

Unit #2

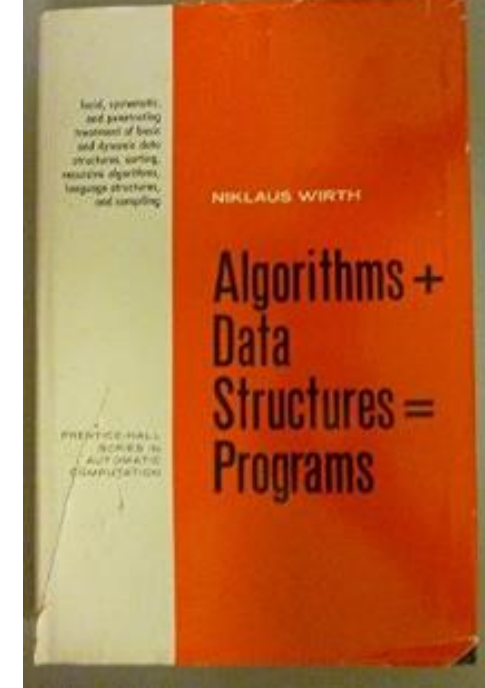
MIS5214 – Security Architecture

Agenda

- Information Systems – some definitions
- Conceptual models of information systems
- NIST Risk Management Framework
- FIPS 199 Security Categorization
- Transforming qualitative risk assessment into quantitative risk assessment
- FedRAMP System Security Plan – overview
 - NIST 800-53 Security controls
 - Role of FIPS 199 in selecting a security control baseline
 - NIST 800-18 classification of security control families

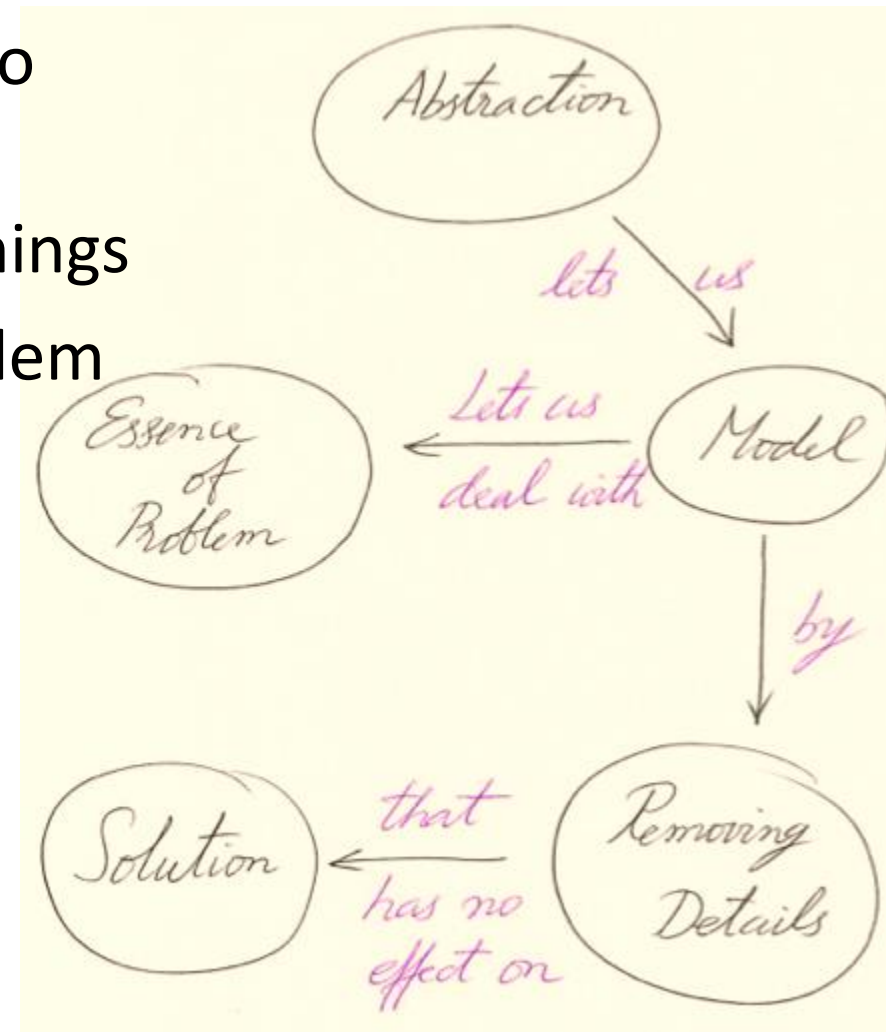
Information Systems – some definitions

- **Data Structure** is a particular way of organizing data in a computer so that it can be manipulated by an algorithm
- **Algorithm** is a step-by-step procedure in a computer program for solving a problem or accomplishing a goal
- **Programs** = Algorithms + Data Structures
- **Software** are programs used to direct the operation of a computer
- **Hardware** are tangible physical parts of a computer system and IT network
- **Firmware** is software embedded in a piece of hardware
- **Information systems** are software and hardware systems that support data-intensive applications
- **Enterprise information system** is an information system which enable an organization to integrate and improve its business functions



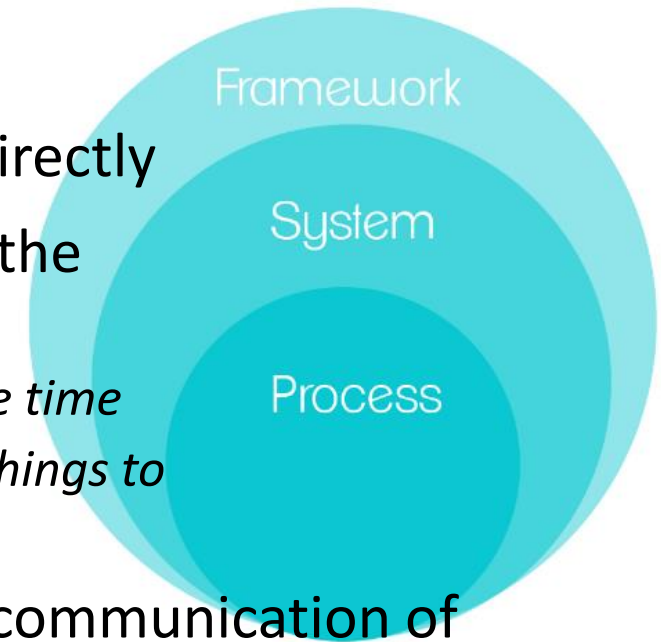
What is meant by the term “abstraction” ?

- A fundamental human capability that enables us to deal with complexity
- Its purpose is to limit the universe so we can do things
- Selective examination of certain aspects of a problem
- Its goal is the purposeful isolation of important aspects and suppression of unimportant aspects (i.e. omitting details)
 - *Purpose determines what is and what is not important*
 - *All abstractions are incomplete and inaccurate – but this is their power and does not limit their usefulness*
- Many different abstractions of the same thing are possible
 - *Depending on the purpose for which they are made – The problem solving context explains the source of their intent*



What is a conceptual model ?

- Are abstractions of things for the purpose of understanding them
- Enable dealing with systems that are too complex to understand directly
- Omit nonessential details making them easier to manipulate than the original entities
 - *The human mind can cope with only a limited amount of information at one time*
 - *Models reduce complexity by separating out a small number of important things to deal with at a time*
- Aid understanding complex systems by enabling visualization and communication of different aspects expressed as individual models (“views”) using precise notations
 - Communicate an understanding of content, organization and function of a system
 - Useful for verifying that the system meets requirements
 - *To be relied on, models must be validated by comparison to the implemented system to assure they accurately represent and document the implemented system*
- Serve several purposes
 - Testing a physical entity before building it
 - Communicating a shared understanding of the system with stakeholders, users, developers, information system auditors and testers



Models help us understand Information Systems... and how to defend them...

Models are ways to describe reality

Model quality depends on skill of model designers and qualities of the selected model

Building blocks of models is a small collection of abstraction mechanisms

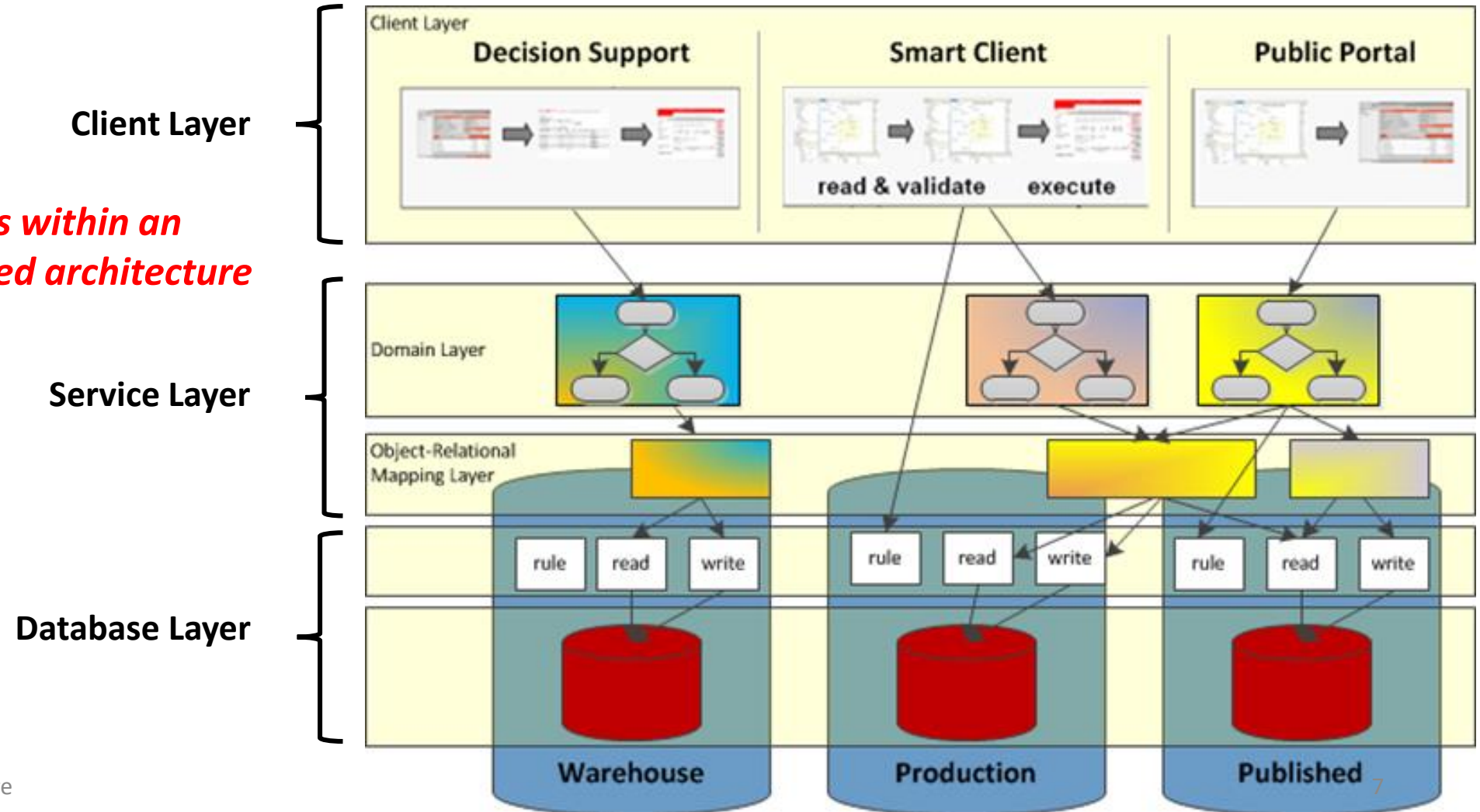
- Classification
- Aggregation
- Generalization
- *Can you think of any others?*

Abstractions help the designer understand, classify, and model reality

Classification

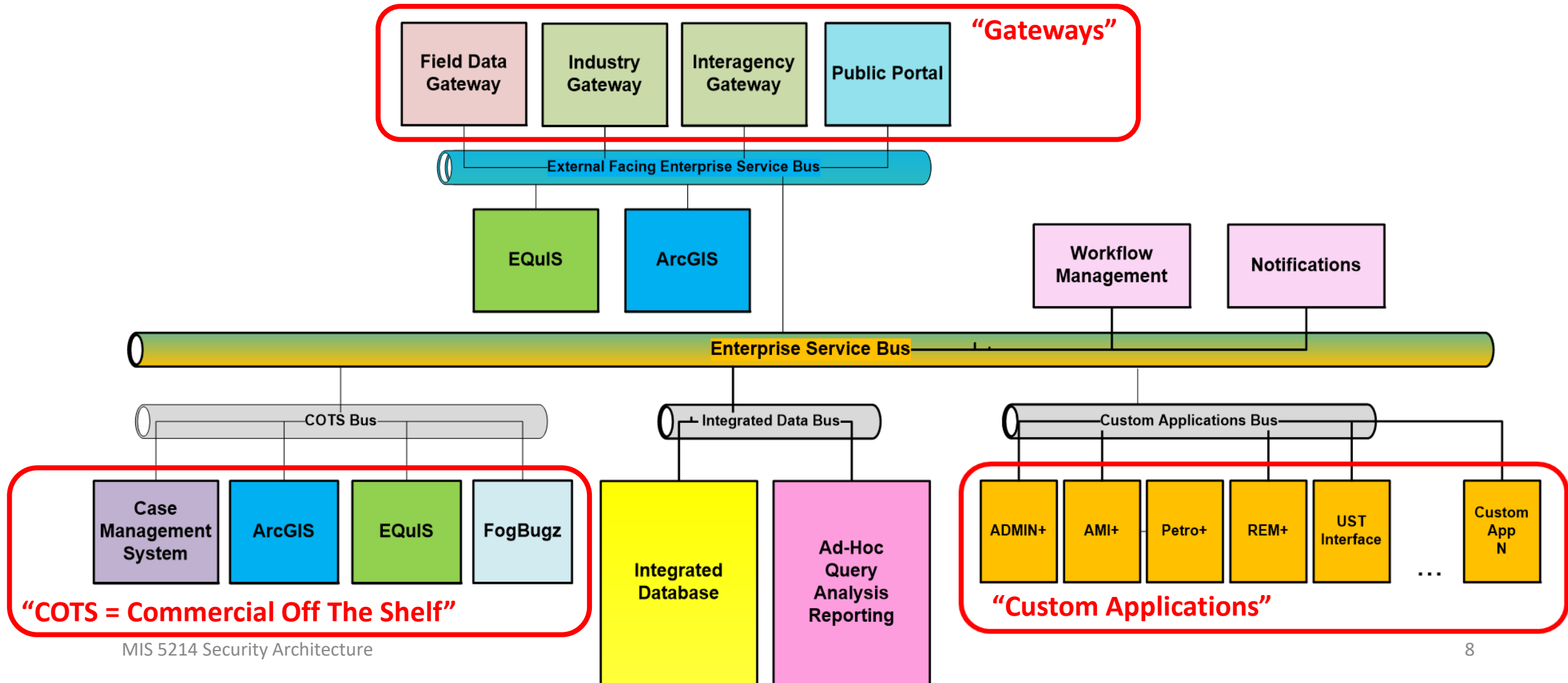
- An abstraction used to define one concept as a class of real-world objects characterized by common properties

Classes of software types within an enterprise service oriented architecture



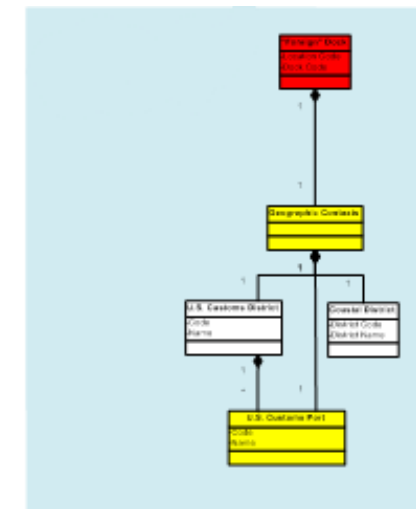
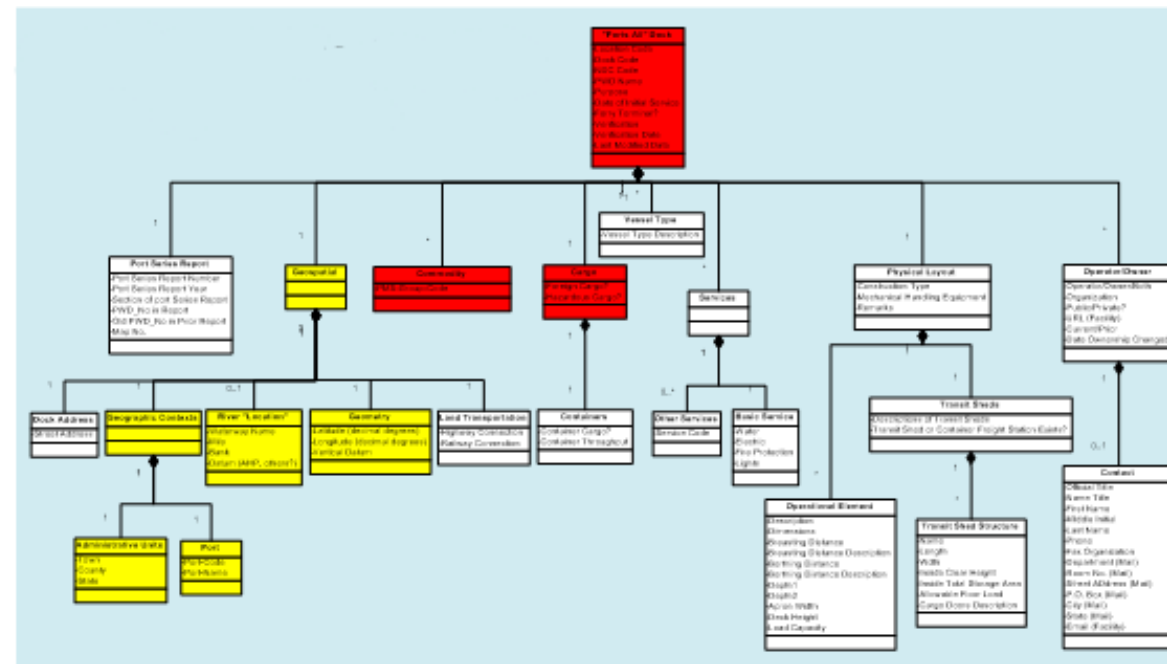
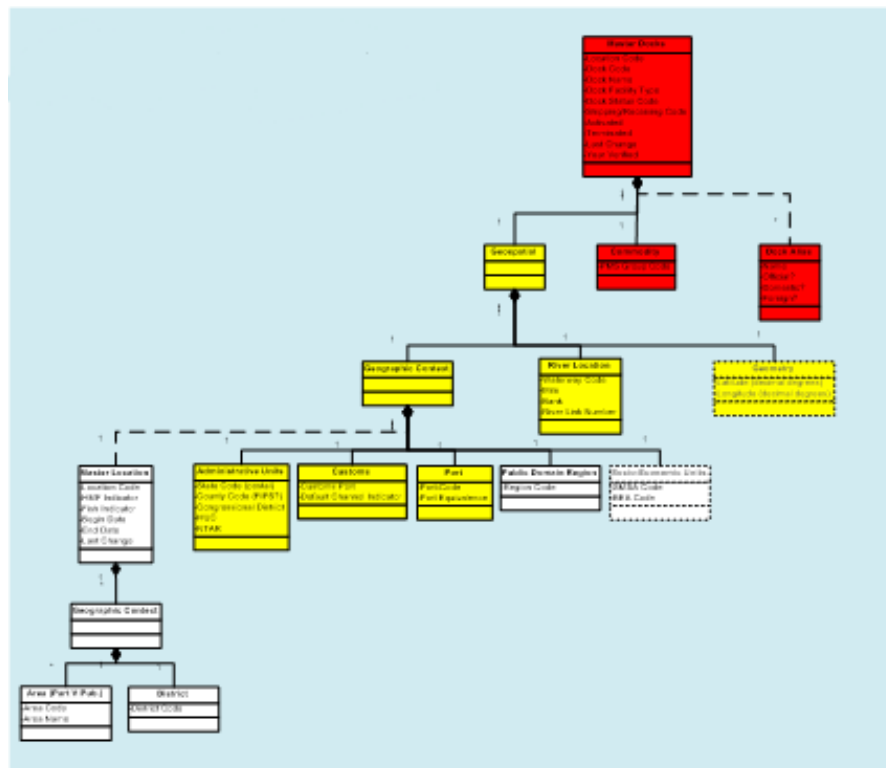
Aggregation

An aggregation abstraction defines a new composite class from a set of other classes that represent its components

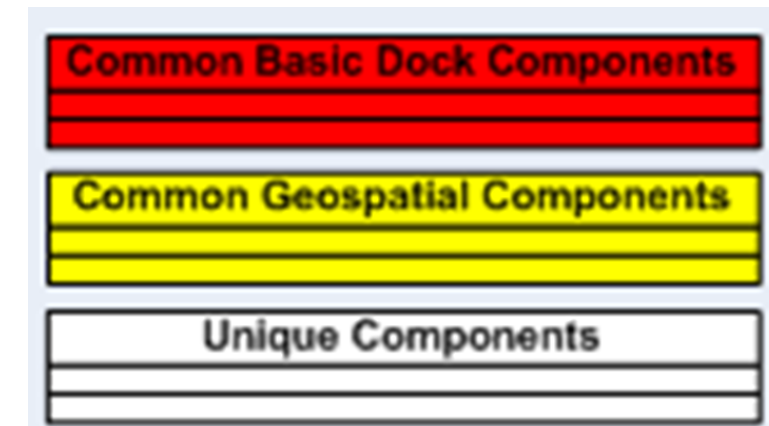


Classification and Aggregation

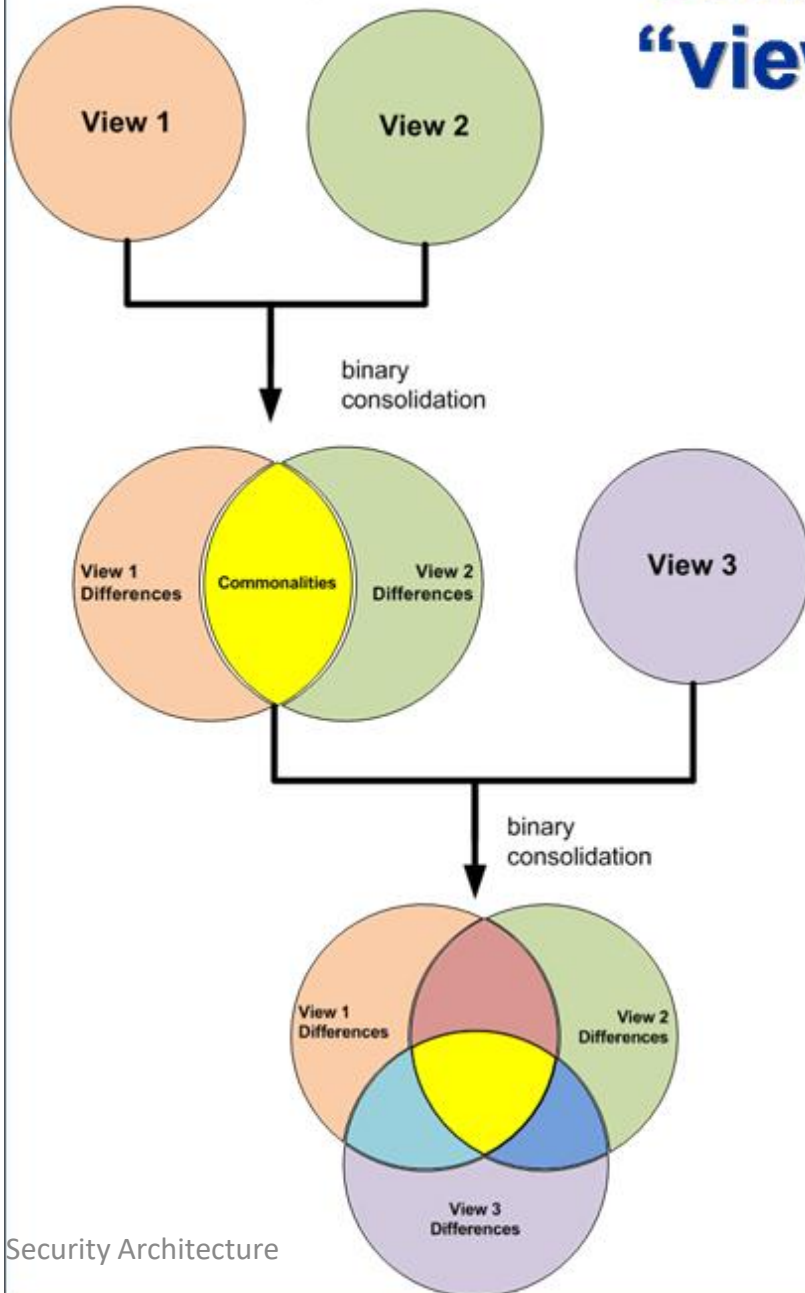
- Are the two basic abstractions used for
 - Building data structures within databases and conventional programming languages
 - Building and organizing computational processes within applications
 - Building and organizing applications within systems
 - Building and organizing minor systems and applications within major systems



Information models from disparate business units



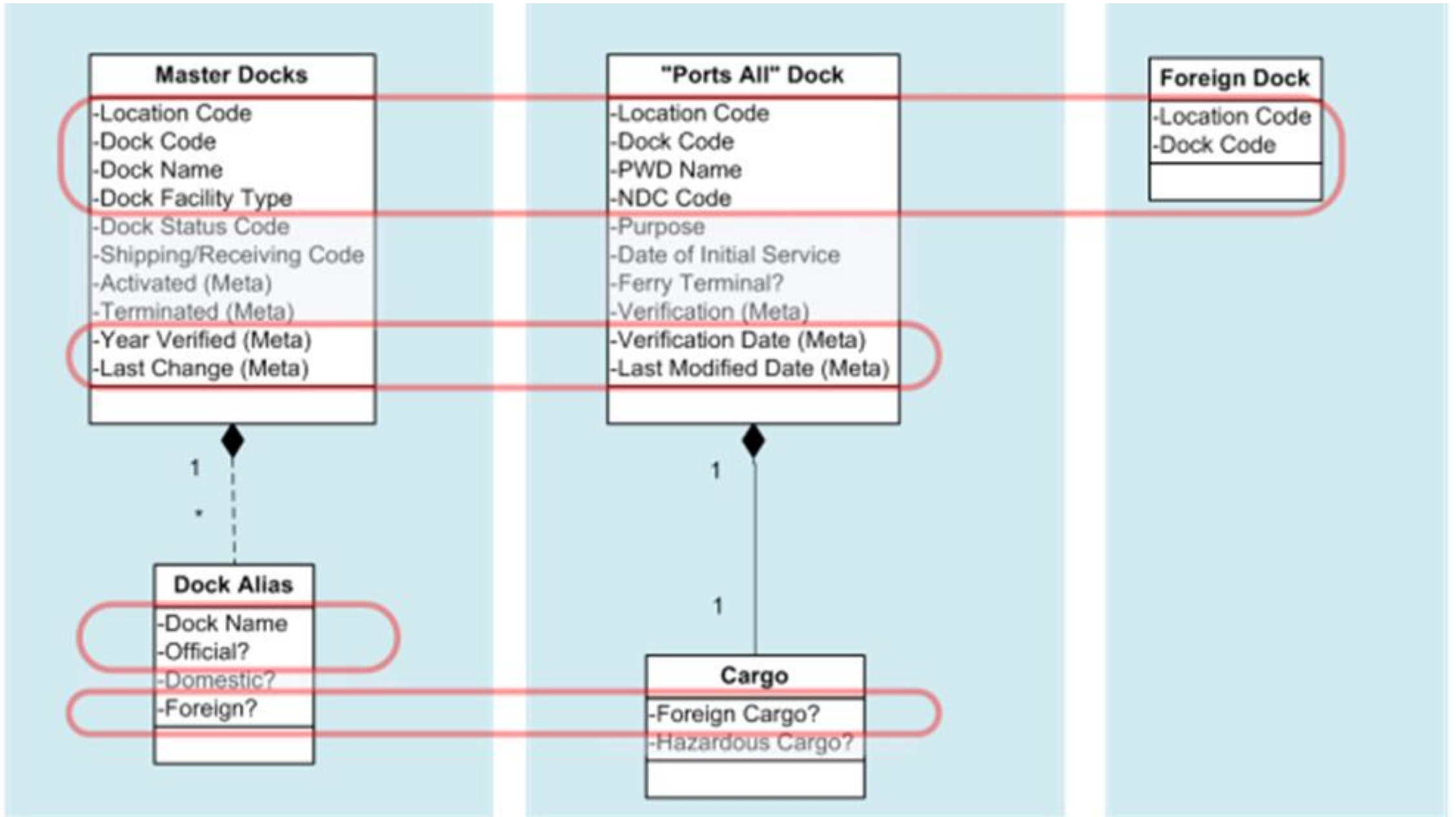
consolidation methodology “view integration”

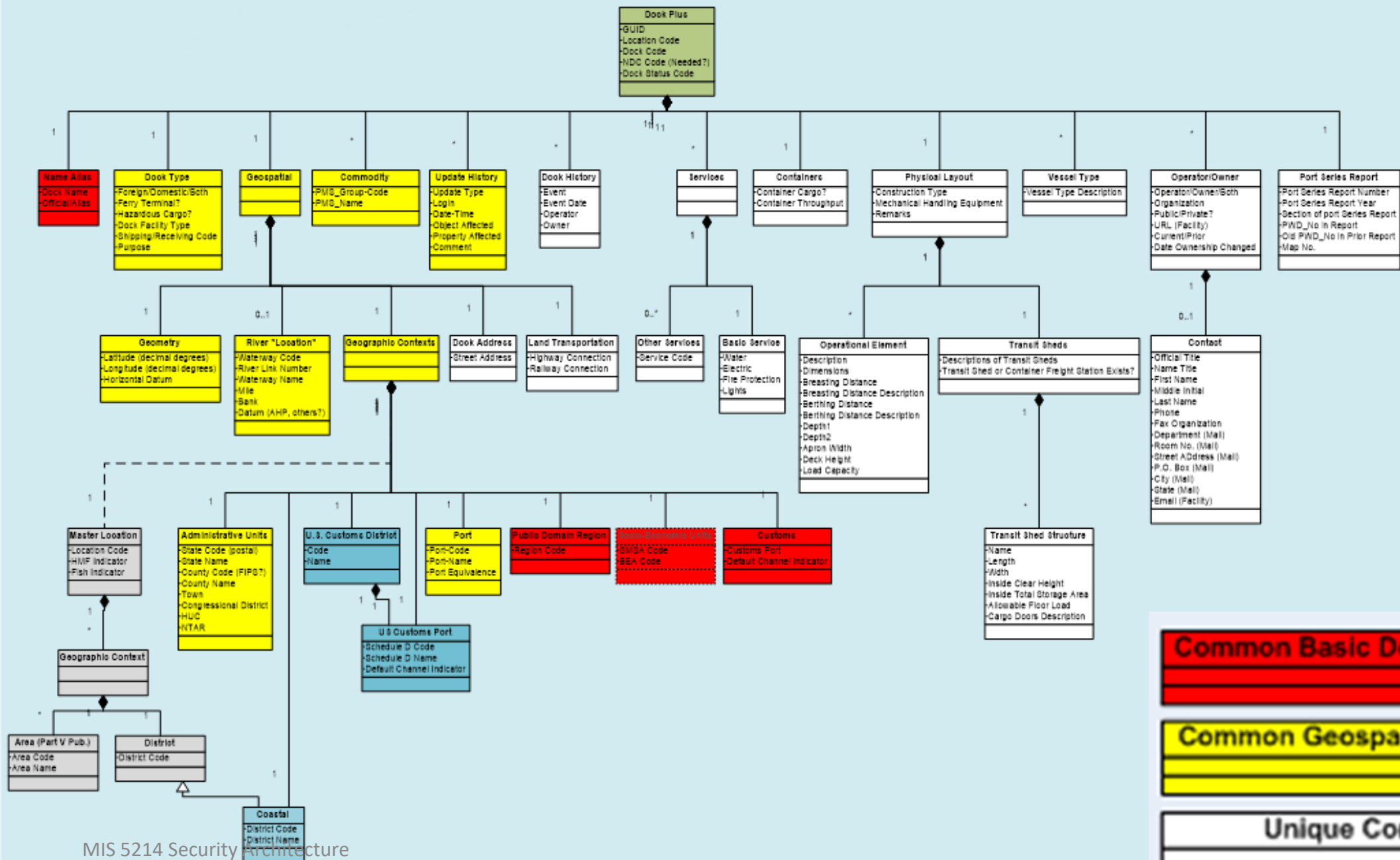


model integration achieved by:

1. Identifying,
2. Resolving, and
3. Consolidating

- **Commonalities** (and synonyms)
- and
- **Differences** (and homonyms)





Common Basic Dock Components

Common Geospatial Components

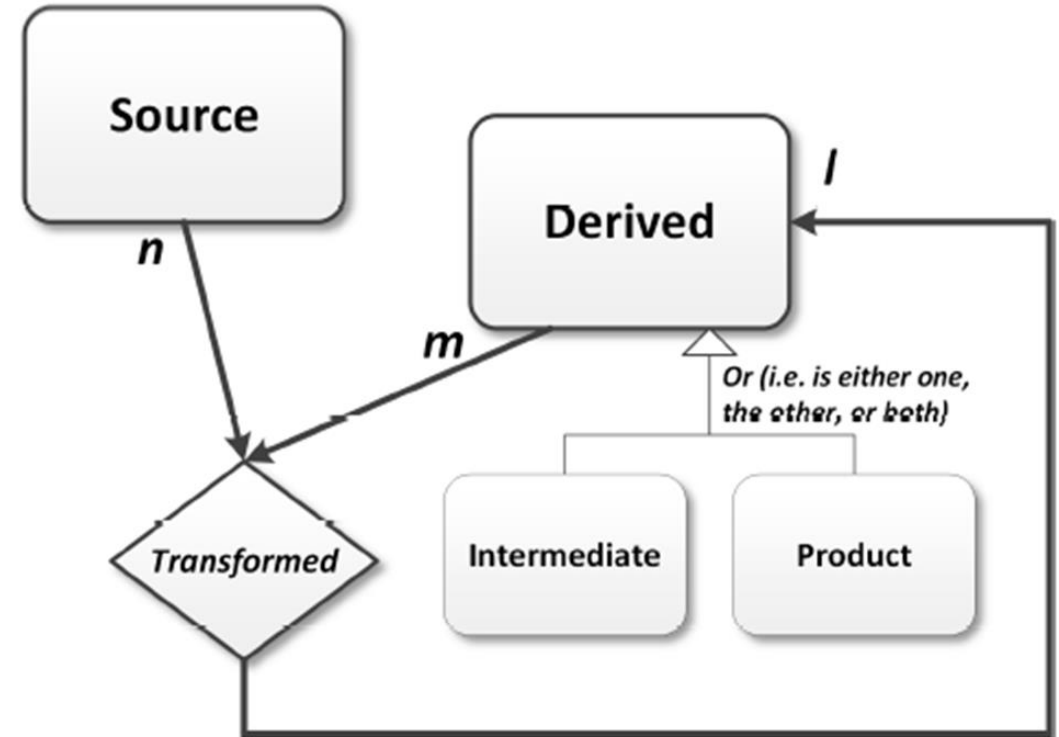
Unique Components

Generalization

- A generalization abstraction defines a subset relationship between elements of two more classes
- In generalization, all the abstractions defined for the generic class (super-class) are inherited by all the subset classes (sub-class)

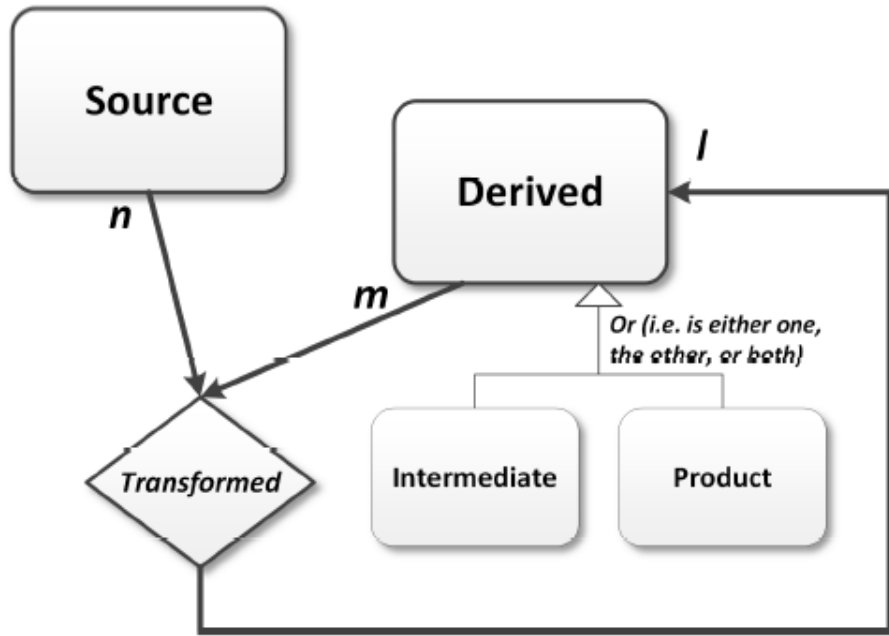
$Datasets = \{Dataset_i : i = source, derived\},$

$Dataset_{derived} = \{Dataset_{derived.k} : k = intermediate, product\}.$

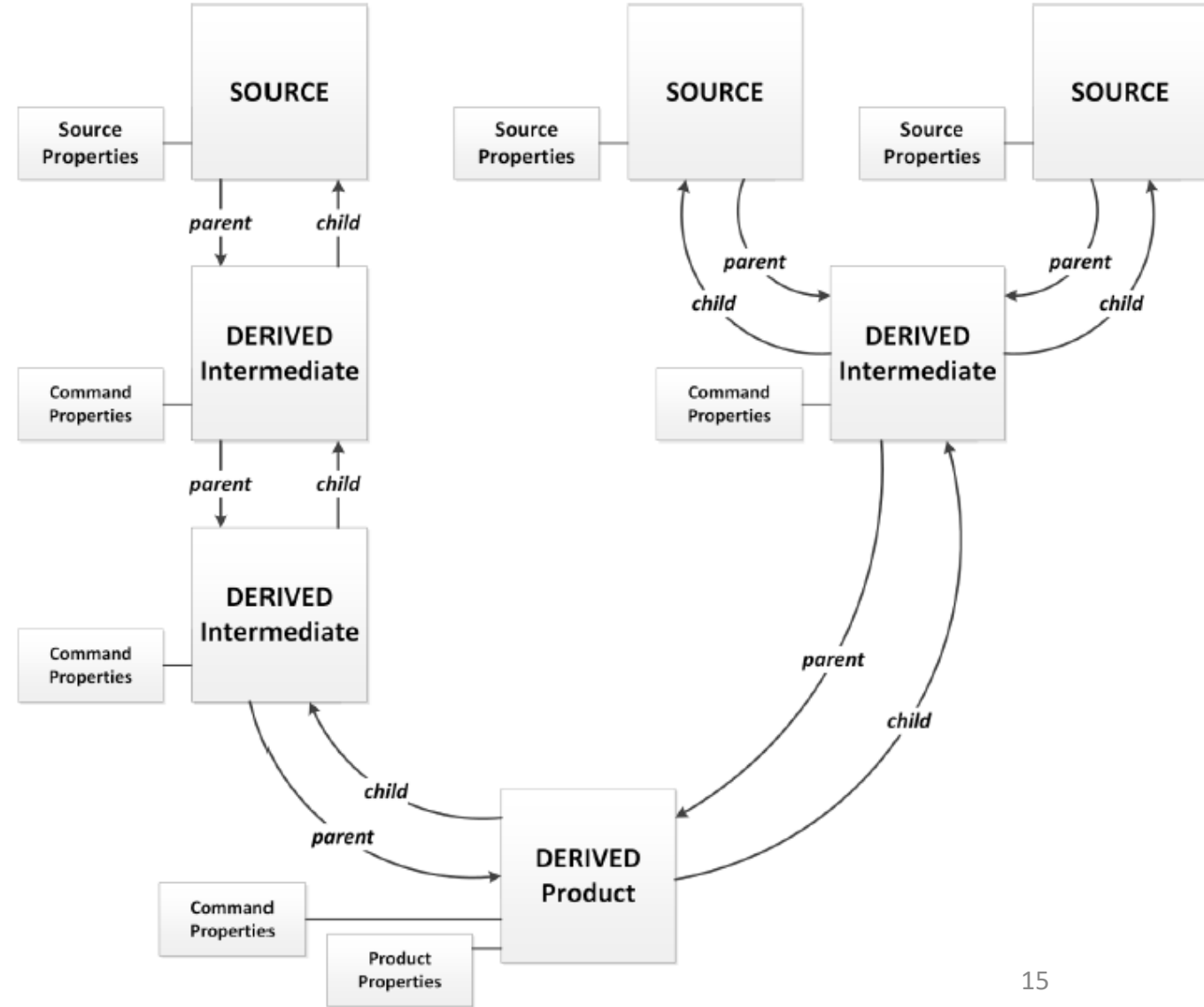


Data lineage metadata model

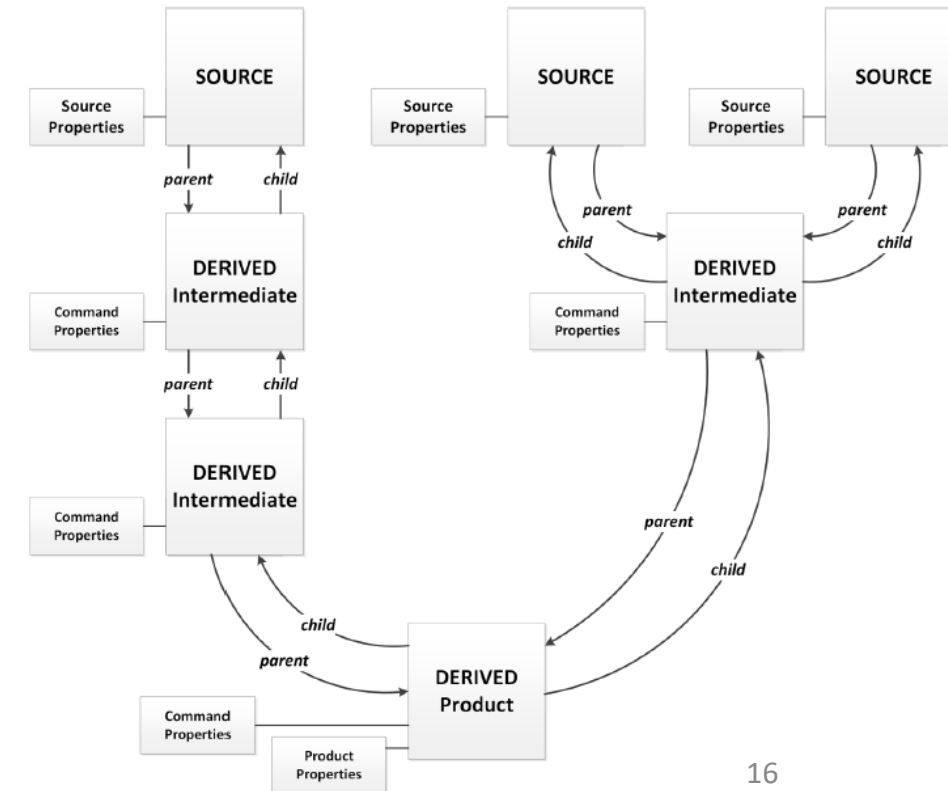
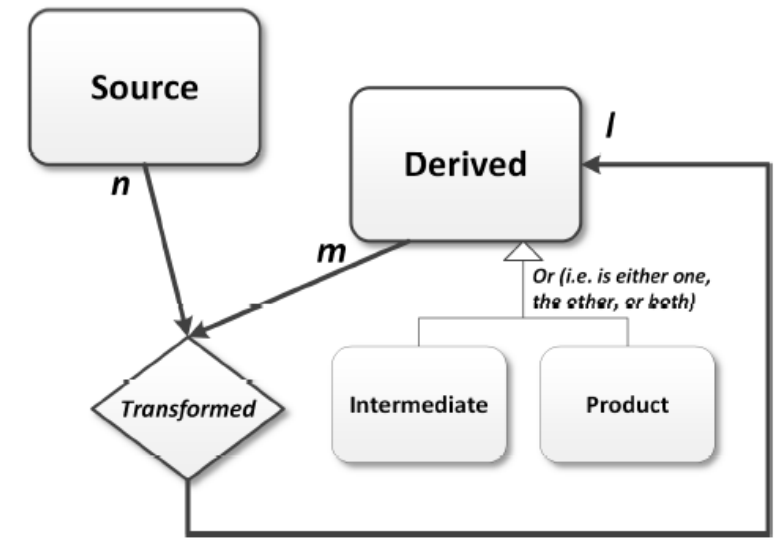
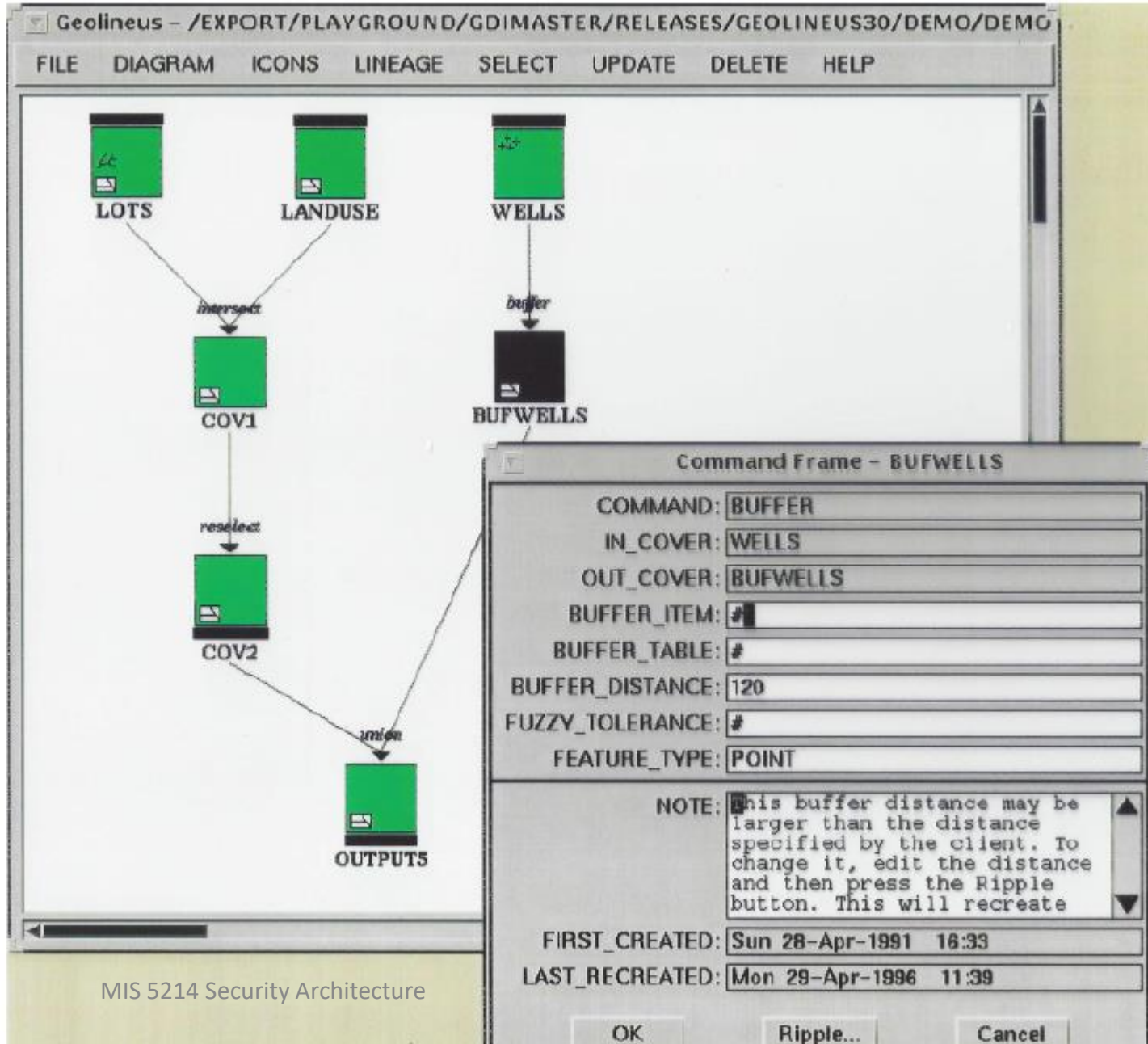
Generalization enables partitioning objects and structuring common properties and methods



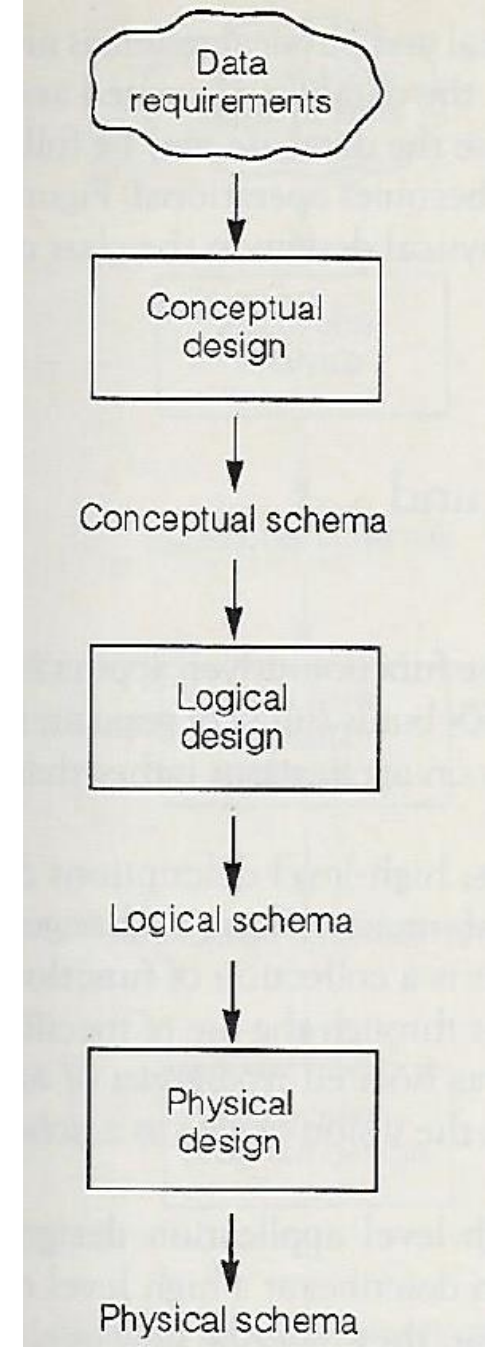
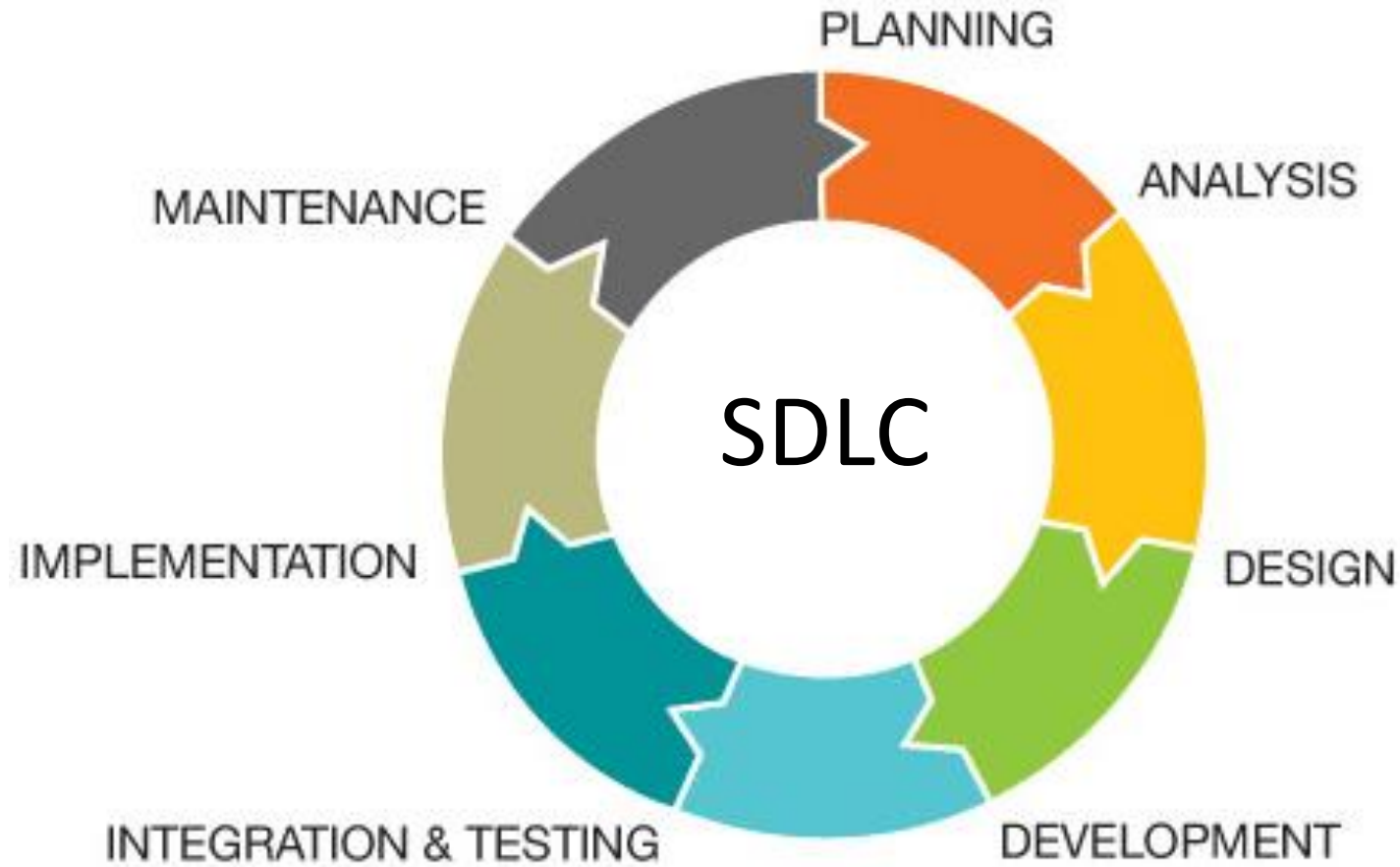
Example of generalizations of different types of datasets



Data Lineage Metadata System

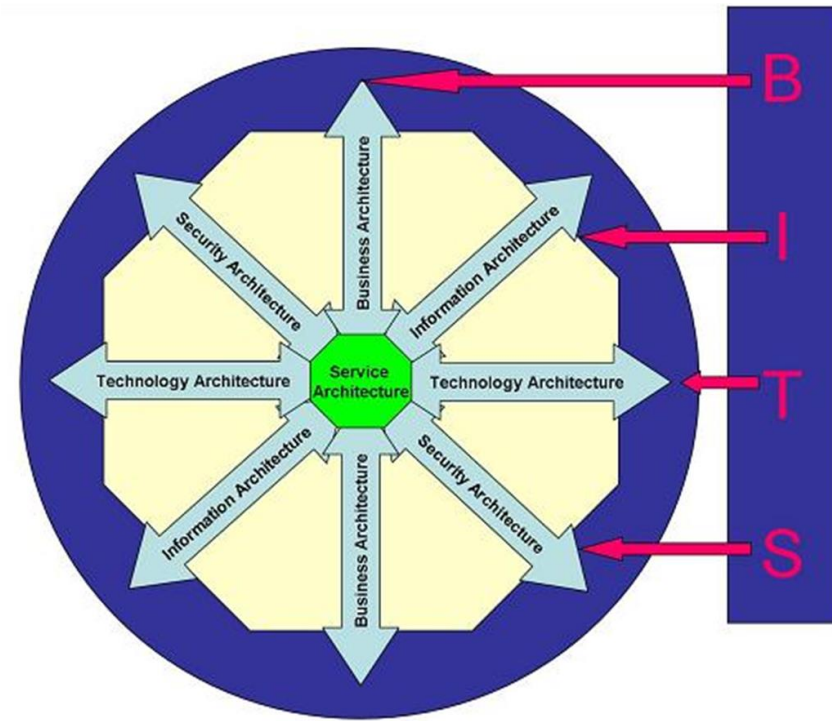


Conceptual models of information system design and development...



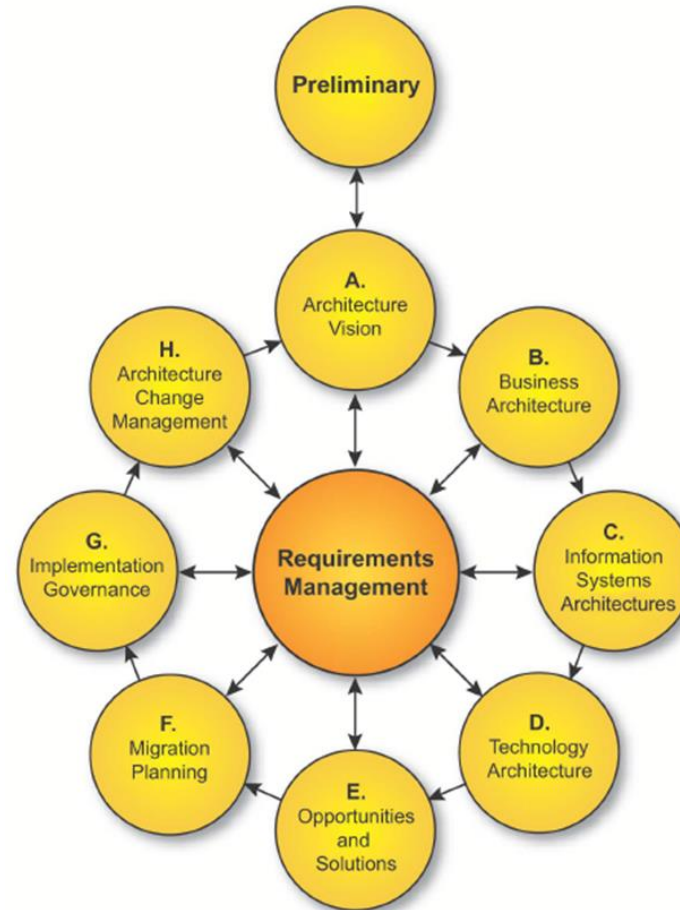
Database design¹⁷

Models help us understand enterprise information systems and their security



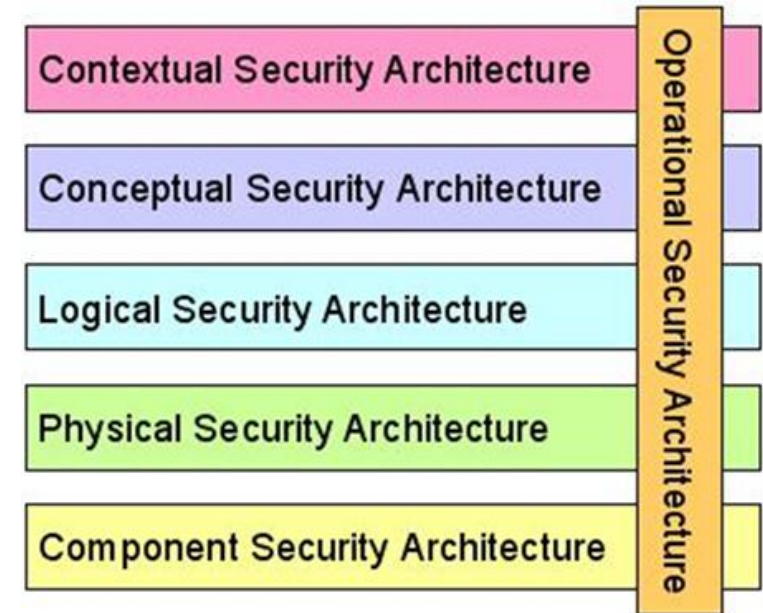
Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise_information_systems_security_architecture



The Open Data Group Architecture Framework (TOGAF) Version 9.1

<https://www.opengroup.org/architecture/togaf91/downloads.htm>



Sherwood Applied Business Security Architecture

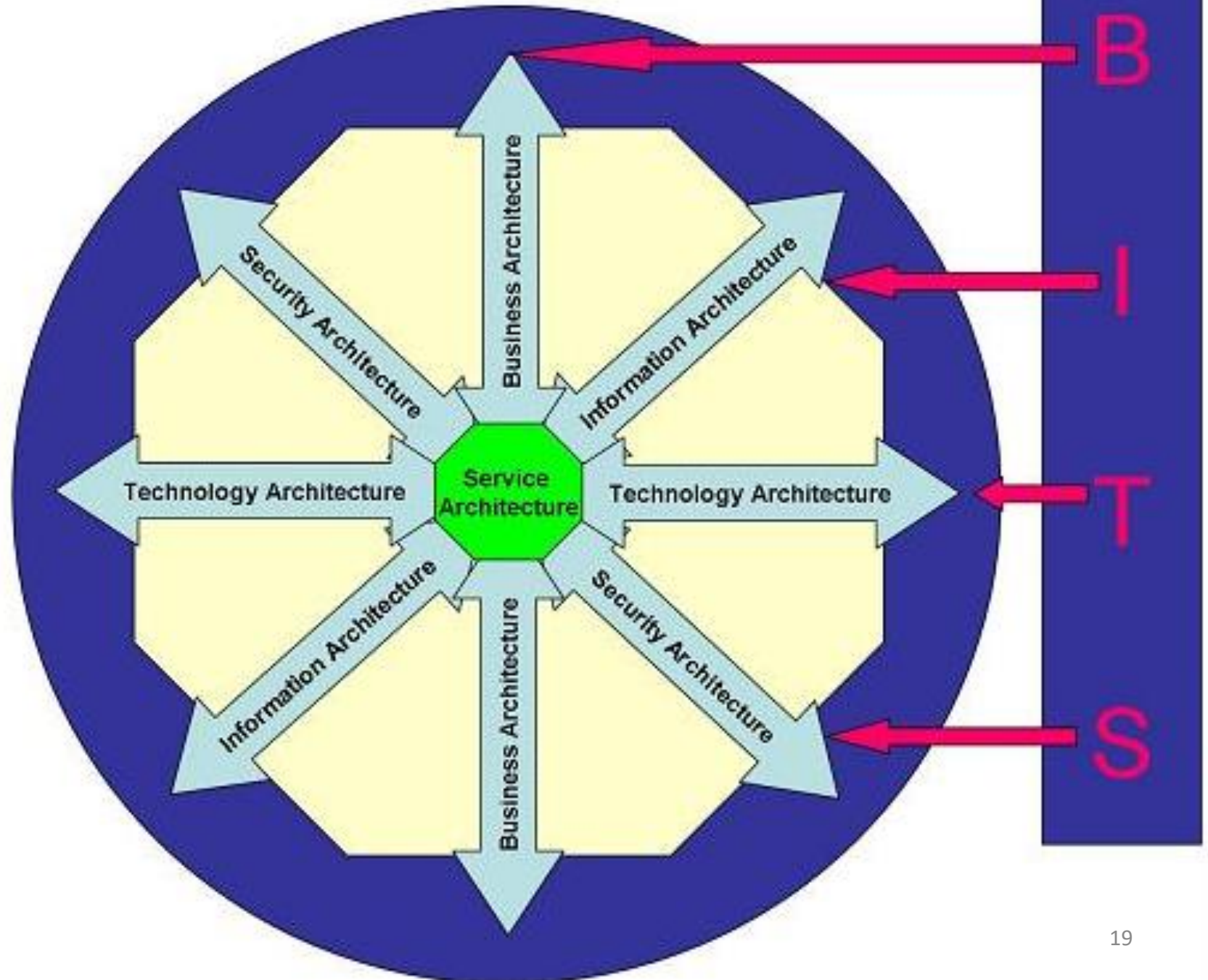
http://www.sabsa.org/white_paper

Enterprise architecture consists of:

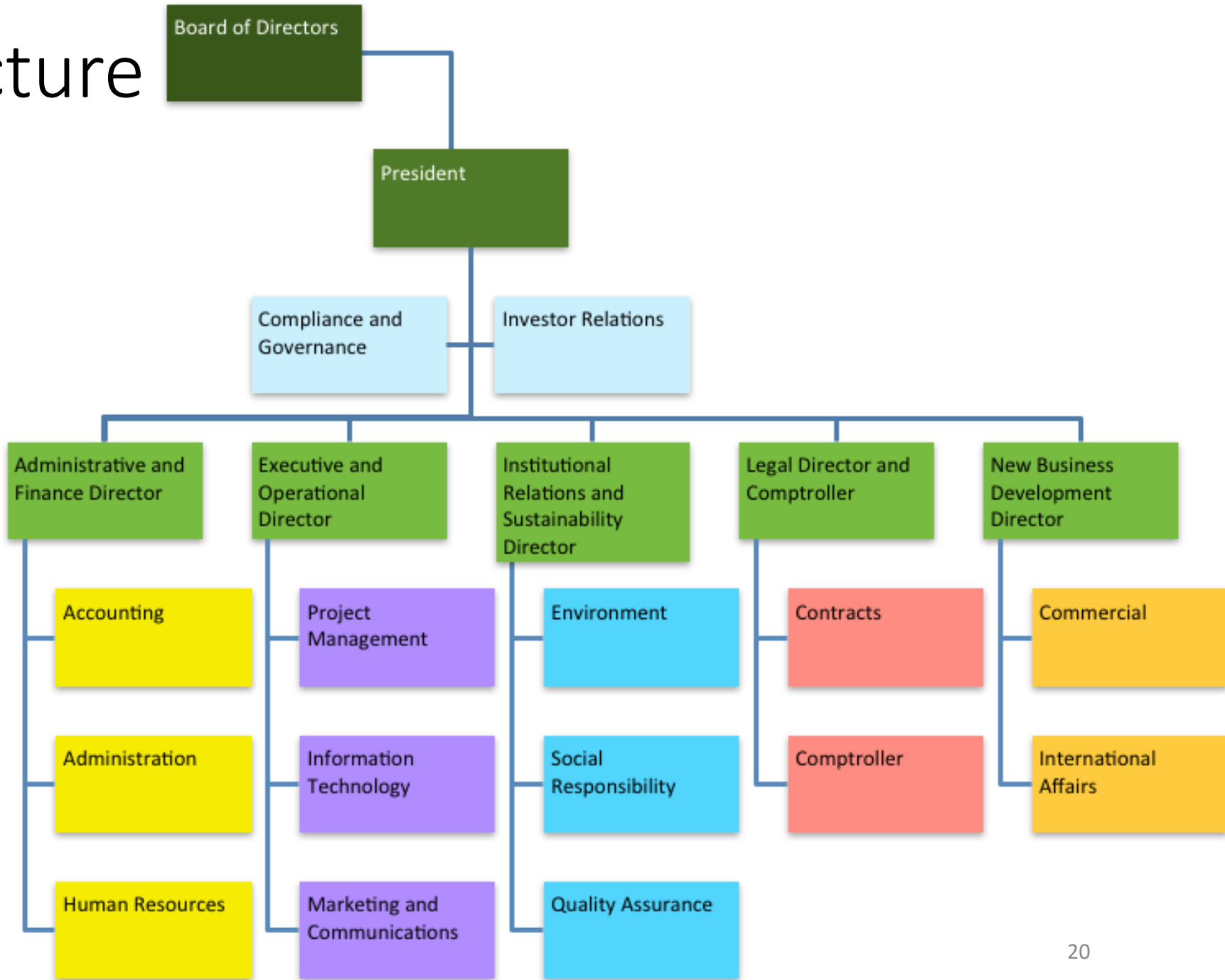
- Business Architecture
- Information Architecture
- Technology Architecture
- Security Architecture

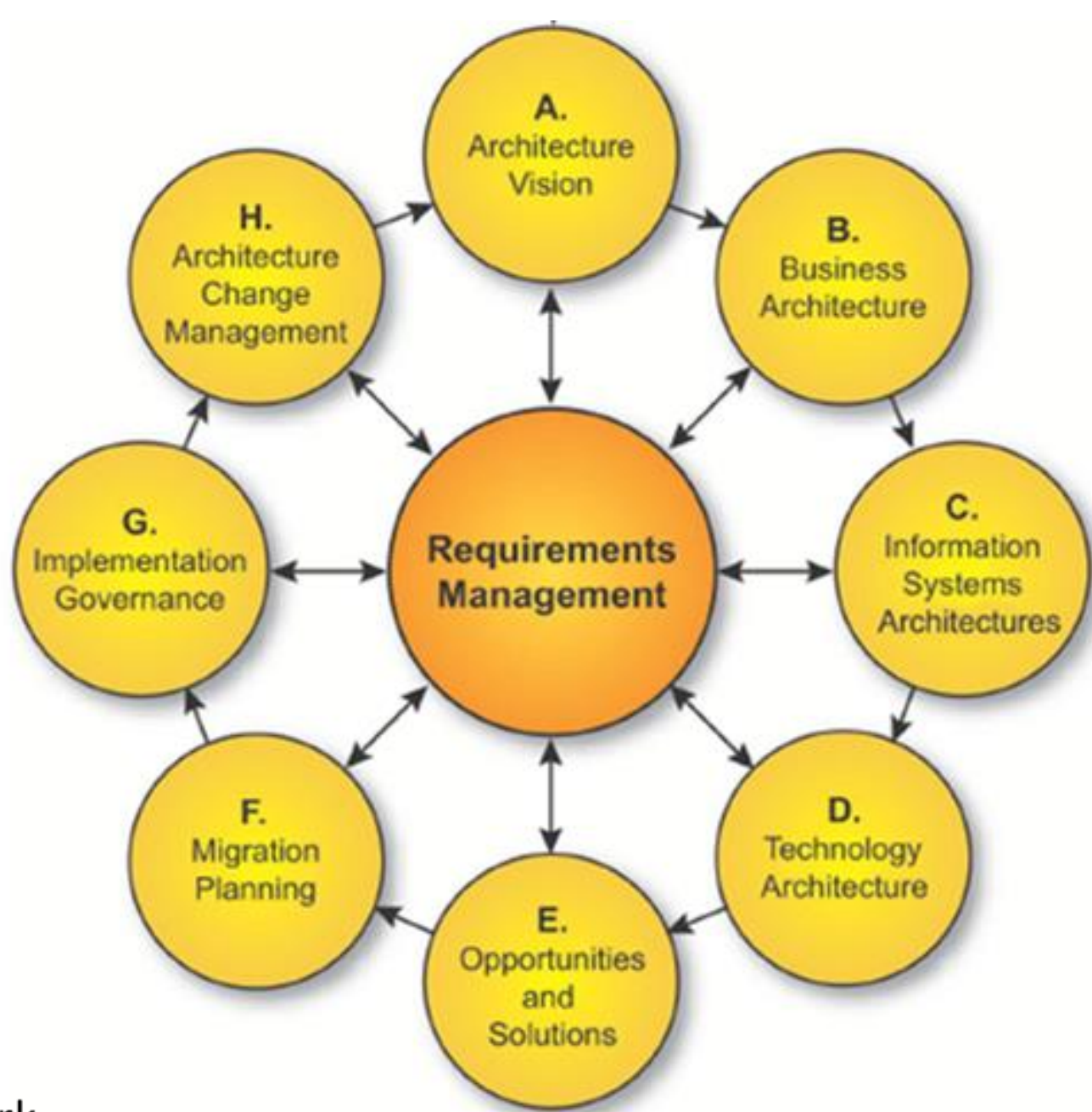
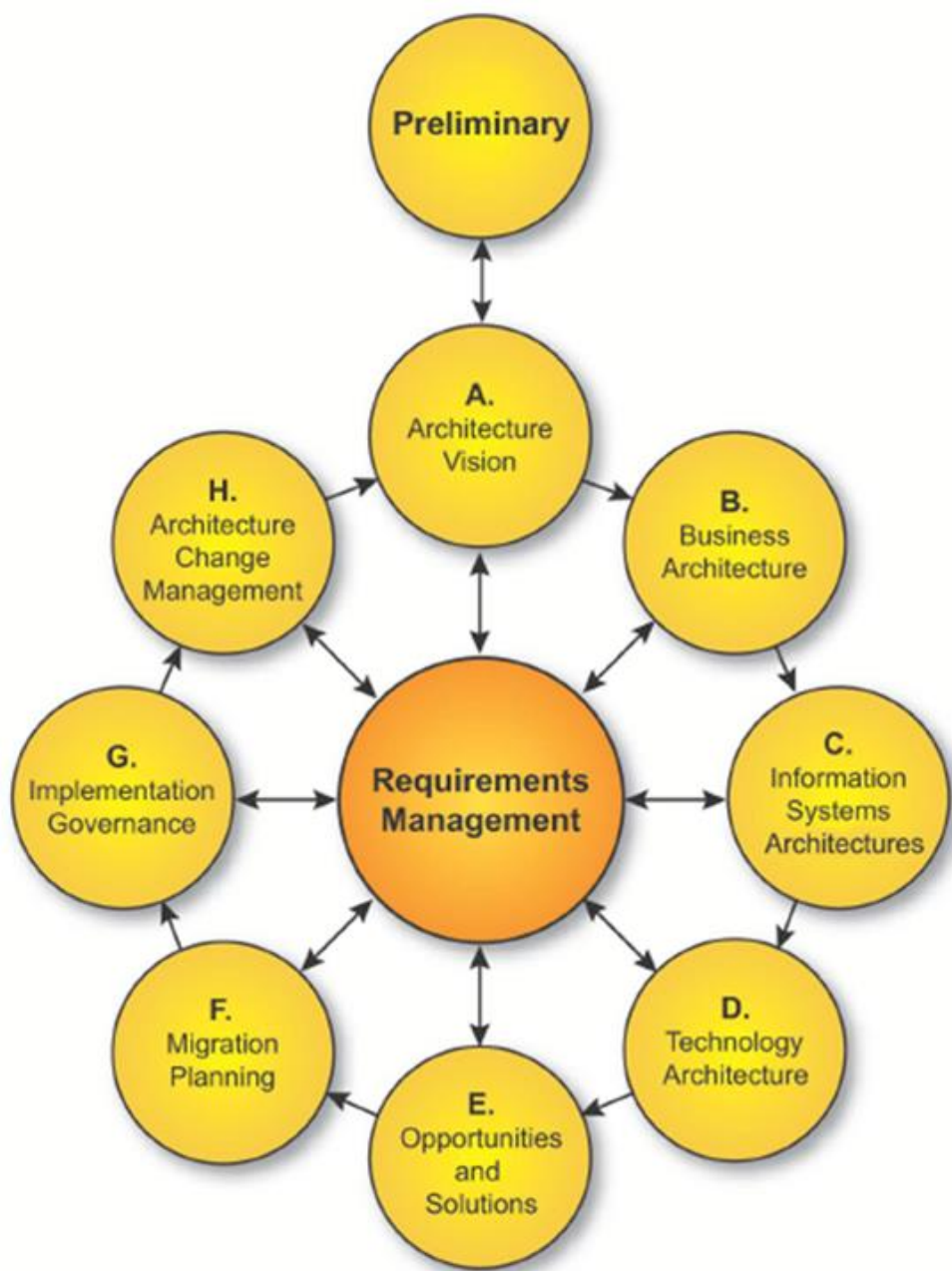
Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise_information_security_architecture



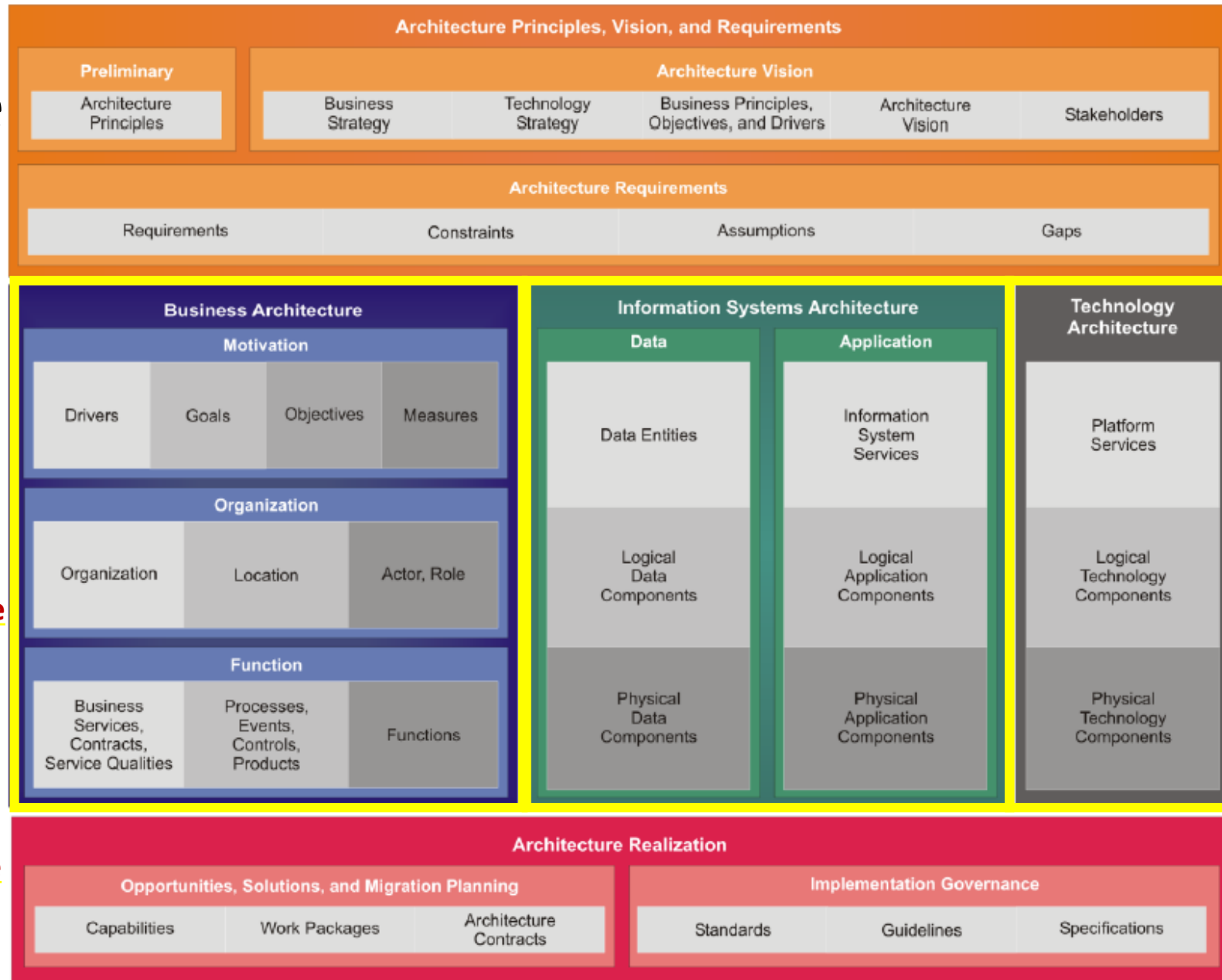
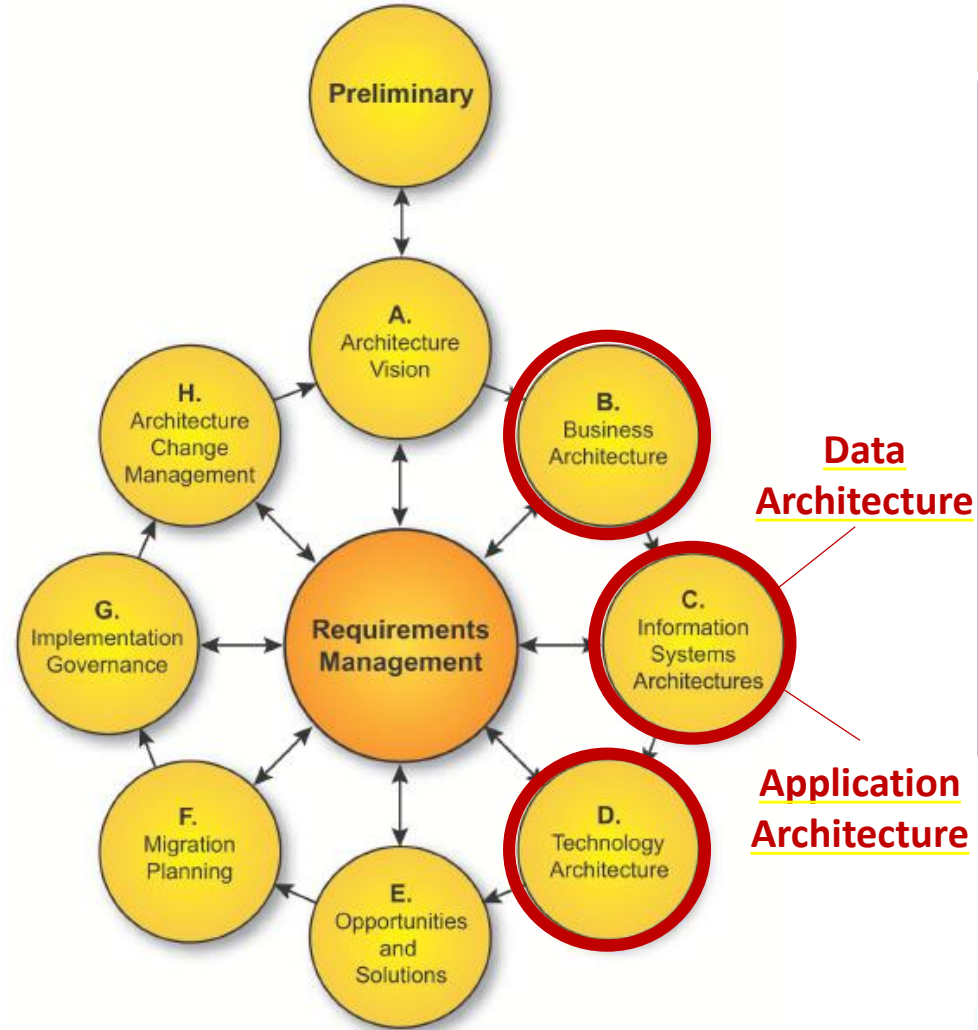
Business Architecture





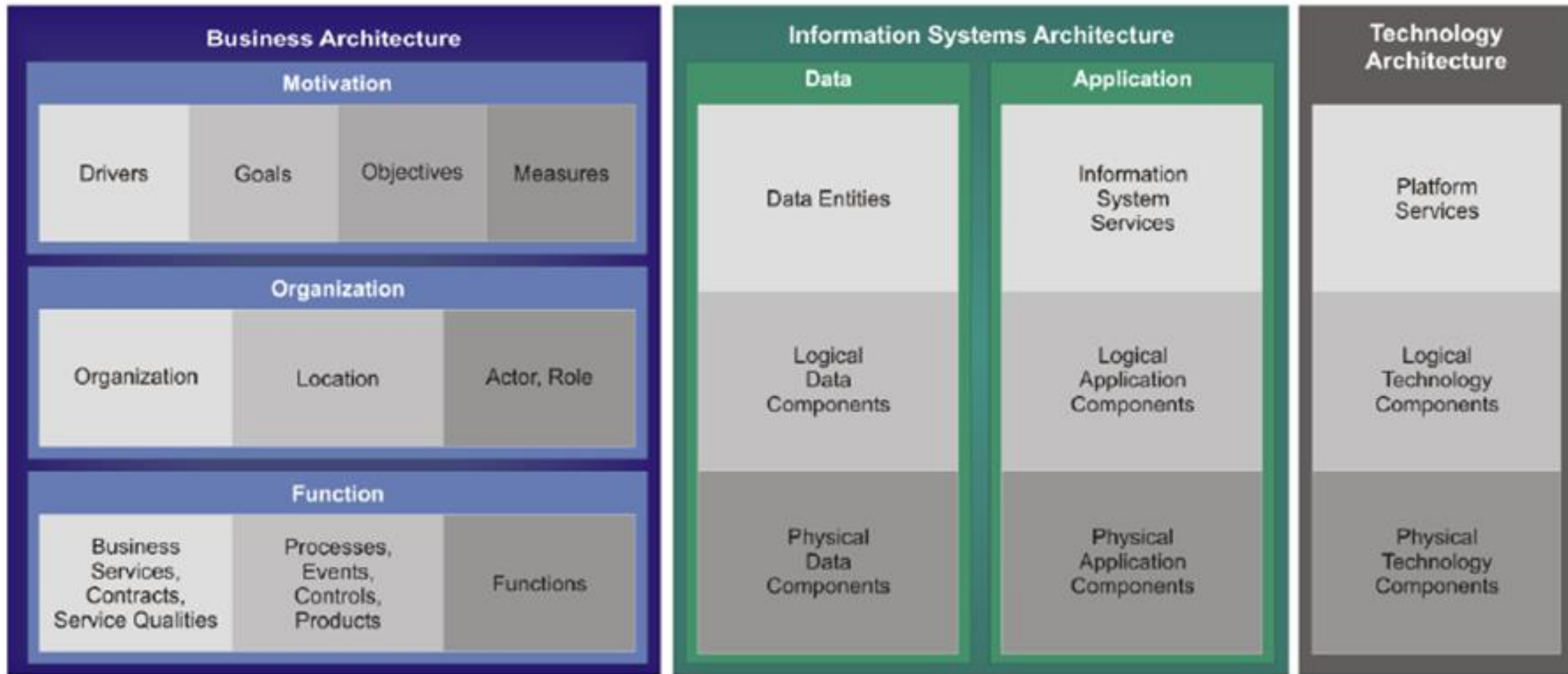
The Open Data Group Architecture Framework

Information Architecture

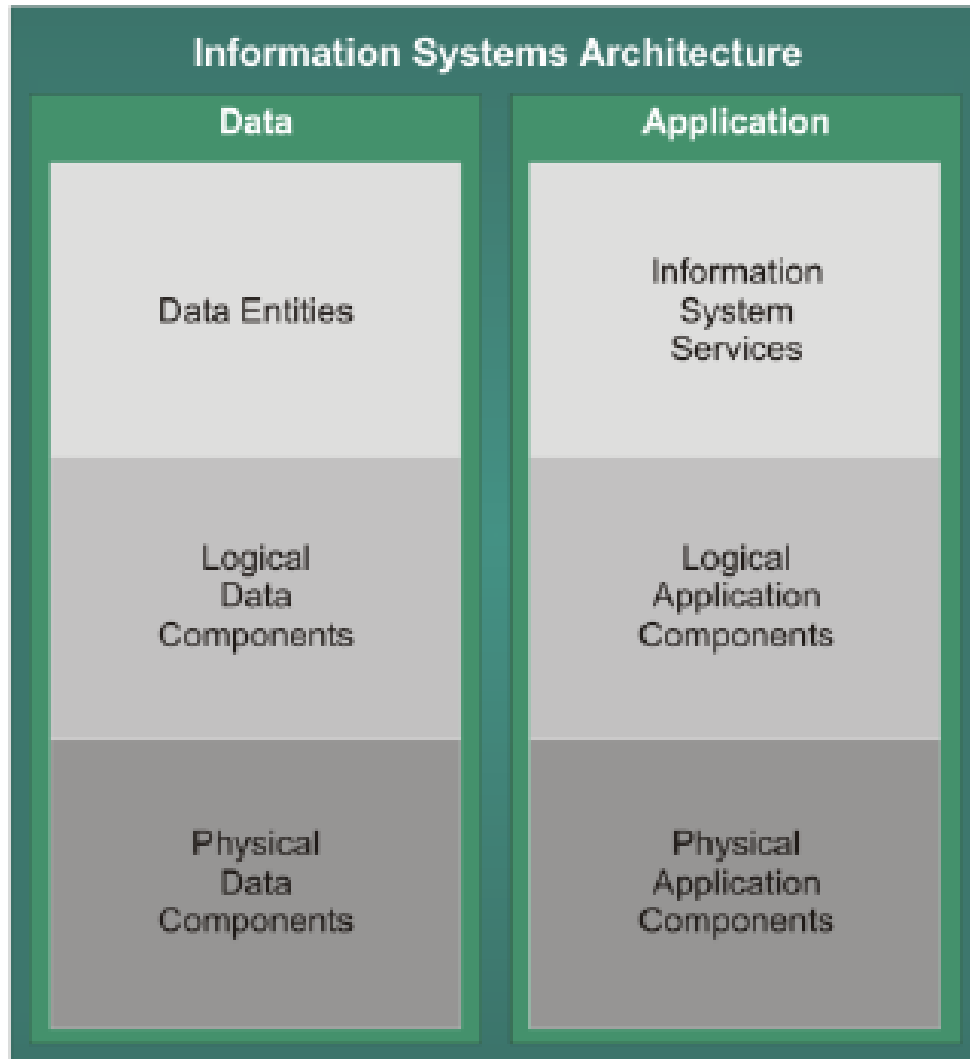


TOGAF Content Metamodel

Information Architecture

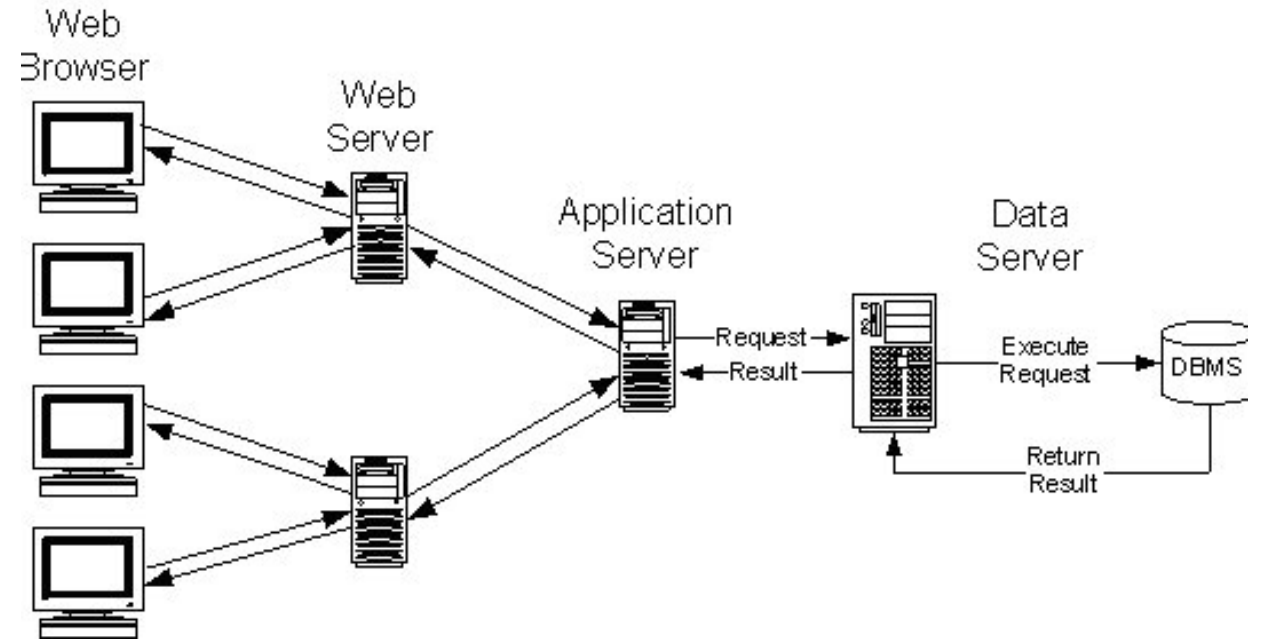


Conceptual models of Information Systems

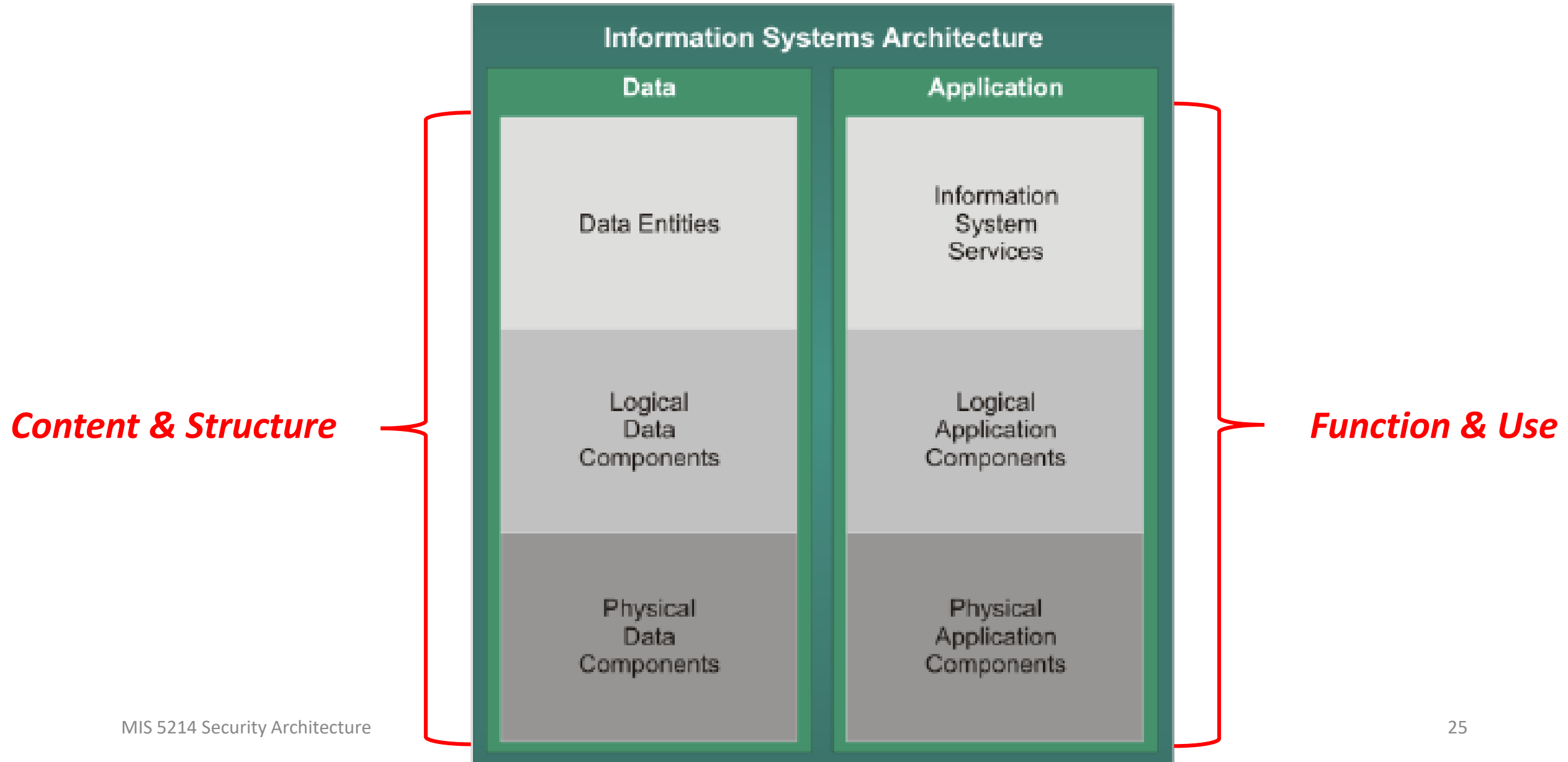


Content &
Structure
Security Architecture

Function &
Use

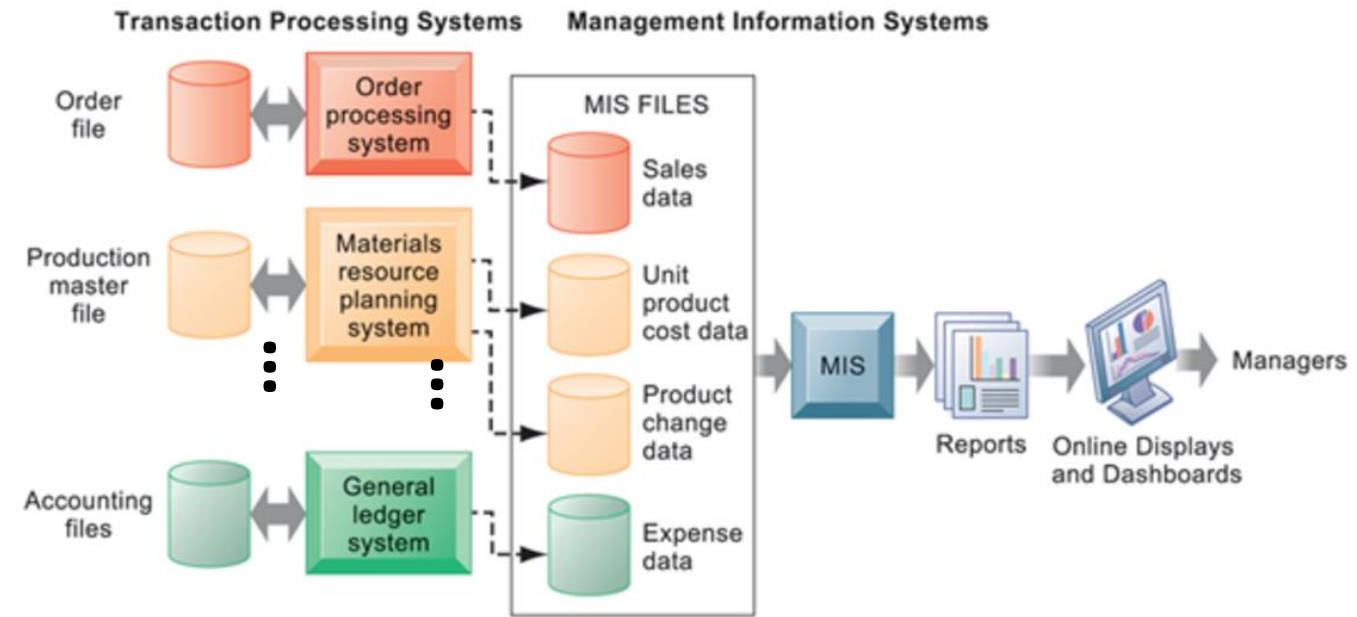
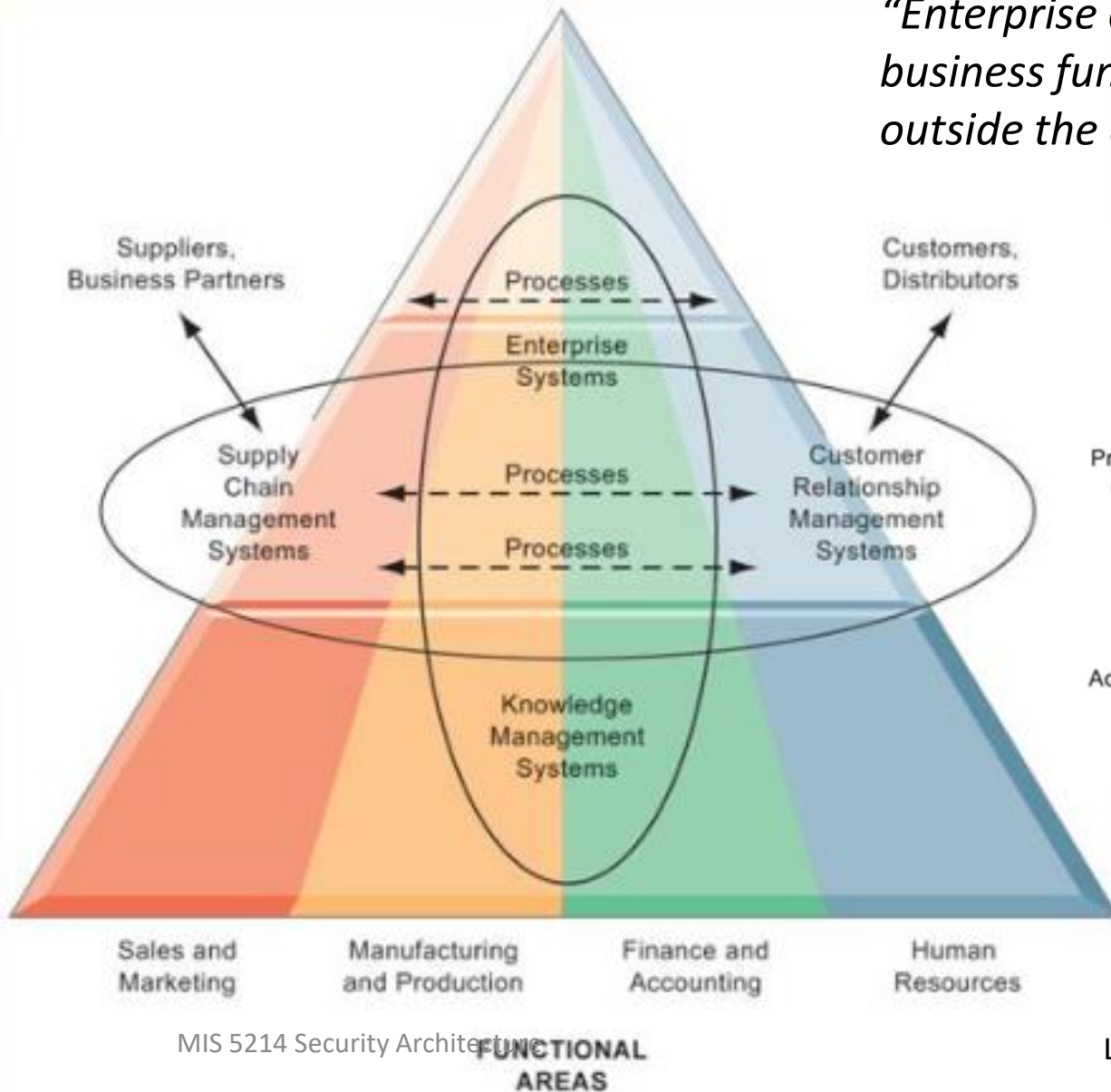


Conceptual models of Information Systems



Information Systems – Models of Information Flows

“Enterprise applications automate processes that span multiple business functions and organizational levels and may extend outside the organization”



Important Security Architecture Model:

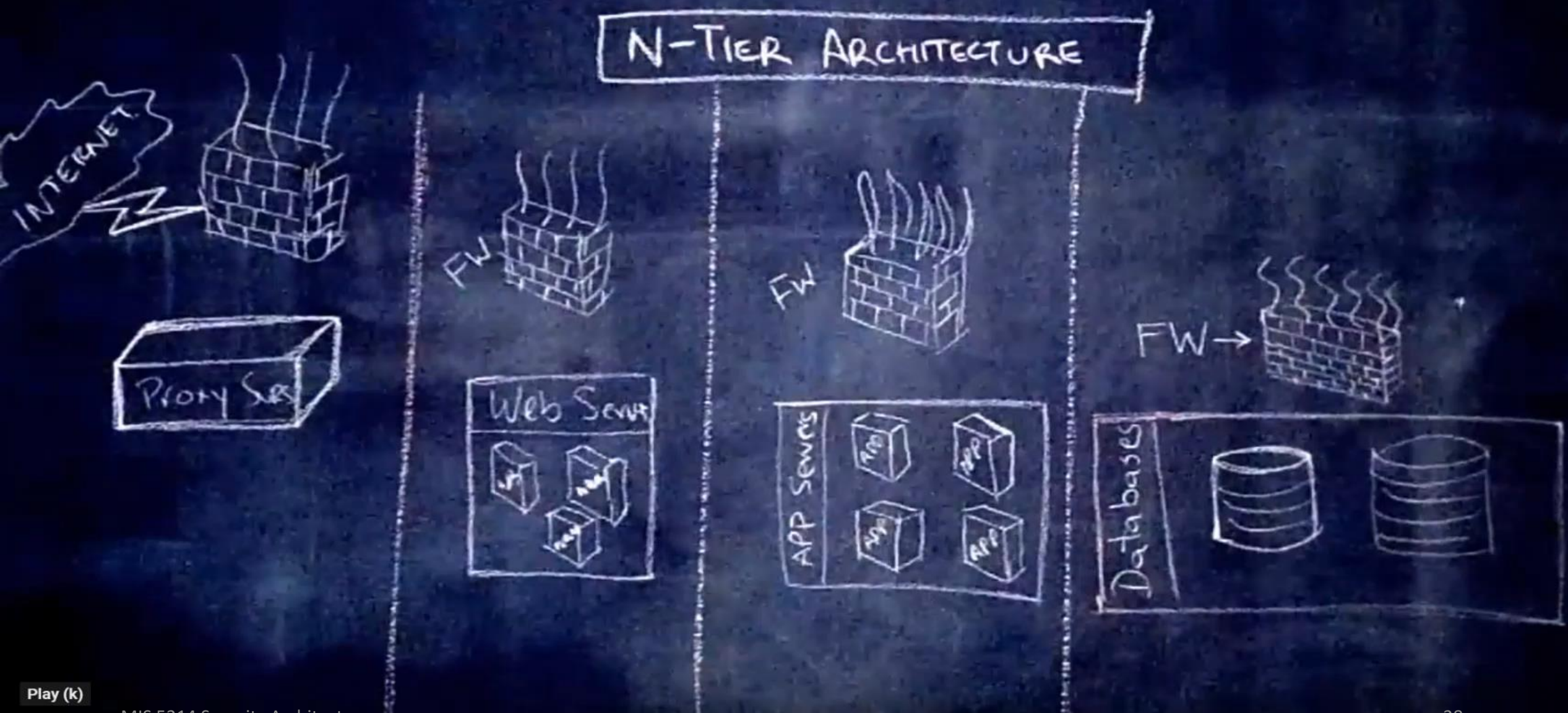
Defense in Depth

Also known as:

- Layered Security

We will studying elements of layered security moving forward...

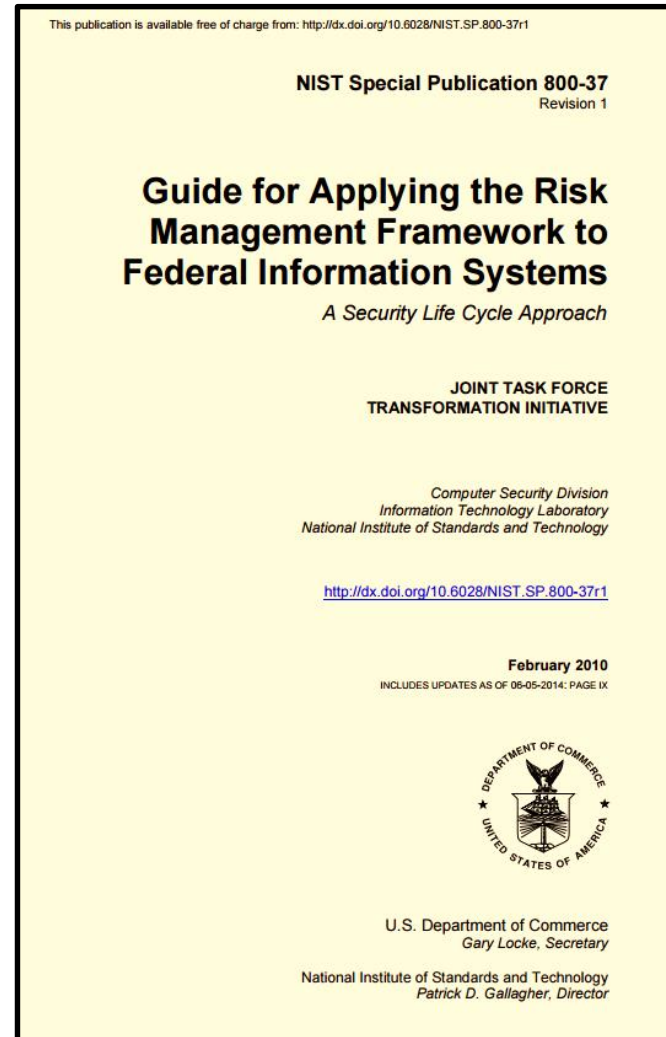
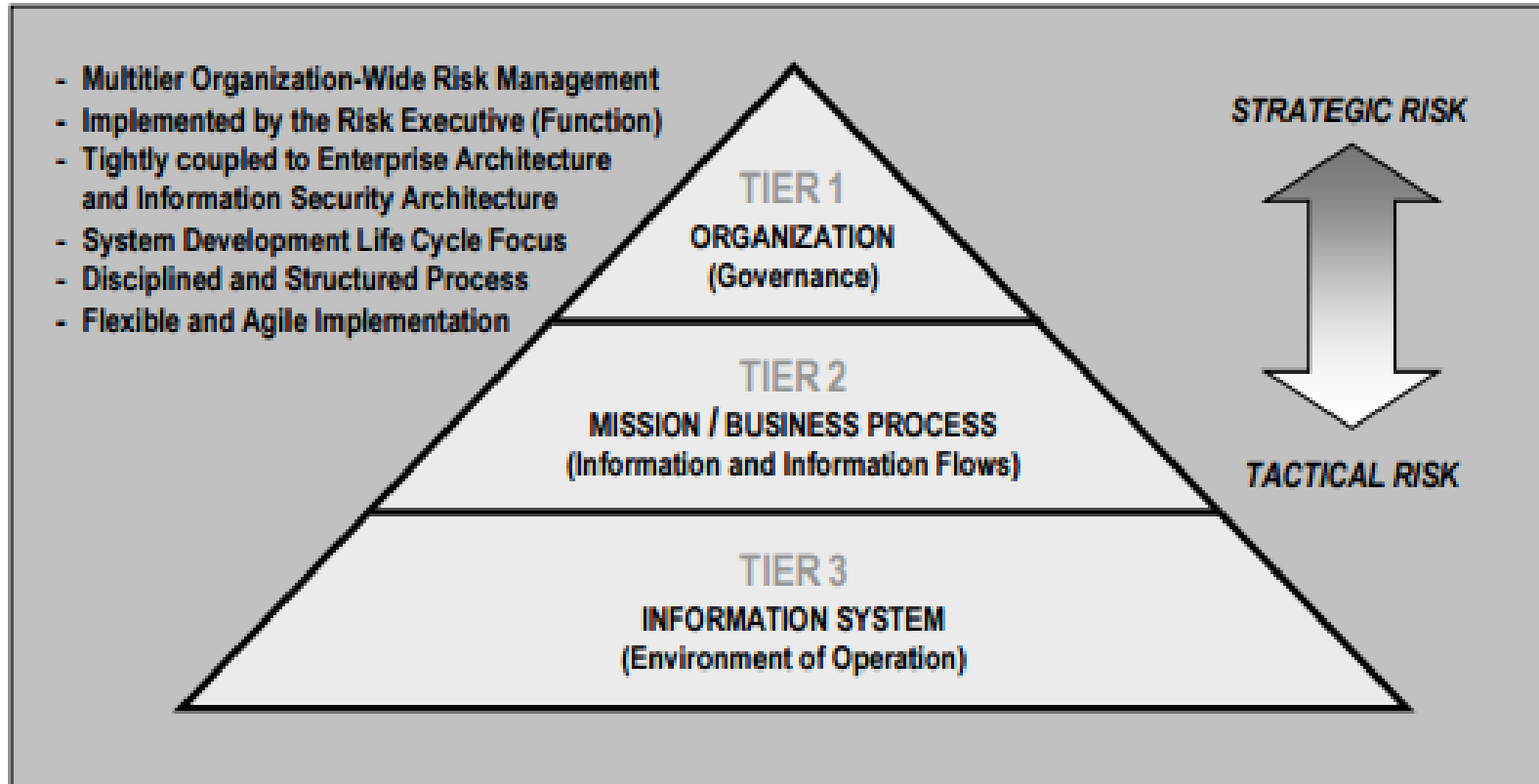




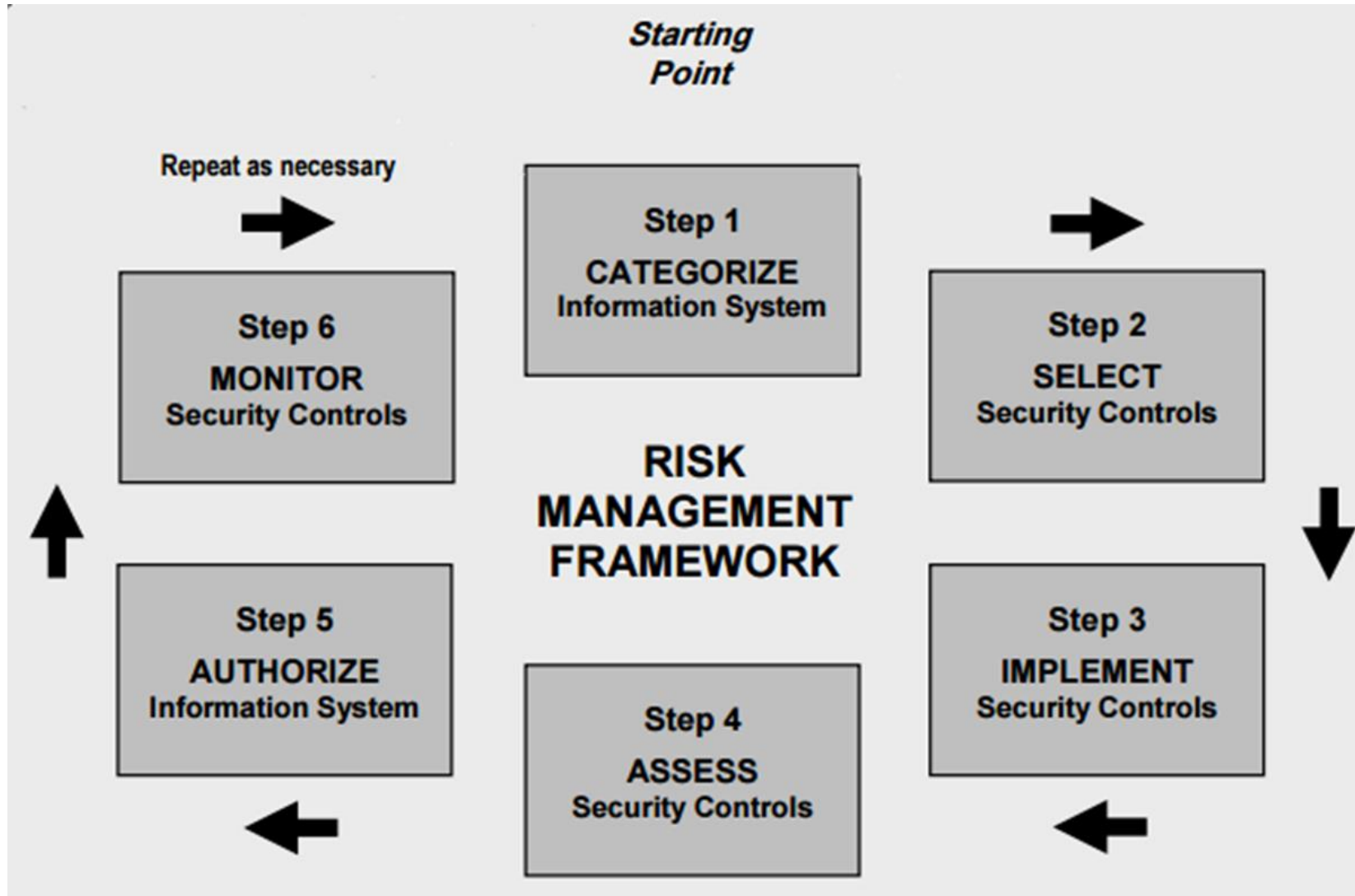
Exercise: Draw an N-Tier Architecture for a Web-Based System

- Consider the purpose and contents of a web-based system for managing the data of public utilities for a small town
- Identify who the users are
- Draw an N-Tier Architecture for the web-based system

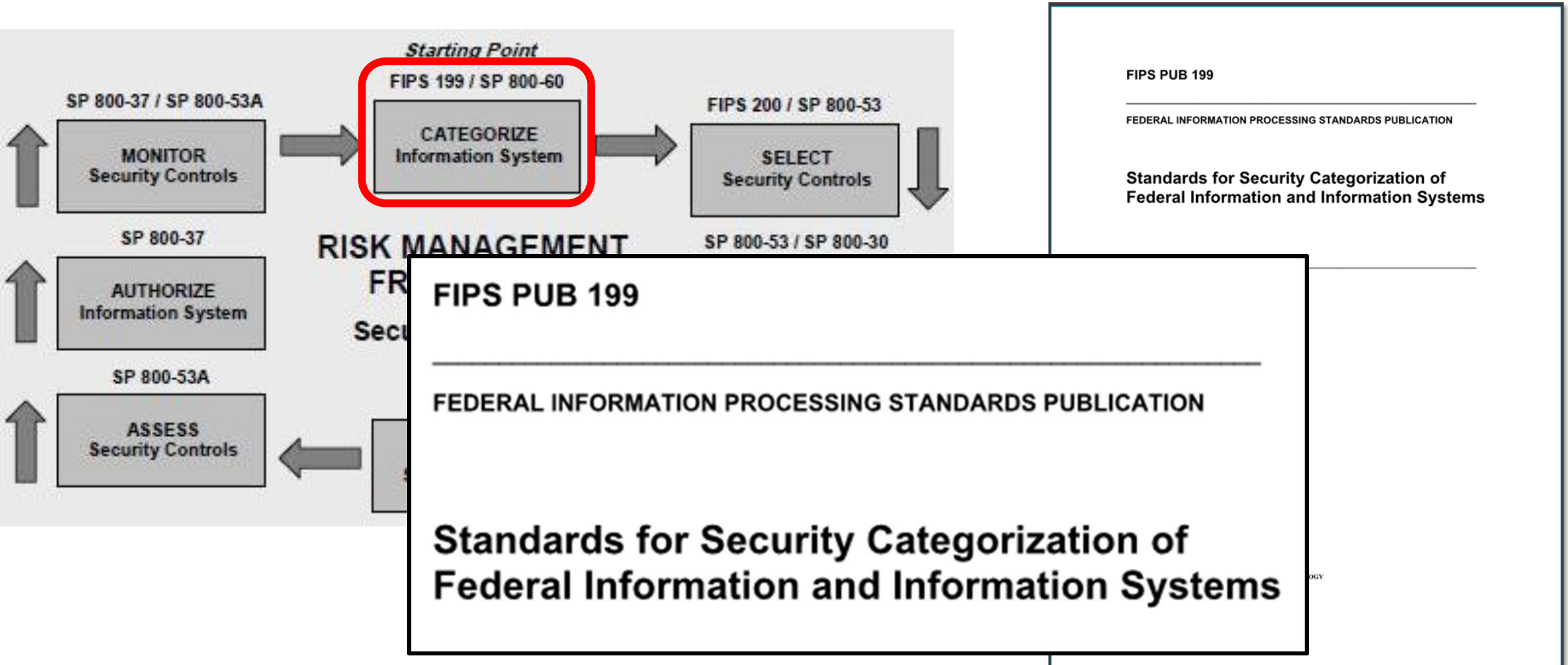
NIST Risk Management Framework



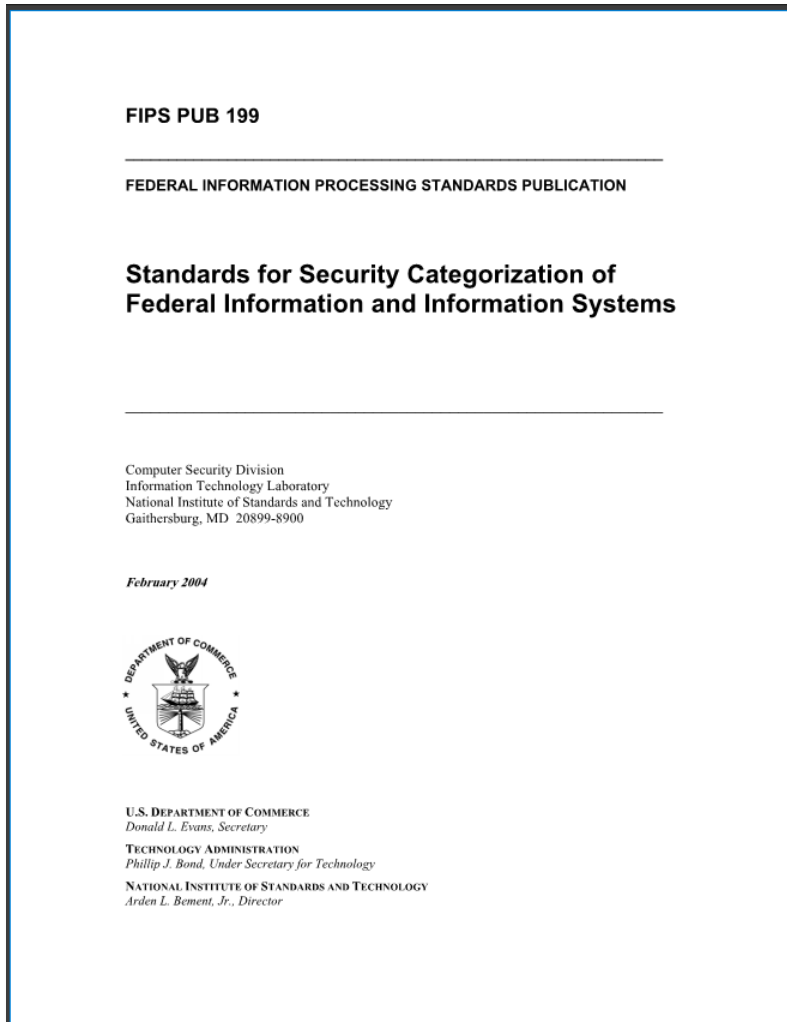
NIST Risk Management Framework



NIST Risk Management Framework



FIPS 199: Qualitative risk assessment based on security objectives



Security Objective	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>

What are the security categorizations of these datasets?

Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	
Electric	Moderate	Moderate	Moderate	
Traffic control	Low	Low	Low	
Comm_Electric Geodatabase				
Water Distribution System	Moderate	Moderate	Low	
Sanitary Collection System	Low	Low	Low	
Storm Collection System	Low	Low	Low	
Water_Sewer Geodatabase				
Parcel Boundary Shapefile	Low	Low	Low	

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect

Medium: Serious adverse effect

High: Severe or catastrophic adverse effect

The generalized format for expressing the security category, SC, of an information system is:

SC information system = $\{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\}$,

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:

SC contract information = $\{(\text{confidentiality}, \text{MODERATE}), (\text{integrity}, \text{MODERATE}), (\text{availability}, \text{LOW})\}$, = MODERATE rating

and

SC administrative information = $\{(\text{confidentiality}, \text{LOW}), (\text{integrity}, \text{LOW}), (\text{availability}, \text{LOW})\}$. = LOW rating

The resulting security category of the information system is expressed as:

SC acquisition system = $\{(\text{confidentiality}, \text{MODERATE}), (\text{integrity}, \text{MODERATE}), (\text{availability}, \text{LOW})\}$, = MODERATE rating

What is the overall impact ratings of the datasets?


Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
Comm_Electric Geodatabase				
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase				
Parcel Boundary Shapefile	Low	Low	Low	Low

What is the overall Information System impact rating?

System - Critical Infrastructure Information				
Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
<i>Comm_Electric Geodatabase</i>	<i>High</i>	<i>Moderate</i>	<i>Moderate</i>	<i>High</i>
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
<i>Water_Sewer Geodatabase</i>	<i>Moderate</i>	<i>Moderate</i>	<i>Low</i>	<i>Moderate</i>
Parcel Boundary Shapefile	Low	Low	Low	Low

High

Transformation of ordinal qualitative risk categories to interval quantitative risk measures



The diagram shows four ovals: Likelihood (green), Threat (pink), Risk (yellow), and Impact (blue). Arrows point from Likelihood to Risk, from Threat to Risk, and from Risk to Impact. The Risk oval also contains the word 'vulnerability'.

	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
Moderate (0.5)	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
Low (0.1)	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$

Risk Scale: High (>50 to 100)

Moderate (>10 to 50)

Low (1 to 10)


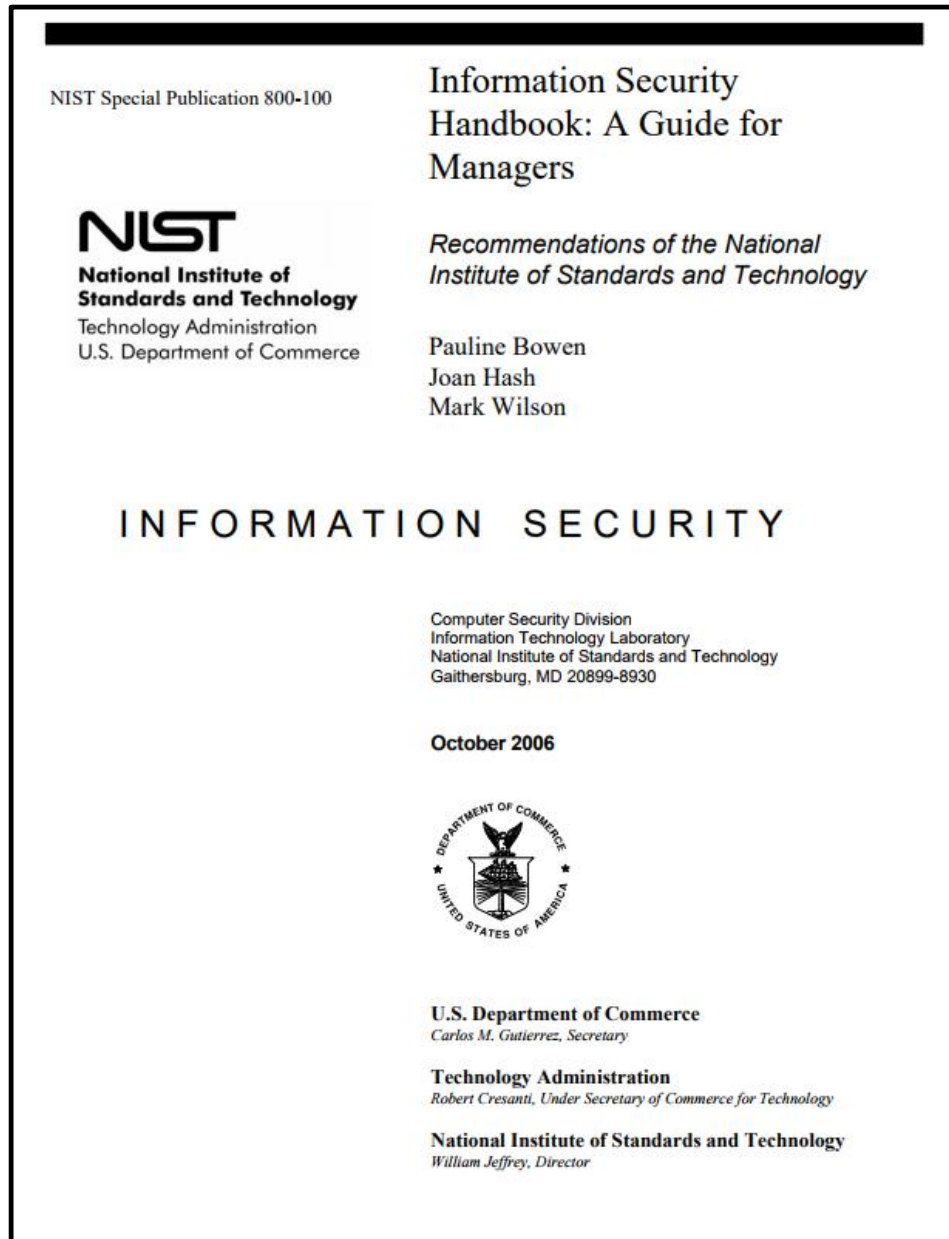
01527a

Requires the risk analyst to contribute additional information to move ordinal onto interval scale...

How would you quantify risk to prioritize asset types for cost-effective information security protection?

Dataset	Impact Rating	Likelihood
Communication	High	High
Electric	Moderate	Low
Traffic control	Low	Low
Water Distribution System	Moderate	Low
Sanitary Collection System	Low	Low
Storm Collection System	Low	Low
Parcel Boundary Shapefile	Low	Moderate

Hint:



	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
Moderate (0.5)	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
Low (0.1)	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$


Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

01527a

Solution

Dataset	Impact Rating	Likelihood
Communication	High	High
Electric	Moderate	Low
Traffic control	Low	Low
Water Distribution System	Moderate	Low
Sanitary Collection System	Low	Low
Storm Collection System	Low	Low
Parcel Boundary Shapefile	Low	Moderate

+



	Impact		
Threat Likelihood	Low (10)	Moderate (50)	High (100)
High (1.0)	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
Moderate (0.5)	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
Low (0.1)	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$

Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

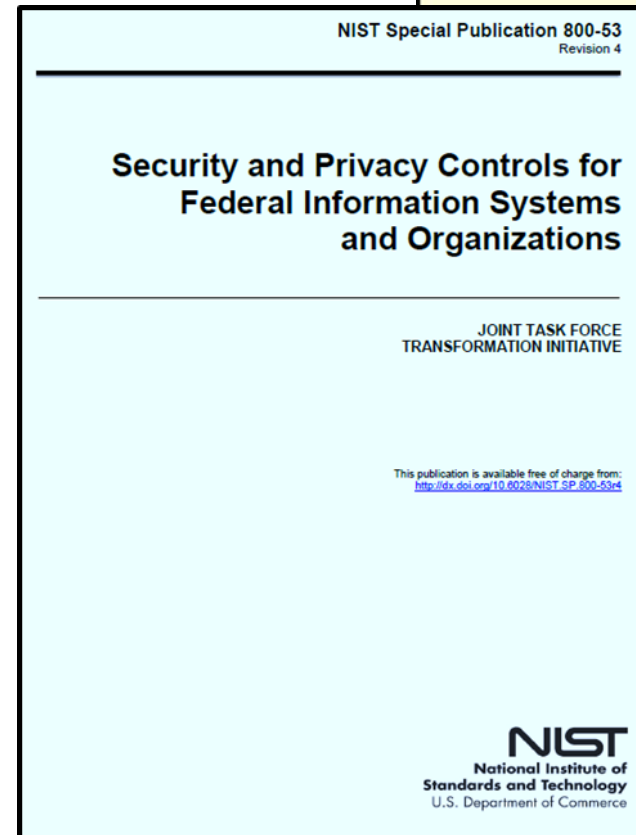
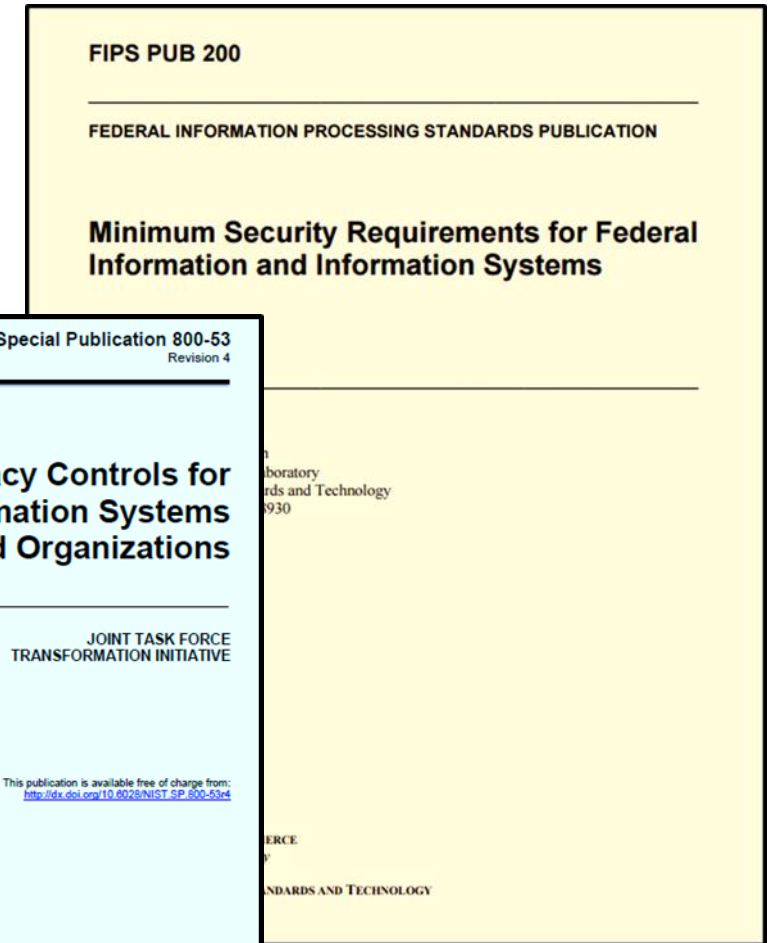
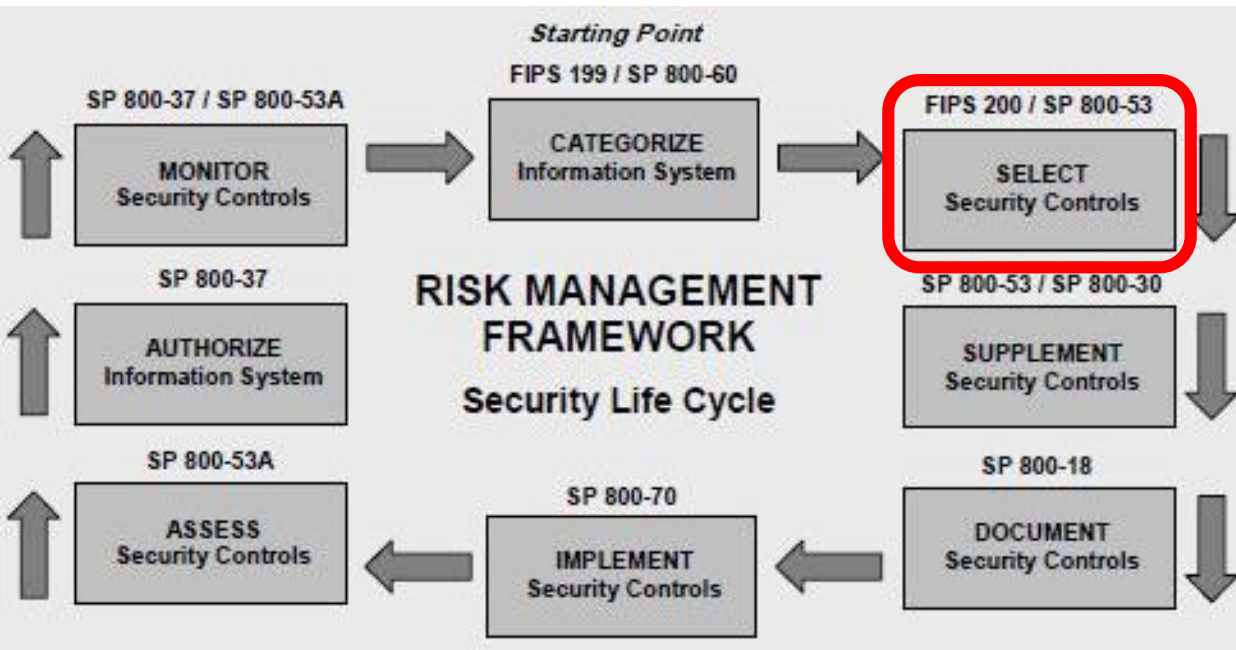
01527a

= ?

Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Traffic control	10	0.1	1
Comm_Electric Geodatabase	High		
			0
Water Distribution System	50	0.1	5
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1
Water_Sewer Geodatabase	Moderate	0.1	
			0
Parcel Boundary Shapefile	10	0.5	5

Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Water Distribution System	50	0.1	5
Parcel Boundary Shapefile	10	0.5	5
Traffic control	10	0.1	1
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1

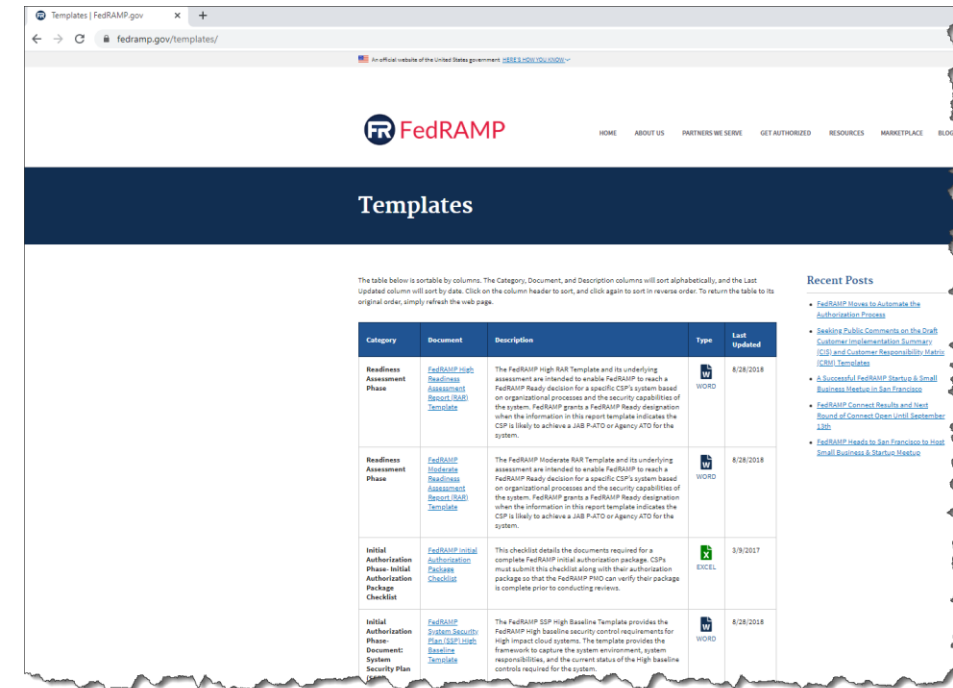
How do we use FIPS 199 security categorization to select security controls?



Agenda

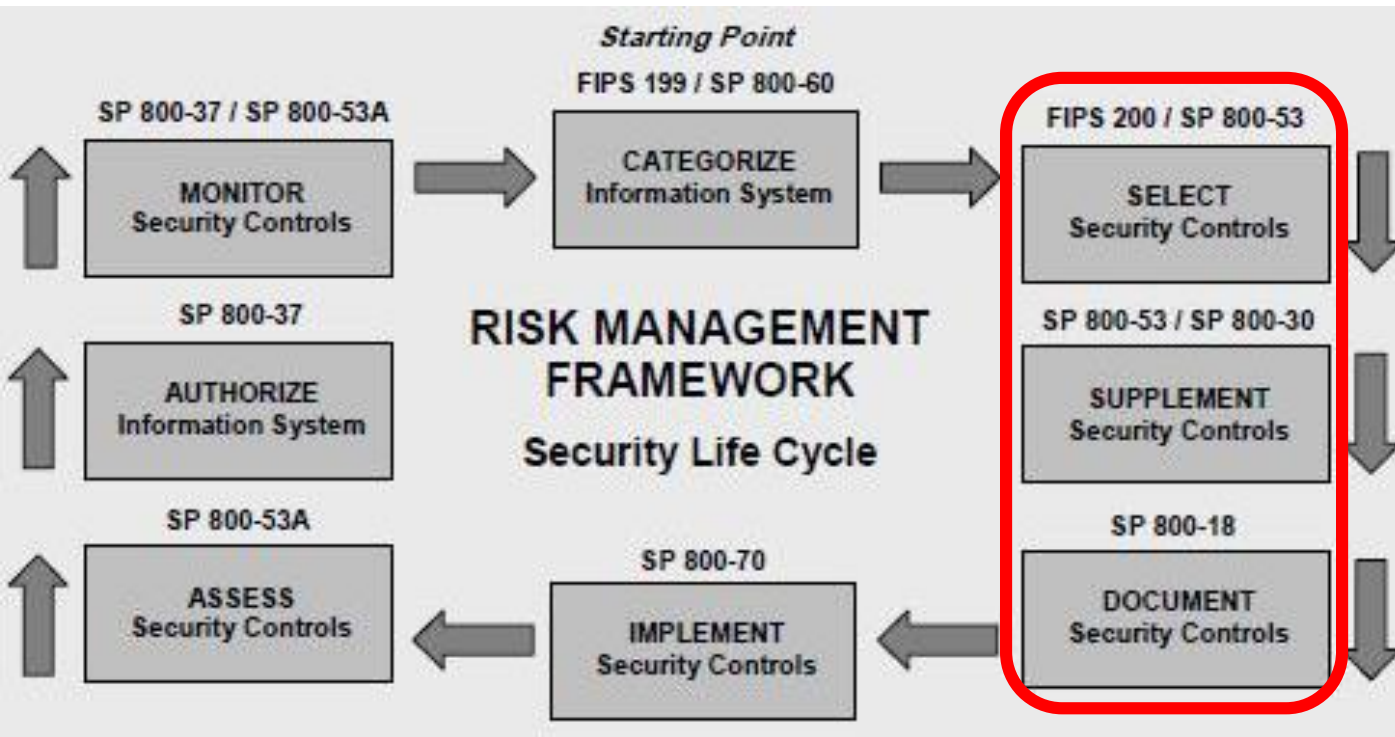
- ✓ Information Systems – some definitions
- ✓ Conceptual models of information systems
- ✓ NIST Risk Management Framework
- ✓ FIPS 199 Security Categorization
- ✓ Transforming qualitative risk assessment into quantitative risk assessment
- **FedRAMP System Security Plan – overview**
 - NIST 800-53 Security controls
 - Role of FIPS 199 in selecting a security control baseline
 - NIST 800-18 classification system for security control families

System Security Plan (SSP)

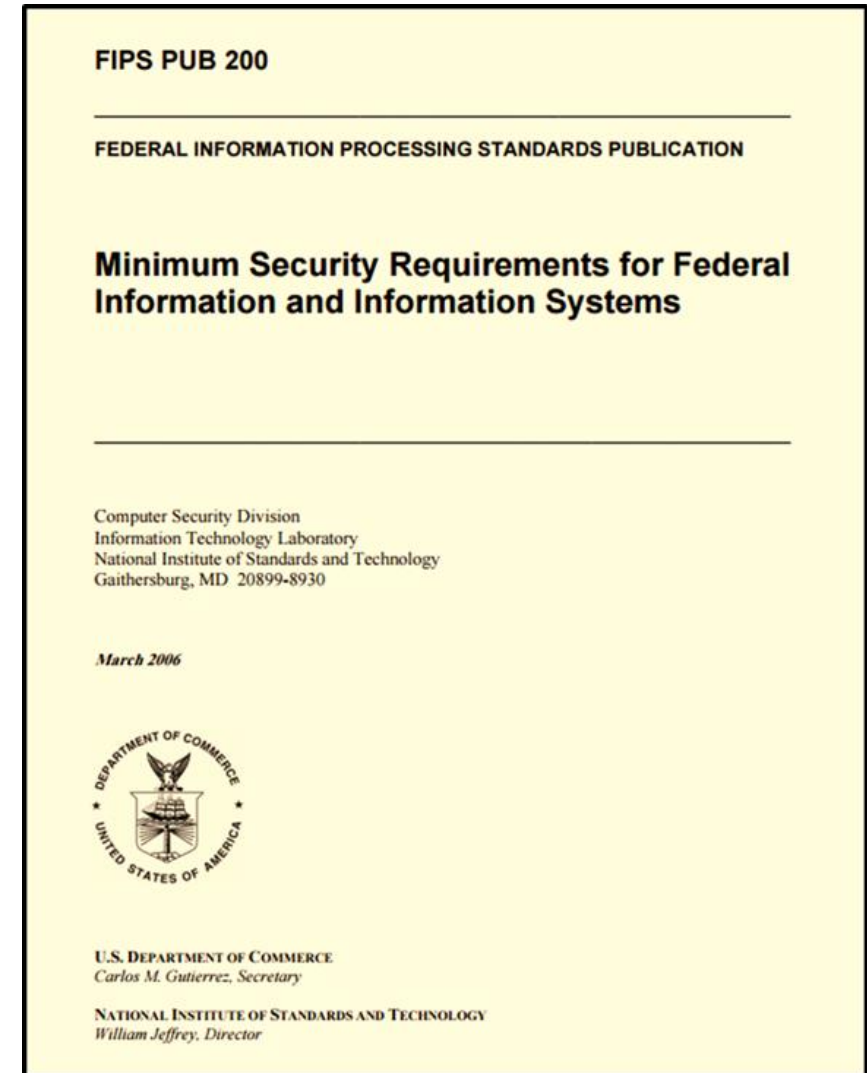


<https://www.fedramp.gov/templates/>

Information System Security Plan (SSP)



1	INFORMATION SYSTEM NAME/TITLE.....	1
2	INFORMATION SYSTEM CATEGORIZATION	1
2.1	Information Types	1
2.2	Security Objectives Categorization (FIPS 199).....	3
2.3	E-Authentication Determination.....	3
3	INFORMATION SYSTEM OWNER.....	4
4	AUTHORIZING OFFICIAL	4
5	OTHER DESIGNATED CONTACTS	4
6	ASSIGNMENT OF SECURITY RESPONSIBILITY	5
7	INFORMATION SYSTEM OPERATIONAL STATUS	6
8	INFORMATION SYSTEM TYPE.....	7
8.1	Cloud Service Models.....	7
8.2	Cloud Deployment Models.....	8
8.3	Leveraged Authorizations	8
9	GENERAL SYSTEM DESCRIPTION	9
9.1	System Function or Purpose	9
9.2	Information System Components and Boundaries	9
9.3	Types of Users	9
9.4	Network Architecture.....	11
10	SYSTEM ENVIRONMENT AND INVENTORY.....	11
10.1	Data Flow	13
10.2	Ports, Protocols and Services	13
11	SYSTEM INTERCONNECTIONS	15
12	LAWS, REGULATIONS, STANDARDS AND GUIDANCE	16
12.1	Applicable Laws and Regulations	16
12.2	Applicable Standards and Guidance.....	16
13	MINIMUM SECURITY CONTROLS	17



FedRAMP SSP – first step: Security Objectives Categorization

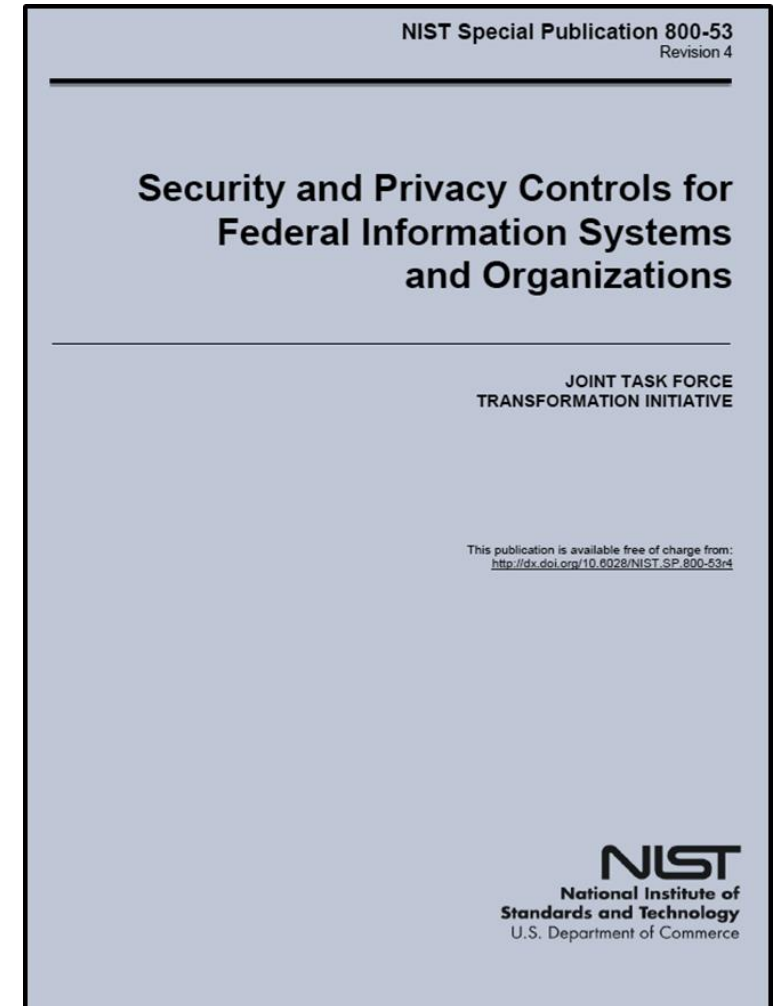
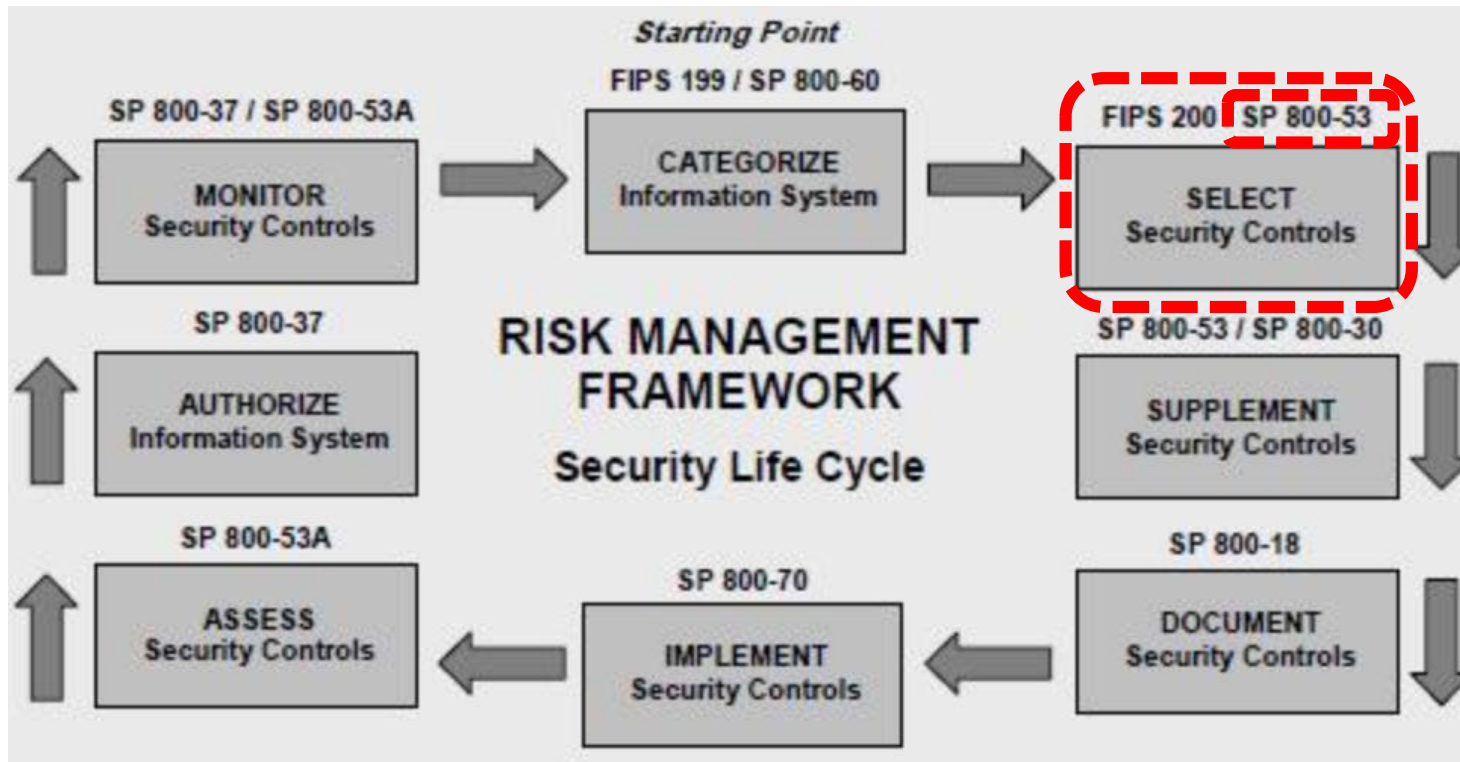
Table of Contents

1	INFORMATION SYSTEM NAME/TITLE.....	1
2	INFORMATION SYSTEM CATEGORIZATION.....	1
2.1	Information Types.....	1
2.2	Security Objectives Categorization (FIPS 199).....	3

FIPS 200 *Minimum Security Control Requirements*

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessment (CA)
5. Configuration Management (CM)
6. Contingency Planning
7. Identification and Authentication
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection *PE)
12. Planning (PL)
13. Personal Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition(SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

NIST Risk Management Framework



Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4

TABLE D-2: SECURITY CONTROL BASELINES*

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES			
			LOW	MOD	HIGH	
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected	Not Selected
SC-26	Homogents	P0	Not Selected	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	Not Selected	SC-28	SC-28
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10	1 Selected Not Selected
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11	1 Selected Not Selected
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12	1 Selected Not Selected
SA-13	Trustworthiness	P0	Not Selected	Not Selected	SA-13	1 Selected Not Selected
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17	1 Selected Not Selected
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18	1 Selected Not Selected
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
PE-20	Asset Monitoring and Tracking	P2	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)	1 Selected Not Selected
IR-4	Incident Handling	P1	IR-4	IR-4 (1) (4)	IR-4 (1) (4)	1 Selected Not Selected
IR-5	Incident Monitoring	P1	IR-5	IR-5 (1)	IR-5 (1)	1 Selected Not Selected
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)	1 Selected Not Selected
MA-1	Configuration Settings	P1	MA-1	MA-1 (2)	MA-1 (2)	1 Selected Not Selected
MA-2	Least Functionality	P1	MA-2	MA-2 (1) (2) (4)	MA-2 (1) (2) (5)	1 Selected Not Selected
MA-3	Information System Component Inventory	P1	MA-3	MA-3 (1) (2) (3) (4) (5)	MA-3 (1) (2) (3) (4) (5)	1 Selected Not Selected
MA-4	Configuration Management Plan	P1	Not Selected	MA-4	MA-4	1 Selected Not Selected
MA-5	Software Usage Restrictions	P2	MA-5	MA-5 (1)	MA-5 (1)	1 Selected Not Selected
MA-6	User-Installed Software	P1	MA-6	MA-6 (1)	MA-6 (1)	1 Selected Not Selected
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1	1 Selected Not Selected
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (3) (8) (4) (5) (6)	1 Selected Not Selected
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)	1 Selected Not Selected
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)	1 Selected Not Selected
CP-5	Withdrawal	---	---	---	---	1 Selected Not Selected
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)	1 Selected Not Selected
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3) (4)	CP-7 (1) (2) (3) (4)	1 Selected Not Selected
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)	1 Selected Not Selected
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)	1 Selected Not Selected
CP-10	Information System Recovery and Reconstruction	P1	CP-10	CP-10 (2)	CP-10 (2) (4)	1 Selected Not Selected
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1	1 Selected Not Selected
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (8) (9) (10) (11) (12)	1 Selected Not Selected
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3	1 Selected Not Selected
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4	1 Selected Not Selected
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)	1 Selected Not Selected
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6	1 Selected Not Selected
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7	1 Selected Not Selected
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	1 Selected Not Selected
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected	1 Selected Not Selected
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1	1 Selected Not Selected
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)	1 Selected Not Selected

TABLE D-2: SECURITY CONTROL BASELINES³⁴

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeyknots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	SA-13
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1) (4)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5 (1)	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6 (1)	IR-6 (1)	IR-6 (1)
CM-6	Configuration Settings	P1	CM-6	CM-6 (1) (2)	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (3) (5)
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Withdrawn	---	---	---	---
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1) (2)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5 (1) (2)	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	AU-10	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12 (1) (3)	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Withdrawn	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connectors	P2	CA-9	CA-9	CA-9
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

- a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
 - 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
- b. Reviews and updates the current:
 - 1. Access control policy [*Assignment: organization-defined frequency*]; and
 - 2. Access control procedures [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW AC-1	MOD AC-1	HIGH AC-1	53
----	----------	----------	-----------	----

AC-1

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Control Family: Access Control

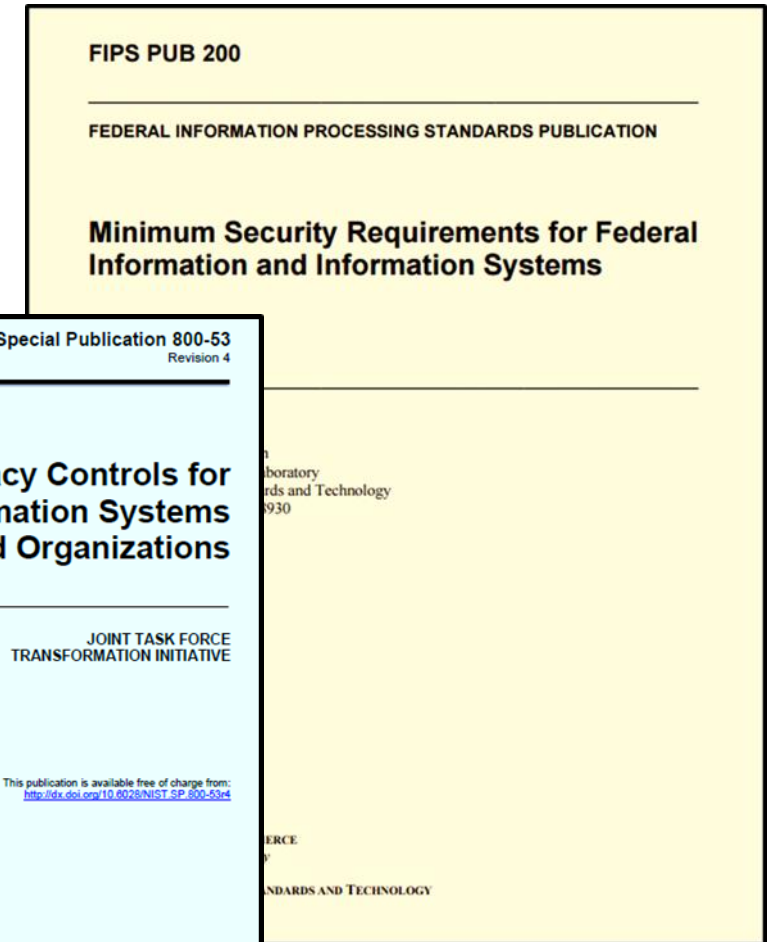
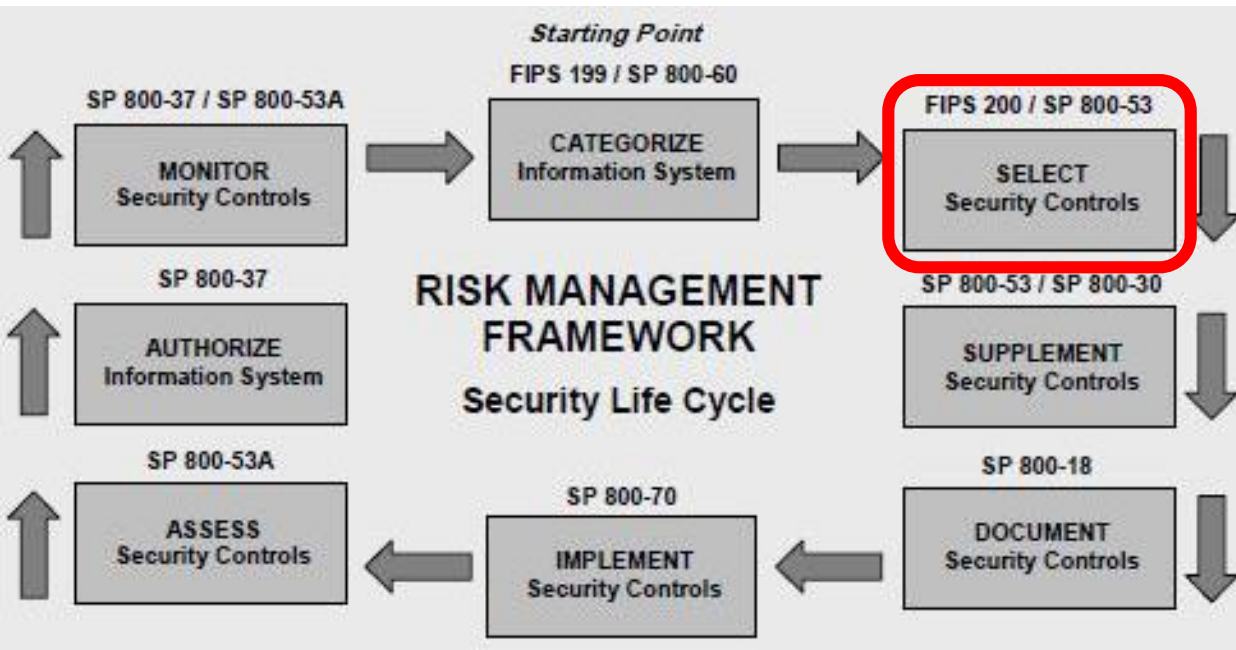
How many access controls are relevant to the web-based system you began designing for managing the data of public utilities for the small town ?

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
<http://dx.doi.org/10.6028/NIST.SP.800-53r4>

How do we use FIPS 199 security categorization to select security controls?



NIST 800-53 Controls are presented alphabetically

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessment (CA)
5. Configuration Management (CM)
6. Contingency Planning
7. Identification and Authentication
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection *PE)
12. Planning (PL)
13. Personal Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition(SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

NIST 800-53 Controls are grouped by “Class”

NIST Special Publication 800-18
Revision 1

Guide for Developing Security
Plans for Federal Information
Systems

NIST
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006



U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

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

Table 2: Security Control Class, Family, and Identifier

Risk Assessment (RA) Controls

Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	Withdrawn	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermesasures Survey	P0	Not Selected	Not Selected	Not Selected

RA-1

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

- a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

- a. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:
 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
- b. Reviews and updates the current:
 1. Risk assessment policy [*Assignment: organization-defined frequency*]; and
 2. Risk assessment procedures [*Assignment: organization-defined frequency*].

scope, roles, responsibilities, organizational entities, and compliance;

risk assessment policy and associated

n-defined frequency]; and

zation-defined frequency].

ment of policy and procedures for the control enhancements in the RA family.

cutive Orders, directives, regulations, es and procedures at the organization

procedures unnecessary. The policy can icy for organizations or conversely, can

nature of certain organizations. The general and for particular information

systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1	LOW RA-1	MOD RA-1	HIGH RA-1	59
----	----------	----------	-----------	----

RA -2

RA-2 SECURITY CATEGORIZATION

Control: The organization:

- a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

RA-2 SECURITY CATEGORIZATION

Control: The organization:

- a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

representative reviews

for effective
e impacts to
information and
availability.

activity with
information
organizations also
with the USA
national-level

adverse impacts. Security categorization processes carried out by organizations facilitate the development of inventories of information assets, and along with CM-8, mappings to specific information system components where information is processed, stored, or transmitted. Related controls: CM-8, MP-4, RA-3, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2	60
----	----------	----------	-----------	----

RA -3

RA-3 RISK ASSESSMENT

Control: The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- b. Documents risk assessment results in [*Selection: security plan; risk assessment report; [Assignment: organization-defined document]*];

RA-3 RISK ASSESSMENT

Control: The organization:

- a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
- b. Documents risk assessment results in [*Selection: security plan; risk assessment report; [Assignment: organization-defined document]*];
- c. Reviews risk assessment results [*Assignment: organization-defined frequency*];
- d. Disseminates risk assessment results to [*Assignment: organization-defined personnel or roles*]; and
- e. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Enhancements: NONE.

References: OMB Memorandum 04-04; NIST Special Publications 800-30, 800-39;
Web: <http://idmanagement.gov>.

Priority and Baseline Allocation:

P1	LOW RA-3	MOD RA-3	HIGH RA-3
----	----------	----------	-----------

TABLE OF CONTENTS

System Security Plan and FIPS 199, FIPS 200 and SP800-53...

1.	INFORMATION SYSTEM NAME/TITLE.....	1	14.	ACRONYMS	392
2.	INFORMATION SYSTEM CATEGORIZATION	1	15.	ATTACHMENTS.....	393
2.1.	Information Types.....	1	Attachment 1	Information Security Policies and Procedures.....	395
2.2.	Security Objectives Categorization (FIPS 199).....	3	Attachment 2	User Guide	396
2.3.	Digital Identity Determination.....	3	Attachment 3	Digital Identity Worksheet	397
3.	INFORMATION SYSTEM OWNER.....	4	Introduction and Purpose	397	
4.	AUTHORIZING OFFICIALS	4	Information System Name/Title.....	397	
5.	OTHER DESIGNATED CONTACTS	4	Digital Identity Level Definitions	397	
6.	ASSIGNMENT OF SECURITY RESPONSIBILITY	5	Review Maximum Potential Impact Levels.....	398	
7.	INFORMATION SYSTEM OPERATIONAL STATUS.....	6	Digital Identity Level Selection	399	
8.	INFORMATION SYSTEM TYPE.....	7	Attachment 4	PTA/PIA	400
8.1.	Cloud Service Models	7	Privacy Overview and Point of Contact (POC).....	400	
8.2.	Cloud Deployment Models	8	Applicable Laws and Regulations.....	400	
8.3.	Leveraged Authorizations.....	8	Applicable Standards and Guidance	401	
9.	GENERAL SYSTEM DESCRIPTION	9	Personally Identifiable Information (PII).....	401	
9.1.	System Function or Purpose	9	Privacy Threshold Analysis	402	
9.2.	Information System Components and Boundaries.....	9	Qualifying Questions	402	
9.3.	Types of Users.....	10	Designation.....	402	
9.4.	Network Architecture.....	11	Attachment 5	Rules of Behavior	403
10.	SYSTEM ENVIRONMENT AND INVENTORY	12	Attachment 6	Information System Contingency Plan	404
10.1.	Data Flow	12	Attachment 7	Configuration Management Plan.....	405
10.2.	Ports, Protocols and Services.....	14	Attachment 8	Incident Response Plan	406
11.	SYSTEM INTERCONNECTIONS	15	Attachment 9	CIS Workbook.....	407
12.	LAWS, REGULATIONS, STANDARDS AND GUIDANCE	17	Attachment 10	FIPS 199.....	408
12.1.	Applicable Laws and Regulations.....	17	Introduction and Purpose	408	
12.2.	Applicable Standards and Guidance	17	Scope	408	
13.	MINIMUM SECURITY CONTROLS	18	System Description.....	408	
			Methodology.....	409	
			Attachment 11	Separation of Duties Matrix.....	411
			Attachment 12	FedRAMP Laws and Regulations	412
			Attachment 13	FedRAMP Inventory Workbook	413

SSP – Control Inventory Example

Control Class	Control Family	Implemented	Partial	Planned	Alternate	NA	System	Empty	FedRamp	Investment
Management	Risk Assessment	2	5	1	2	1	11		10	110%
Management	Planning	1	2	1			4	2	6	67%
Management	System & Service Acquisition						0	22	22	0%
Management	Security Assessments & Authorization				1		1	14	15	7%
Technical	Identification & Authentication	9	3	8		9	29		27	107%
Technical	Access Control	4	3	28	1	13	49		43	114%
Technical	Audit & Accountability	1	3	13		4	21		19	111%
Technical	System & Communication Protection	17	8	9	1	5	40		32	125%
Operational	Personnel Security	6	1			2	9		9	100%
Operational	Physical & Environmental Protection					19	19	1	20	95%
Operational	Contingency Planning	1	2	24			27		24	113%
Operational	Configuration Management	8	6	11		5	30	1	26	115%
Operational	Maintenance						0	11	11	0%
Operational	System & Information Integrity		5	16		8	33		28	118%
Operational	Media Protection	2				3	5	7	10	50%
Operational	Incident Response						0	18	18	0%
Operational	Awareness & Training			5			5		5	100%
	Total:	55	38	116	5	69	283	76	325	87%

Agenda

- ✓ Information Systems – some definitions
- ✓ Conceptual models of information systems
- ✓ NIST Risk Management Framework
- ✓ FIPS 199 Security Categorization
- ✓ Transforming qualitative risk assessment into quantitative risk assessment
- ✓ FedRAMP System Security Plan – overview
 - ✓ NIST 800-53 Security controls
 - ✓ Role of FIPS 199 in selecting a security control baseline
 - ✓ NIST 800-18 classification of security control families

Agenda

- ✓ Information Systems – some definitions
- ✓ Conceptual models of information systems
- ✓ NIST Risk Management Framework
- ✓ FIPS 199 Security Categorization
- ✓ Transforming qualitative risk assessment into quantitative risk assessment
- ✓ FedRAMP System Security Plan – overview
 - ✓ NIST 800-53 Security controls
 - ✓ Role of FIPS 199 in selecting a security control baseline
 - ✓ NIST 800-18 classification of security control families
- Bonus: Threat Modeling exercise...

STRIDE

Threat model created by Microsoft, based 6 categories of threats:

- **Spoofing** – Can an attacker gain access using a false identity?
- **Tampering** – Can an attacker modify data as it follows through the application?
- **Repudiation** – If an attacker denies doing something, can we prove he/she did it?
- **Information disclosure** – Can an attacker gain access to private or potentially injurious data?
- **Denial of service** – Can an attacker crash or reduce the availability of the system?
- **Elevation of privilege** – Can an attacker assume the identify of a privileged user?

STRIDE threats and desired properties they impact

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Automotive Security example

<https://www.youtube.com/watch?v=MK0SrxBC1xs>

Modern cars are computer networks on wheels, with most have many computers that control various aspects of the car

Two hackers developed a tool that can hijack a Jeep over the internet. WIRED senior writer Andy Greenberg takes the SUV for a spin on the highway while the hackers attack it from miles away.

University of Washington Security Cards

A security threat brainstorming activity

Break up into groups of 2 or 3:

- Pretend you are security professionals
 - A car company tasked you with thinking through the security implications of the modern car computer systems
- Start with the blue suit of cards (“Human Impact”), consider what impacts to people would result if an attacker misused modern car systems like the attack you just witnessed
 - Either think about one car, or think about the entire car product line
 - Rank order the cards from most relevant
 - Explain your 3 top choices

University of Washington Security Cards

A security threat brainstorming activity

- Next move onto the orange “Adversary Motivation” suit
- Consider what motivations adversaries might have for attacking modern car systems
 - Either think about one car, or think about the entire car product line
 - Rank order the adversary motivations from most relevant to least
 - Explain your 3 top choices

University of Washington Security Cards

A security threat brainstorming activity

- Next move onto the red “Adversary’s Resources” suit
- Consider what resources adversaries might have for attacking modern car systems
 - Either think about one car, or think about the entire car product line
 - Rank order the cards from most relevant
 - Explain your 3 top choices

STRIDE Threat Modeling

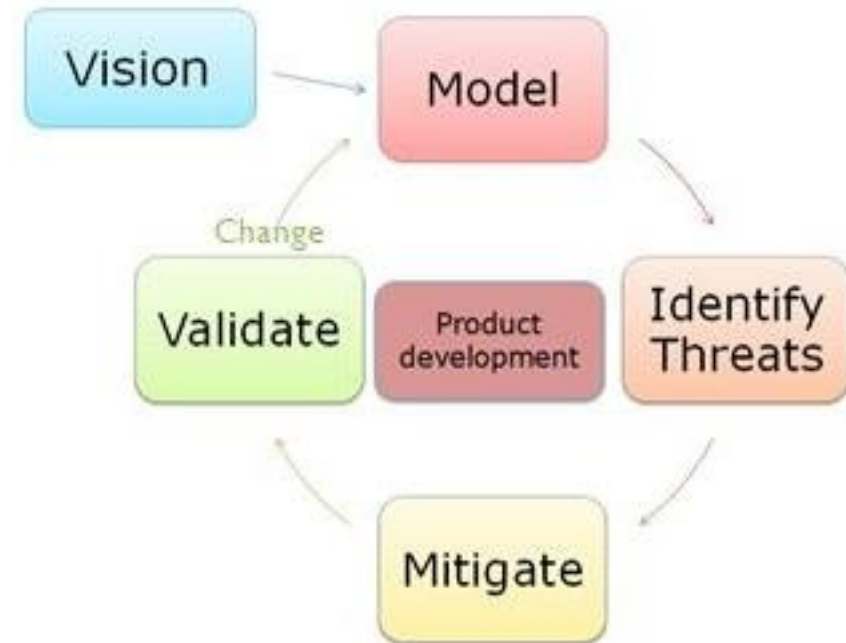
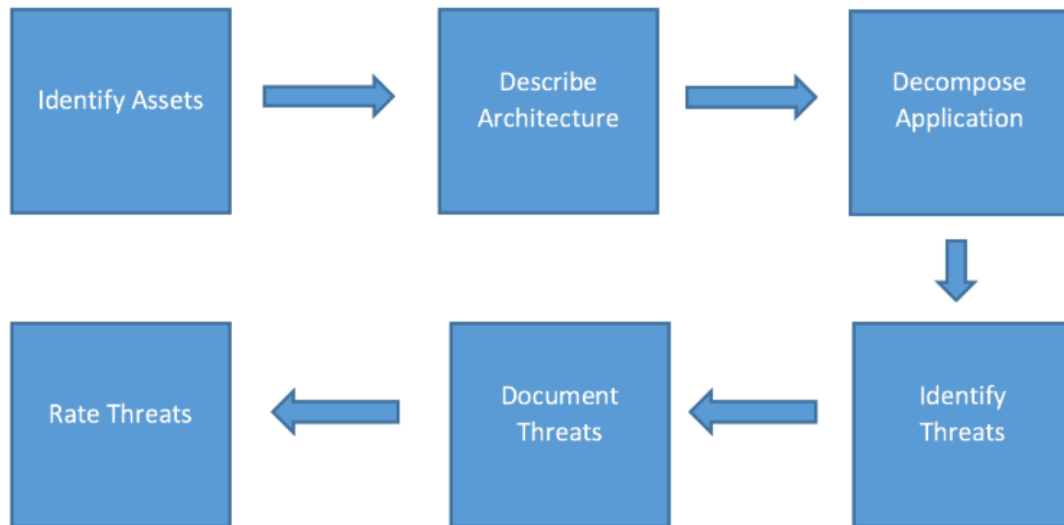
A security threat brainstorming activity

- Set aside the cards, and use the STRIDE model
- Consider what methods adversaries might use for attacking modern car systems
 - Either think about one car, or think about the entire car product line
 - Rank order the threats from most relevant
 - Explain your 3 top choices

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Threat Modeling

- Can be a full-time job for cyber security professionals
- Is now a skill information systems designers, developers and architects need to have



Agenda

- ✓ Information Systems – some definitions
- ✓ Conceptual models of information systems
- ✓ NIST Risk Management Framework
- ✓ FIPS 199 Security Categorization
- ✓ Transforming qualitative risk assessment into quantitative risk assessment
- ✓ FedRAMP System Security Plan – overview
 - ✓ NIST 800-53 Security controls
 - ✓ Role of FIPS 199 in selecting a security control baseline
 - ✓ NIST 800-18 classification of security control families
- ✓ Bonus: Threat Modeling exercise...