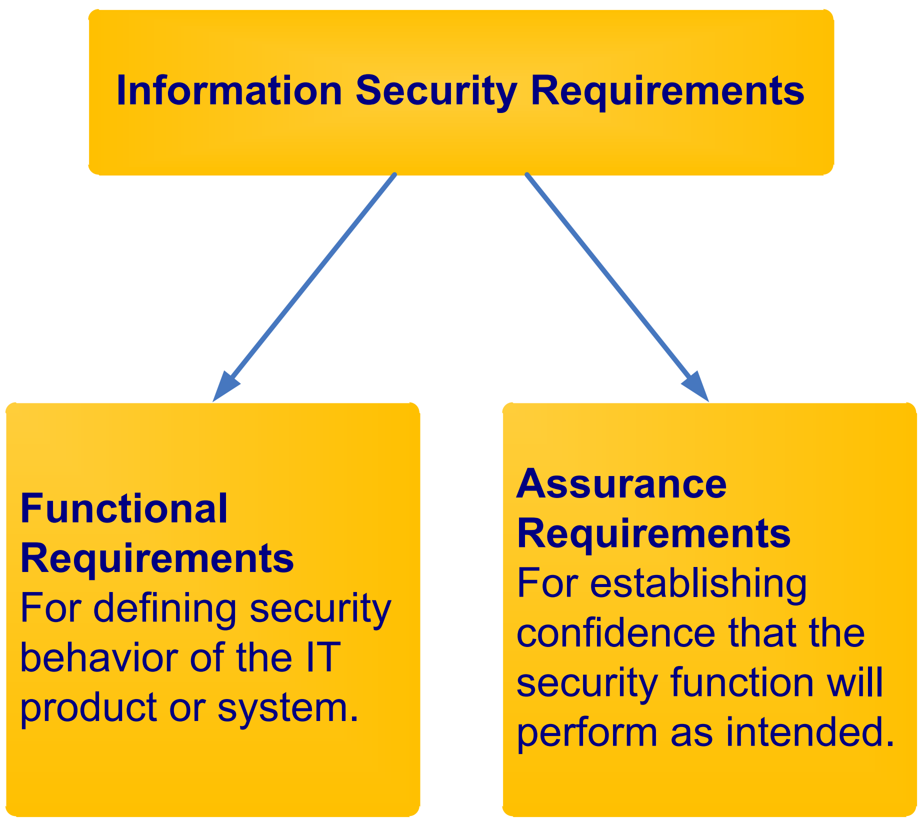
  - The number of information systems by FIPS 199 security categories.
  - The number of systems for which security controls have been tested and evaluated in the past year.

- Performance Requirements

  Example:

  What extent the agency-wide security configuration policy (i.e., NIST Checklist Program [a.k.a. National Checklist Program]) has been implemented.

Information Security Requirements



- 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).

Security Controls

Security controls are the management, operational, and technical safeguards/countermeasures prescribed for information systems or organizations that are designed to:

1. protect the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those systems/ organizations; and
2. Satisfy a set of defined security requirement.

Key questions:

– What security controls are needed to satisfy the security requirements and to adequately mitigate risk incurred by using information and informaiton systems in the execution of organizational missions and business functions?

– Have the security controls been implemented, or is there an implementation plan in place?

– What is the desired or required level of assurance that the selected security controls, as implemented are effective in their application?

Reference: NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

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.

Categories of Security Controls …(2/4)

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
	Planning	PL
	System and Services Acquisition	SA
	Certification, Accreditation, and Security Assessment	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*

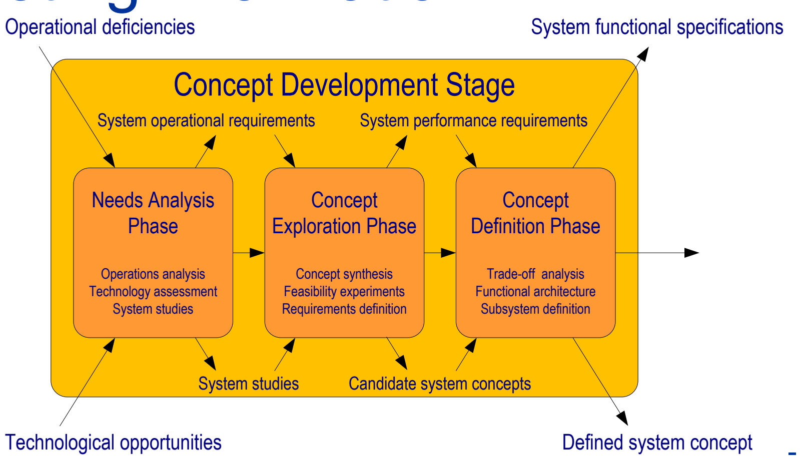
Categories of Security Controls …(3/4)

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

Implementable & Testable Security Requirements …(4/4)

- Assurance requirements are generic; they define information protection needs. For example:
  - From SP 800-53: *SC-6: Resource Priority. The information system limits the use of resources by priority.*
  - From ISO 27001: *A.10.3.1: Capacity Management. The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system*.
- Functional requirements defines "what & how" the system shall perform in meeting information protection needs.
  - Generated through system engineering process



Reference: _Systems Engineering Principles and Practice_, A. Kossiakoff, W. Sweet, S. Seymour, S. Biemer, 2011.

Questions:

- What architecture framework is best for defining the relationship between business investment and system components?
  -
- What architecture framework is designed for defining the IT enterprise systems?
  -
- What architecture framework is designed specifically for U.S. Department of Defense?
  -

Answers:

- What architecture framework is best for defining the relationship between business investment and system components?
  - Federal Enterprise Architecture (FEA) Framework
- What architecture framework is designed for defining the IT enterprise systems?
  - Zachman Enterprise Architecture Framework
- What architecture framework is designed specifically for U.S. Department of Defense?
  - DoD Architecture Framework

Validation Time… ☺

1. Class Exercise

2. Review Answers

Exercise #1: Security Models

1. Discuss & provide example implementations for the Bell-LaPadula security model?

- How is a high assurance guard (HAG) related to the Bell-LaPadula security model?

2. Discuss & provide example implementations for the Clark-Wilson security model?

- How is an internet proxy server related to the Clark-Wilson security model?

Exercise #2: Security Requirements & System Architecture

1. Discuss how is NIST SP 800-53 or ISO 27001 specified security controls are…
- Related to system functional requirements?
- Related to system architecture & detailed design?

2. Discuss how are functional requirements relate to STIGs, CIS Benchmarks, or FDCC security settings?