Unit #2

MIS5214

System Security Plan

Agenda

- Threat Modeling Exercise
- 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

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 – find threat modeling cards here:

Break up into teams:

- 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

- Optionally, outside of class review 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

- Optionally, outside of class review 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 model created by Microsoft, based on 6 types of threats:

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

STRIDE Threat Modeling

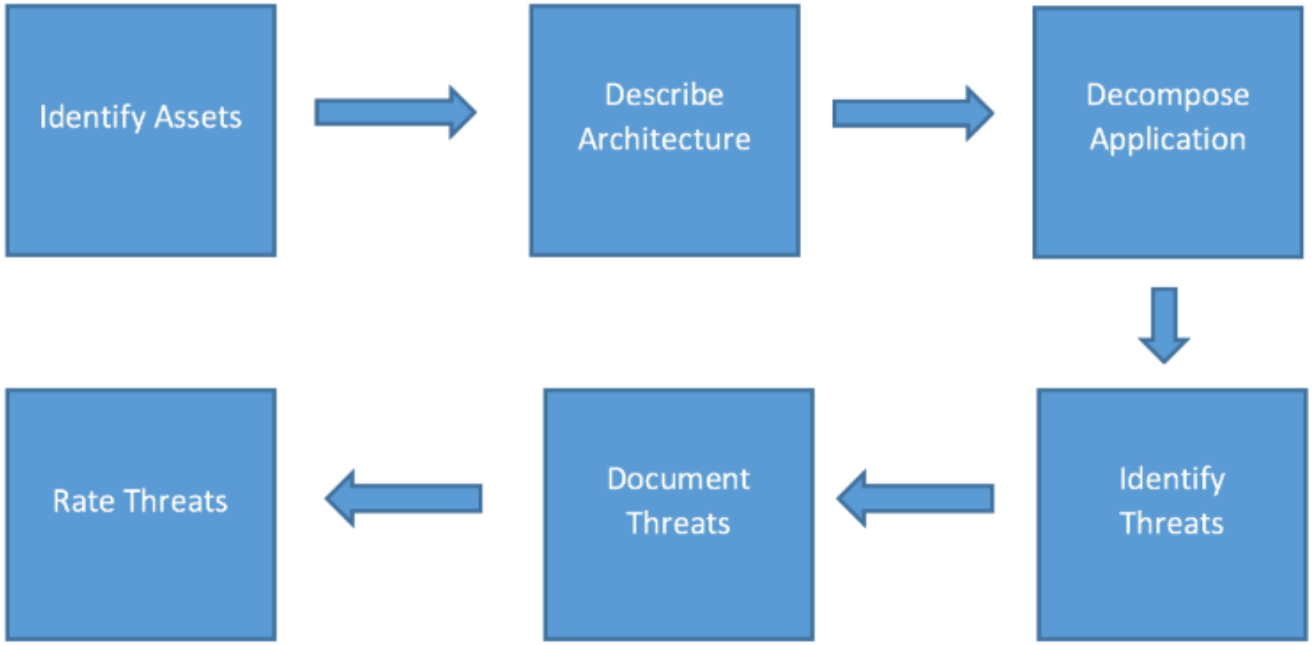
A security threat brainstorming activity

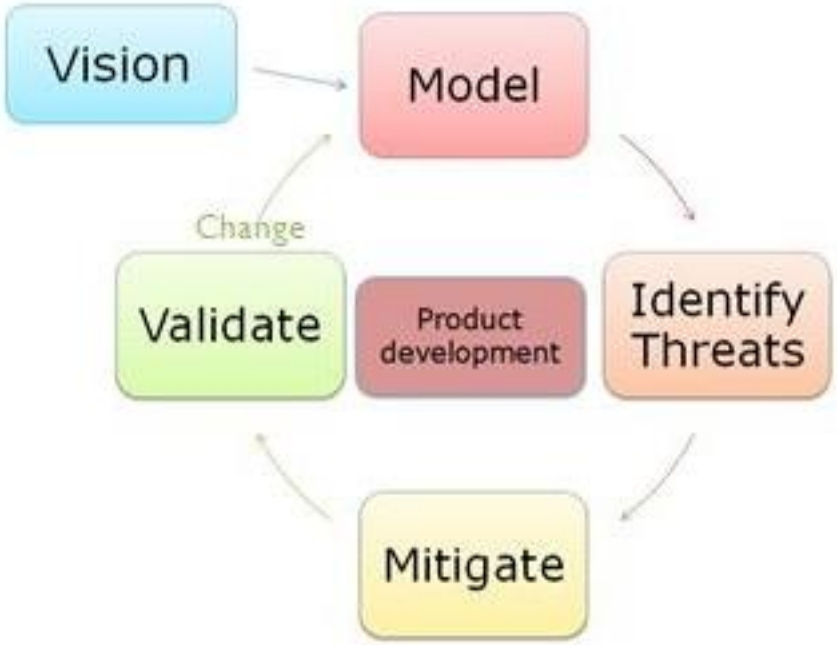
- Set aside the cards, and use the STRIDE model
- Consider what methods adversaries might use for attacking modern car systems
  1. Either think about one car, or think about the entire car product line
  2. Rank order the threats from most relevant
  3. Explain your 3 top choices

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

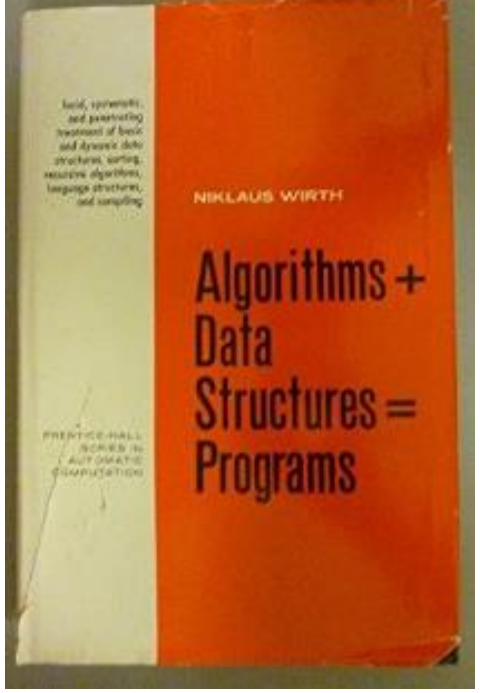




Agenda

- ✓Threat Modeling Exercise
- 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

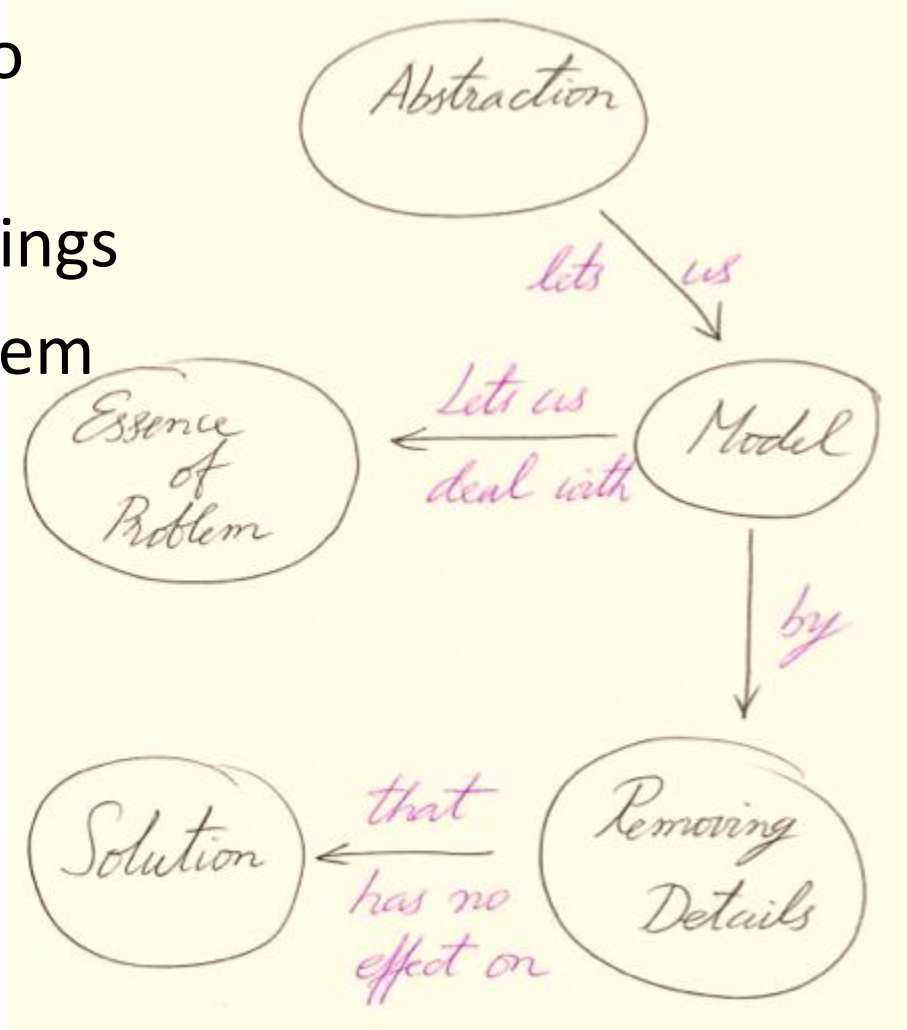
- **Software** are programs used to direct the operation of a computer
- **Hardware** are tangible physical parts of a computer system and IT network
- **Firmware** is software embedded in a piece of hardware
- **Information systems** are software and hardware systems that support data-intensive applications
- **Enterprise information system** is an information system which enable an organization to integrate and improve its business functions

Information System Architecture

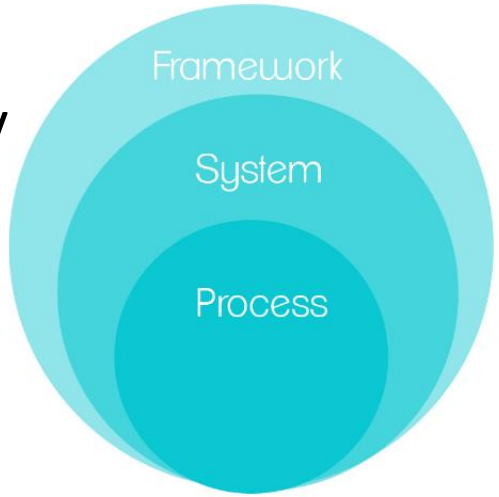
- Is an **abstraction** that provides the “big picture” goals for the system
  - Guides the development process, answering questions including:
    - How is it going to be used?
    - What environment will it work within?
    - What type of security and protection is required?
    - What does it need to be able to communicate with?
  - Describes the major components of the system and how they interact with each other, with the users, and with other systems

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 ?



- An abstraction of things for the purpose of understanding them
- Enables dealing with systems that are too complex to understand directly
- Omits 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*
- Aids 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*
- Serves 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

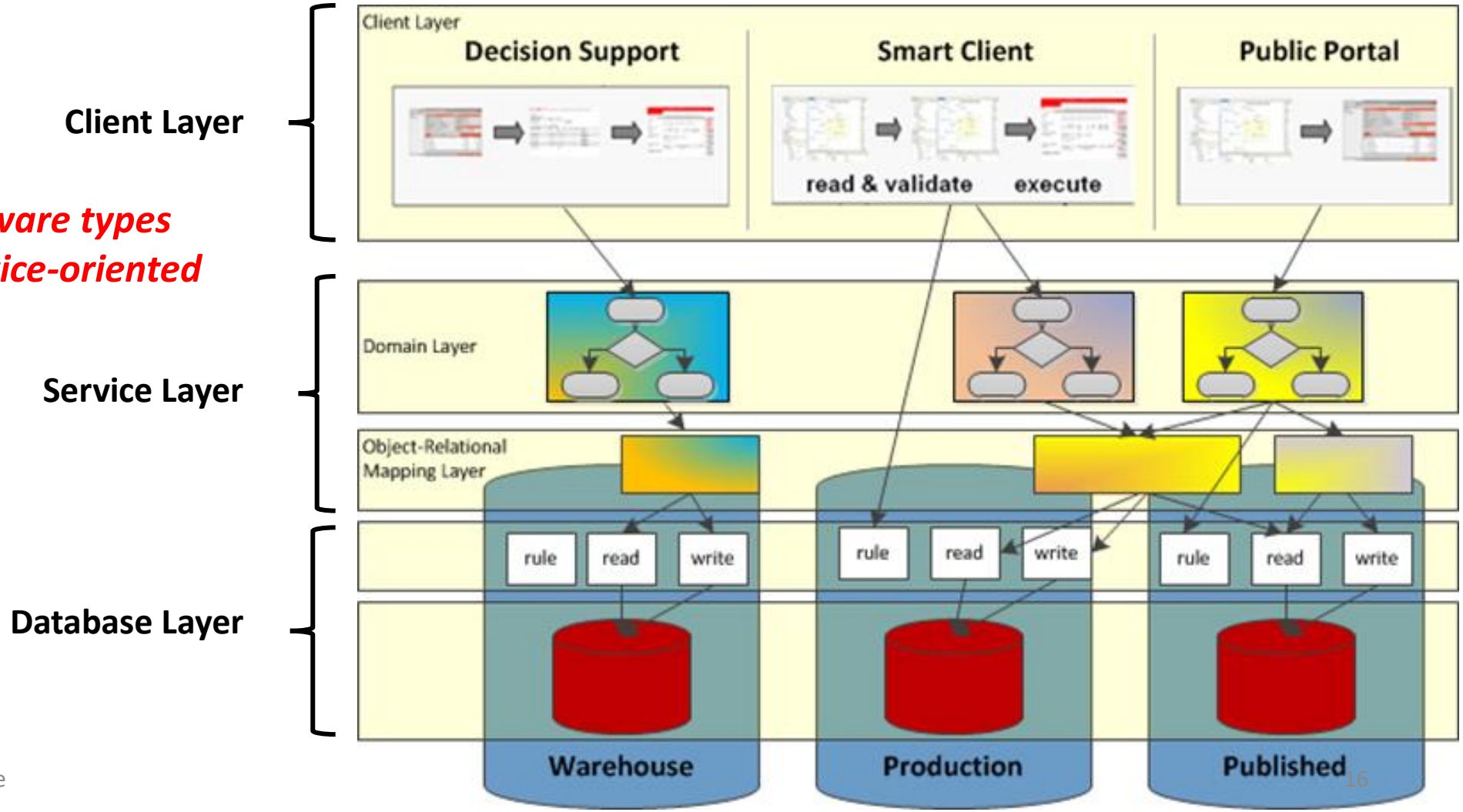
- Classification
- Aggregation
- Generalization
- *Can you think of any others?*

Abstractions help the designer understand, classify, and model reality

Classification

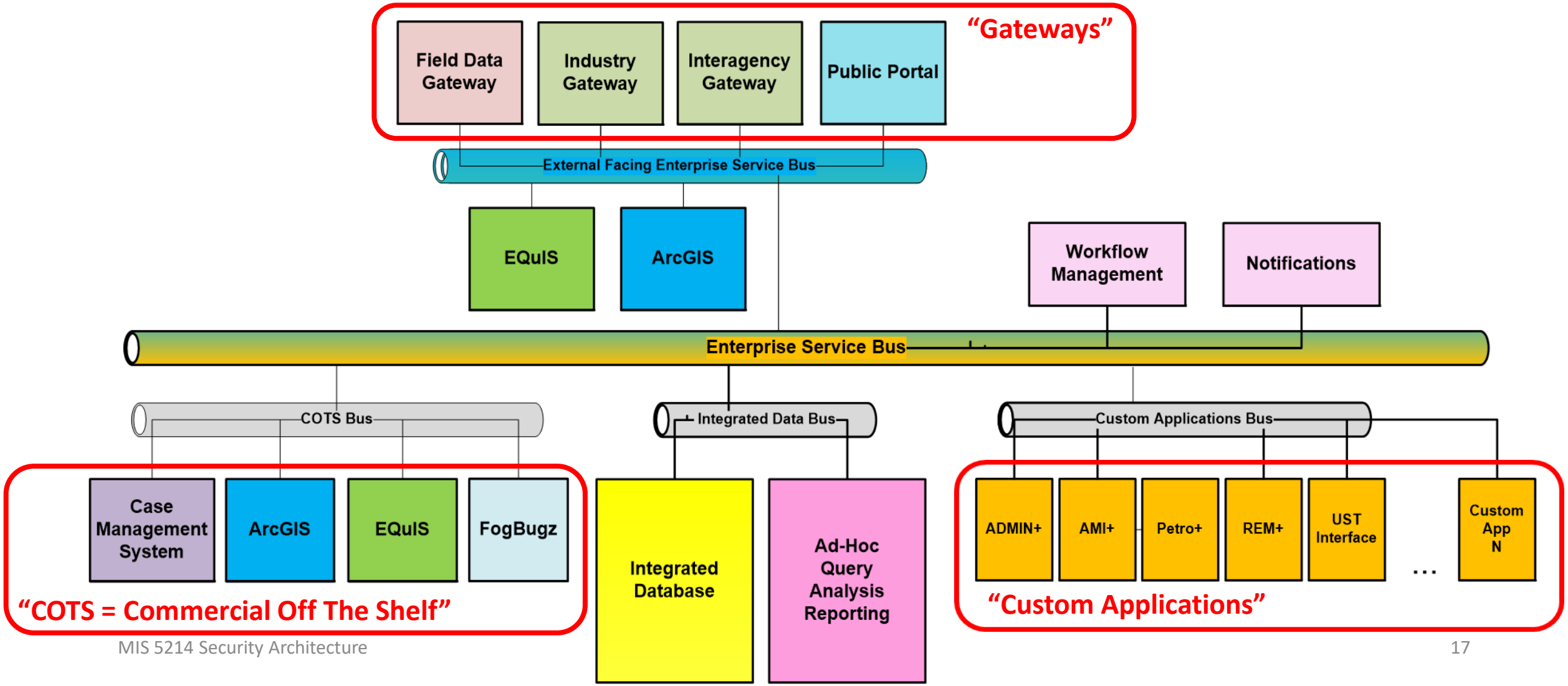
- An abstraction used to define one concept as a class of real-world objects characterized by common properties

Example: 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 it components

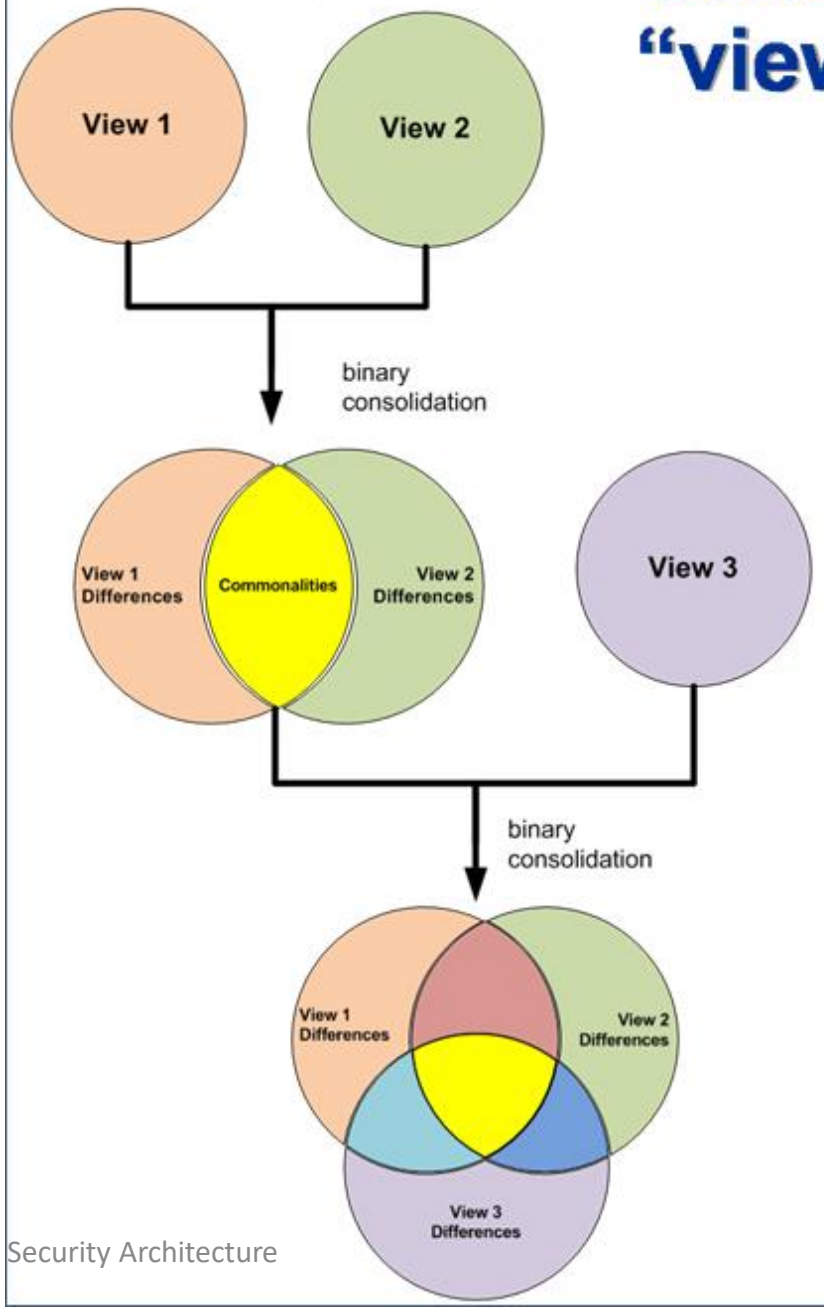


Classification and Aggregation

Are 2 basic abstractions used for:

- **Building data structures** within databases and programming languages
- **Building and organizing computational processes** within applications
- **Building and organizing applications** within systems
- **Building and organizing applications and minor systems** within major systems

consolidation methodology "view integration"



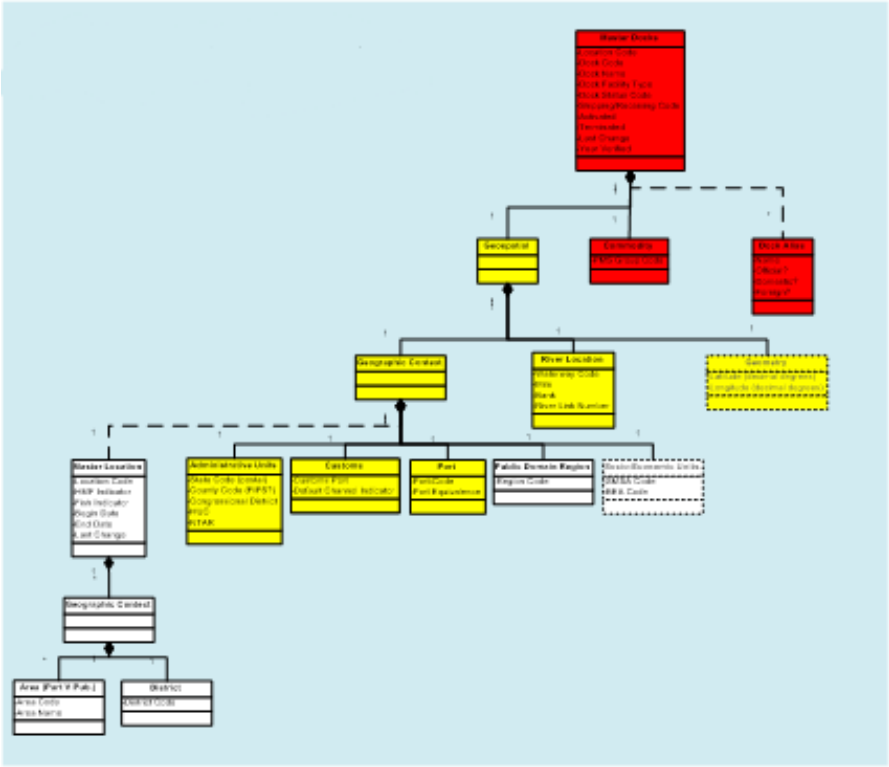
model integration achieved by:

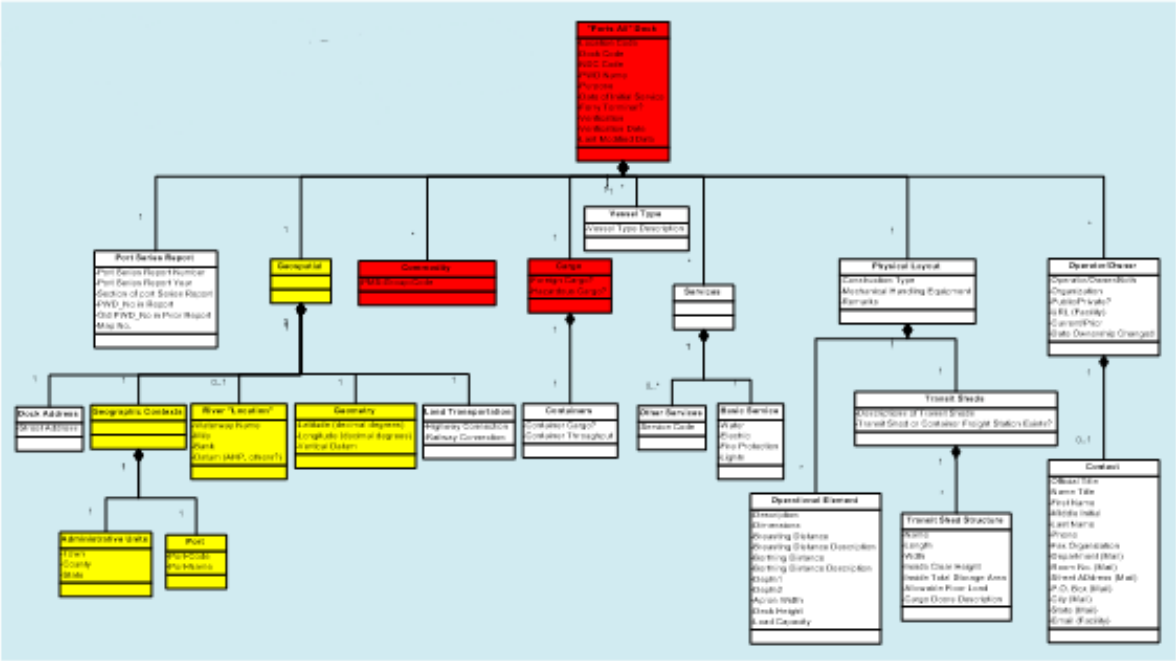
1. Identifying,
2. Resolving, and
3. Consolidating

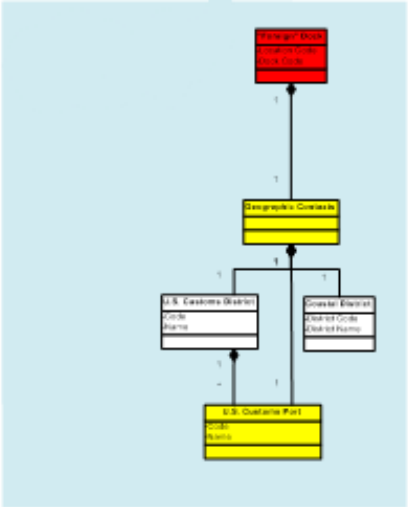
- **Commonalities** (and synonyms)

and

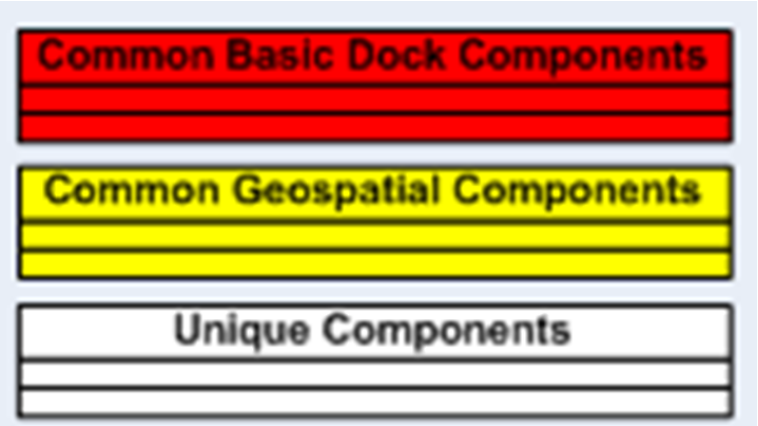
- **Differences** (and homonyms)

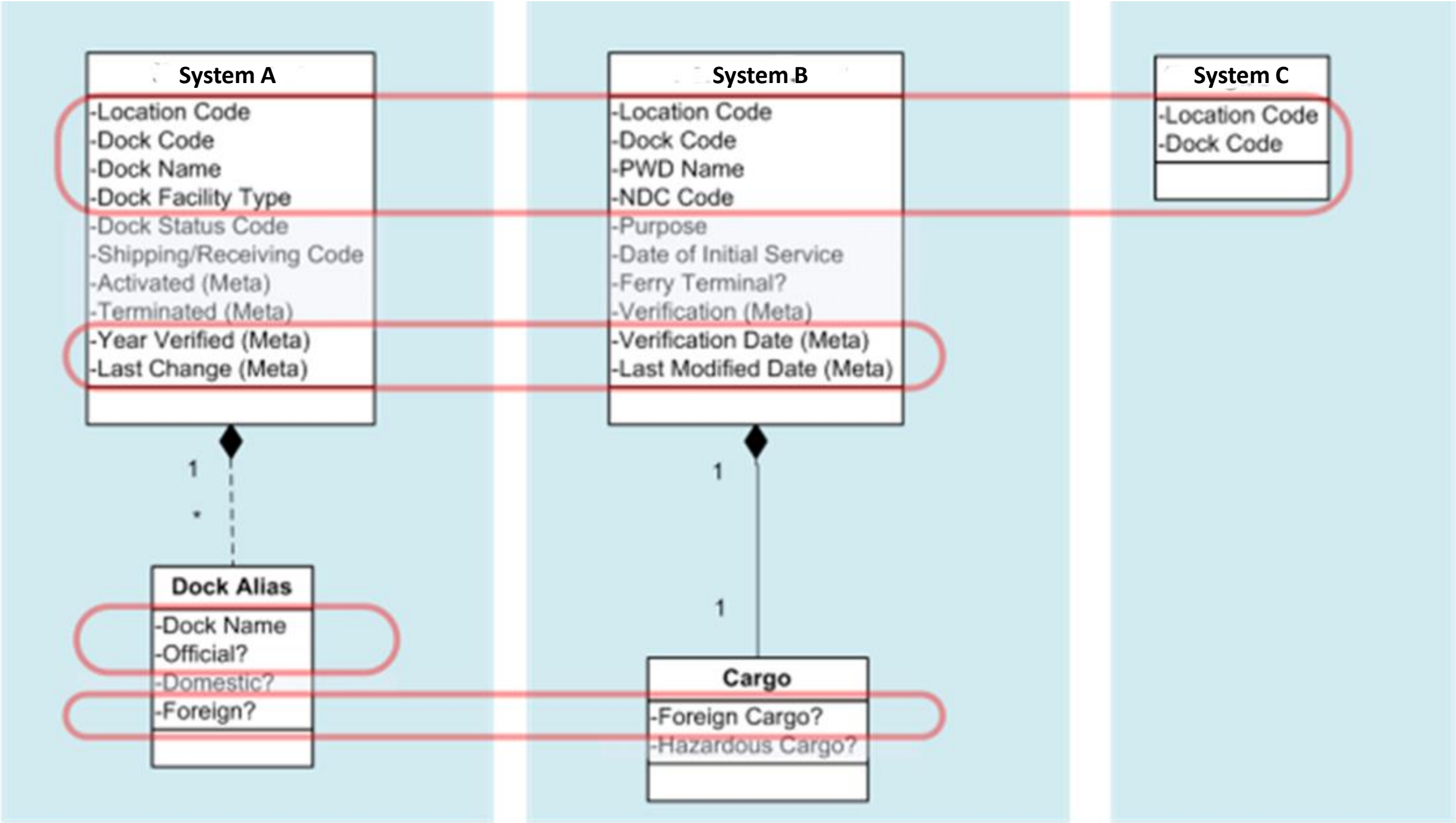


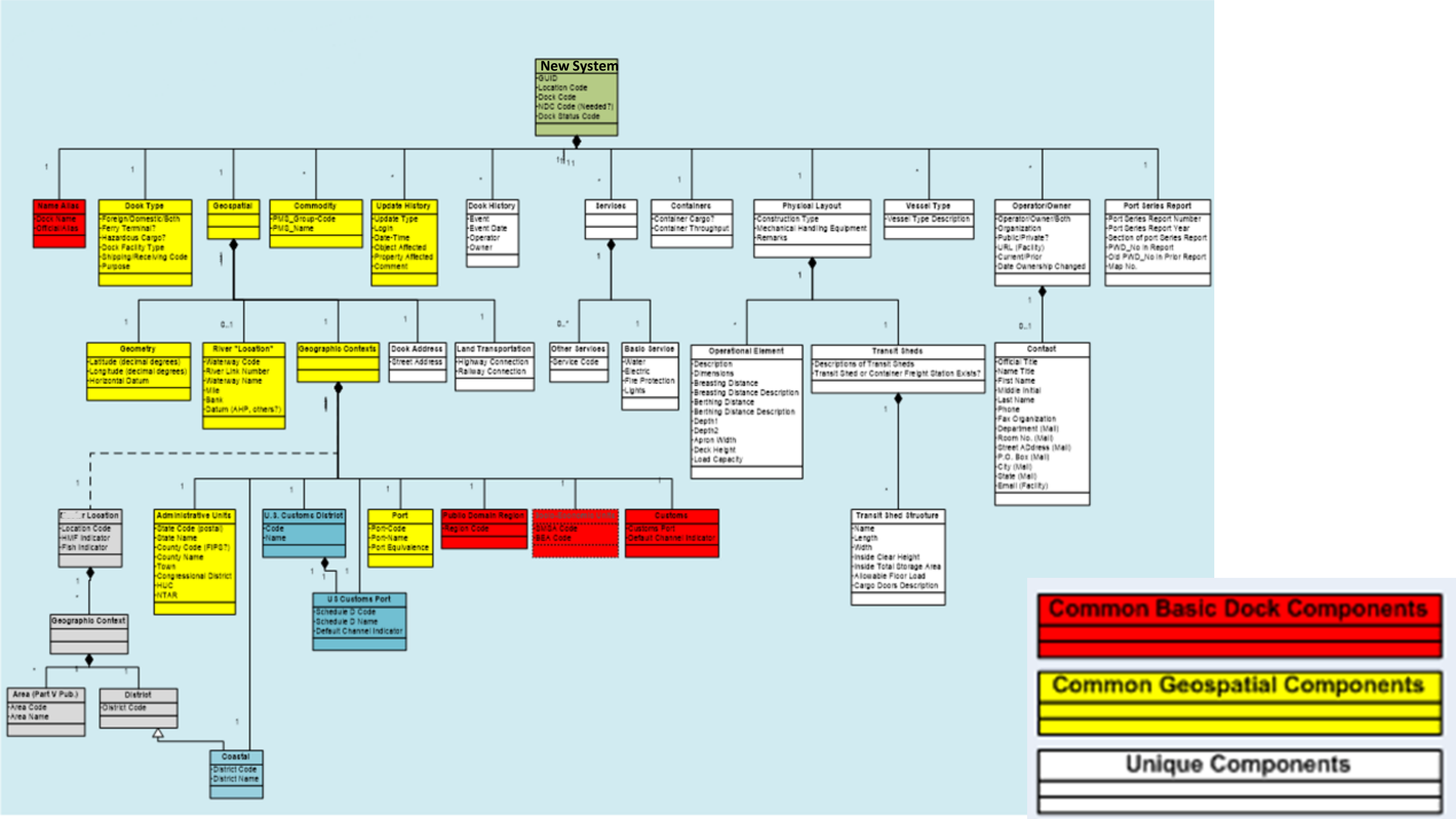




Information models from disparate business units




System A
-Location Code
-Dock Code
-Dock Name
-Dock Facility Type
-Dock Status Code
-Shipping/Receiving Code
-Activated (Meta)
-Terminated (Meta)
-Year Verified (Meta)
-Last Change (Meta)
1
*
Dock Alias
-Dock Name
-Official?
-Domestic?
-Foreign?
System B
-Location Code
-Dock Code
-PWD Name
-NDC Code
-Purpose
-Date of Initial Service
-Ferry Terminal?
-Verification (Meta)
-Verification Date (Meta)
-Last Modified Date (Meta)
1
1
Cargo
-Foreign Cargo?
-Hazardous Cargo?
System C
-Location Code
-Dock Code

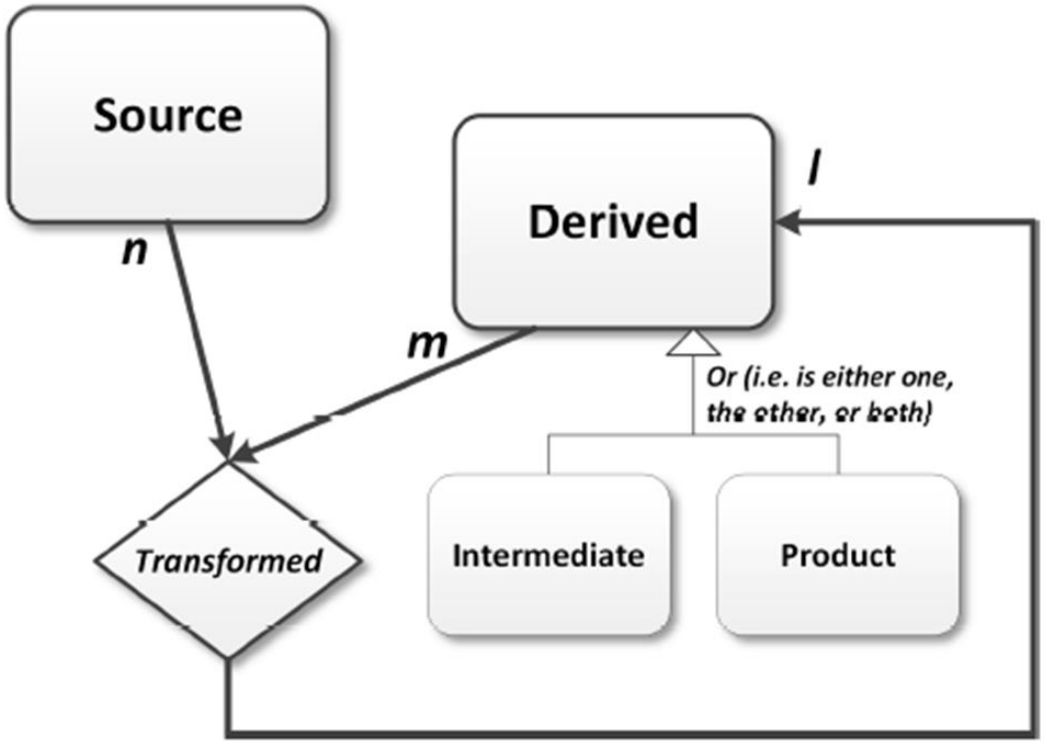

New System
GUID
Location Code
Dock Code
NDC Code (Needed?)
Dock Status Code
Name Alias
Dock Name
Official Alias
Dock Type
Foreign/Domestic/Both
Ferry Terminal?
Hazardous Cargo?
Dock Facility Type
Shipping/Receiving Code
Purpose
Geospatial
Commodity
PWD_Group-Code
PWD_Name
Update History
Update Type
Login
Date-Time
Object Affected
Property Affected
Comment
Dock History
Event
Event Date
Operator
Owner
Services
Containers
Container Cargo?
Container Throughput
Physical Layout
Construction Type
Mechanical Handling Equipment
Remarks
Vessel Type
Vessel Type Description
Operator/Owner
Operator/Owner/Both
Organization
Public/Private?
URL (Facility)
Current/Prior
Date Ownership Changed
Port Series Report
Port Series Report Number
Port Series Report Year
Section of port Series Report
PWD_No in Report
Old PWD_No in Prior Report
Map No.
Geometry
Latitude (decimal degrees)
Longitude (decimal degrees)
Horizontal Datum
River "Location"
Waterway Code
River Link Number
Waterway Name
Mile
Bank
Datum (AHP, others?)
Geographic Contexts
Dock Address
Street Address
Land Transportation
Highway Connection
Railway Connection
Other Services
Service Code
Basic Service
Water
Electric
Fire Protection
Lights
Operational Element
Description
Dimensions
Breasting Distance
Breasting Distance Description
Berthing Distance
Berthing Distance Description
Depth1
Depth2
Apron Width
Deck Height
Load Capacity
Transit Sheds
Descriptions of Transit Sheds
Transit Shed or Container Freight Station Exists?
Contact
Official Title
Name Title
First Name
Middle Initial
Last Name
Phone
Fax Organization
Department (Mail)
Room No. (Mail)
Street Address (Mail)
P.O. Box (Mail)
City (Mail)
State (Mail)
Email (Facility)
Location
Location Code
HUF Indicator
Fish Indicator
Administrative Units
State Code (postal)
State Name
County Code (FIPS?)
County Name
Town
Congressional District
HUC
NTAR
U.S. Customs District
Code
Name
Port
Port-Code
Port-Name
Port Equivalence
Public Domain Region
Region Code
SMSA Code
BEA Code
Customs
Customs Port
Default Channel Indicator
Transit Shed Structure
Name
Length
Width
Inside Clear Height
Inside Total Storage Area
Allowable Floor Load
Cargo Doors Description
Geographic Context
Area (Part V Pub.)
Area Code
Area Name
District
District Code
Coastal
District Code
District Name
U S Customs Port
Schedule D Code
Schedule D Name
Default Channel Indicator
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 abstract properties defined for the general generic class (super-class) are inherited by all the subset specialized classes (sub-class)

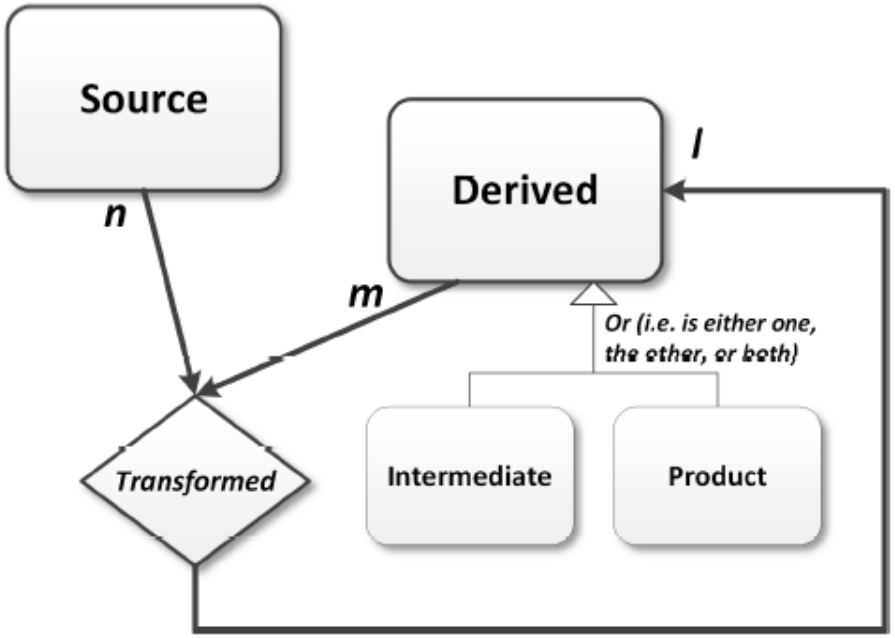
$$Datasets = \{Dataset_i : i = source,\ derived\},$$

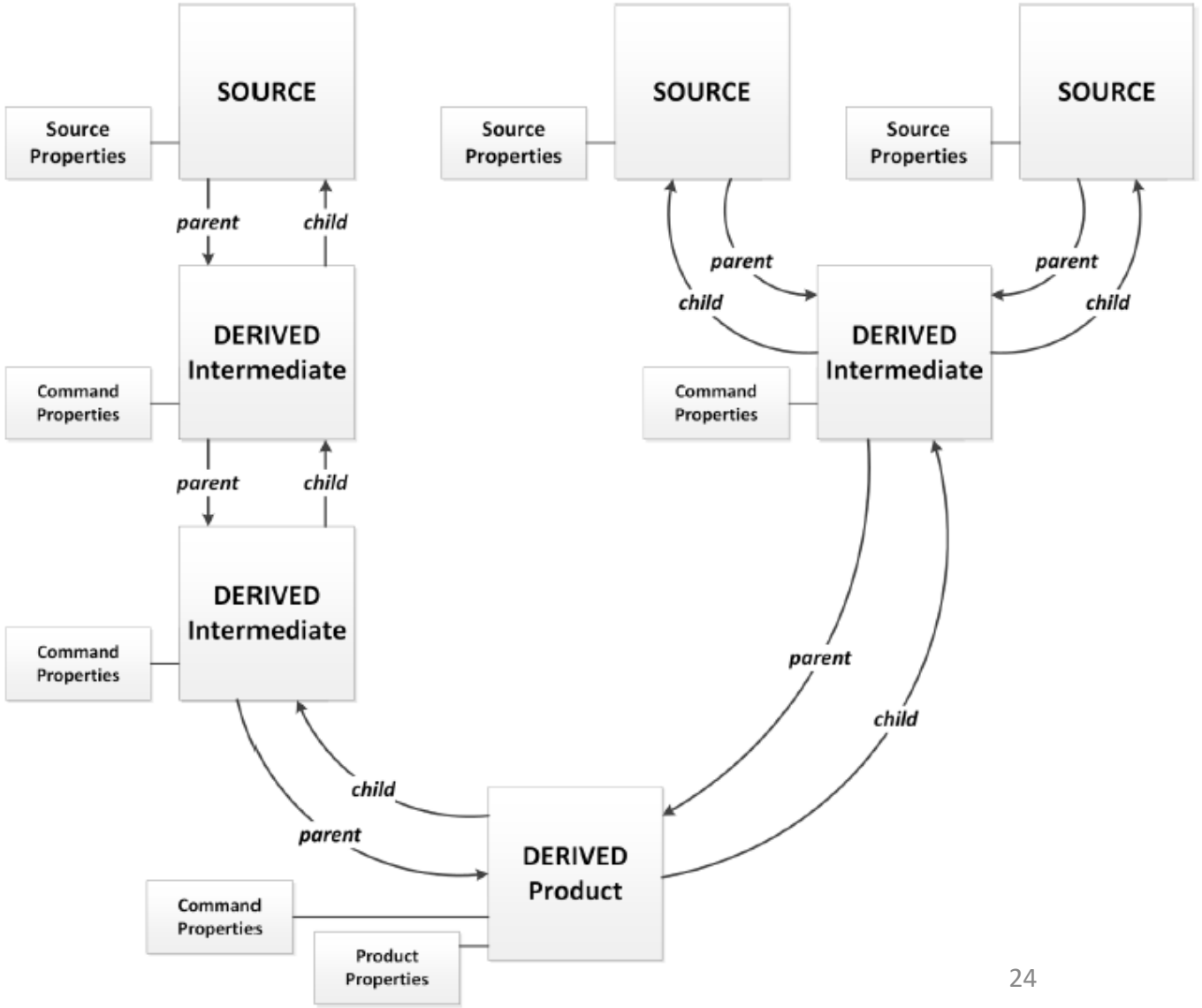
$$Dataset_{derived} = \{Dataset_{derived.k} : k = intermediate,\ product\}.$$



Data lineage metadata model

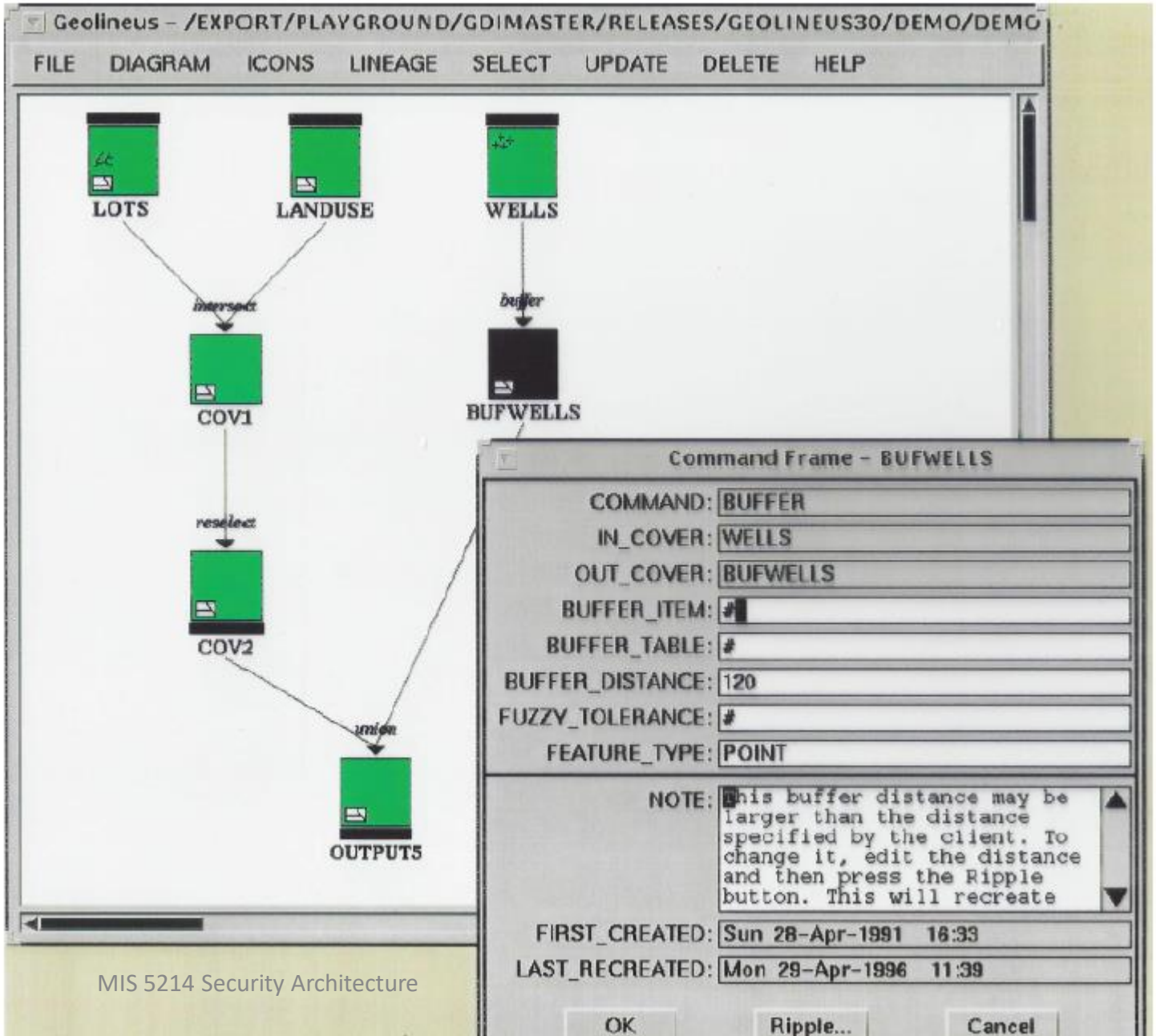
Generalization enables partitioning objects and structuring common properties and methods

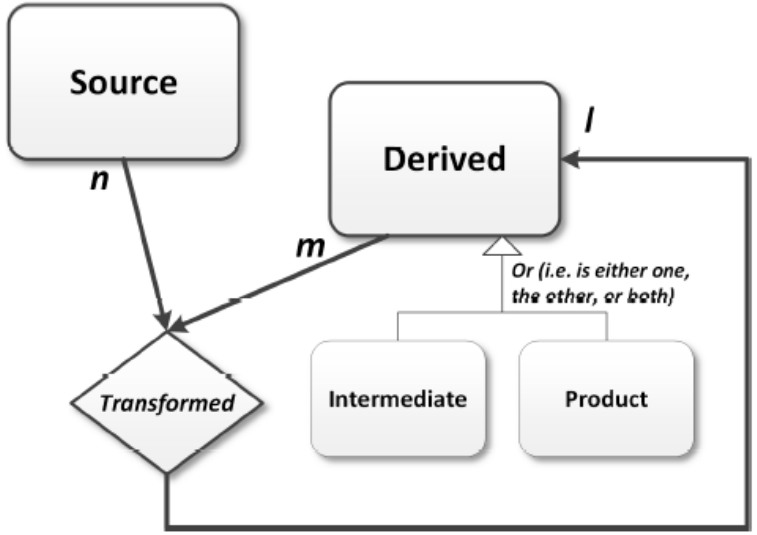


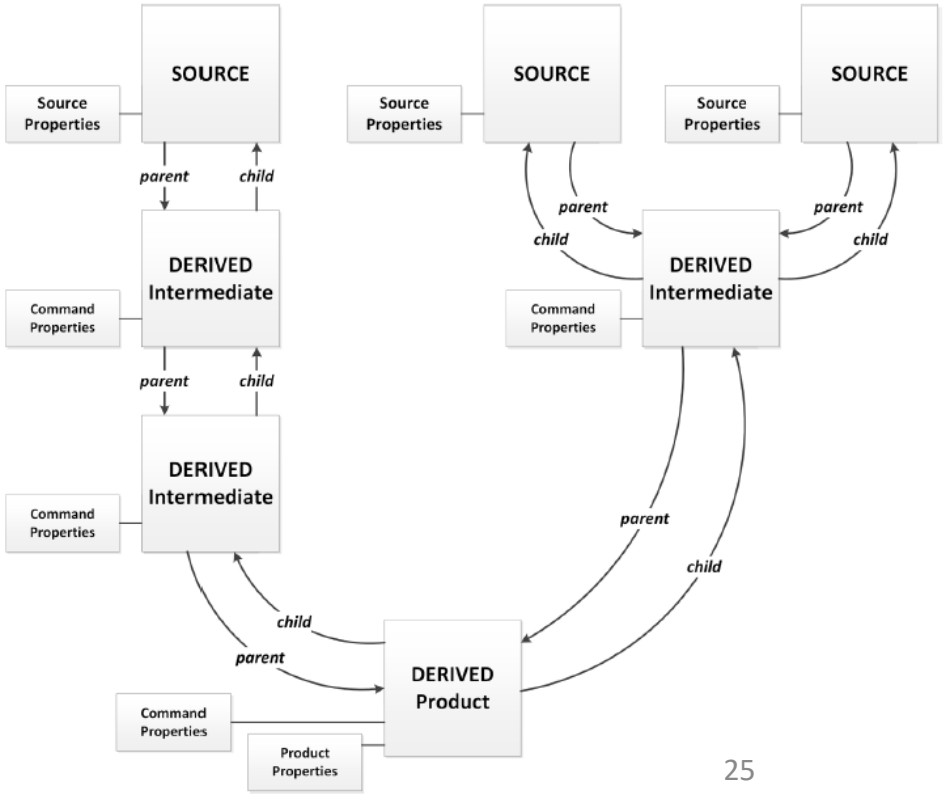


Example of generalizations of different types of datasets

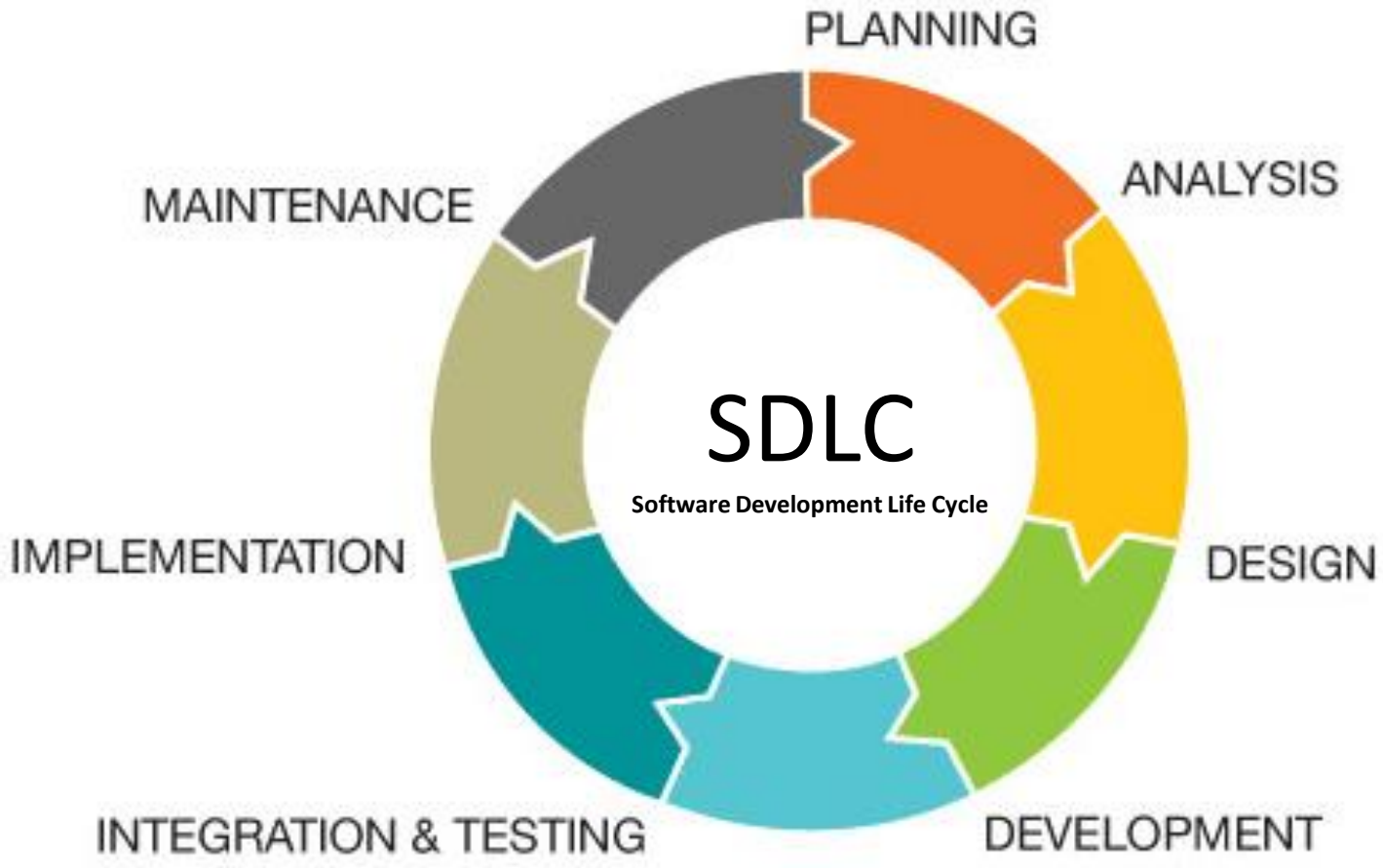
Data Provenance Metadata System

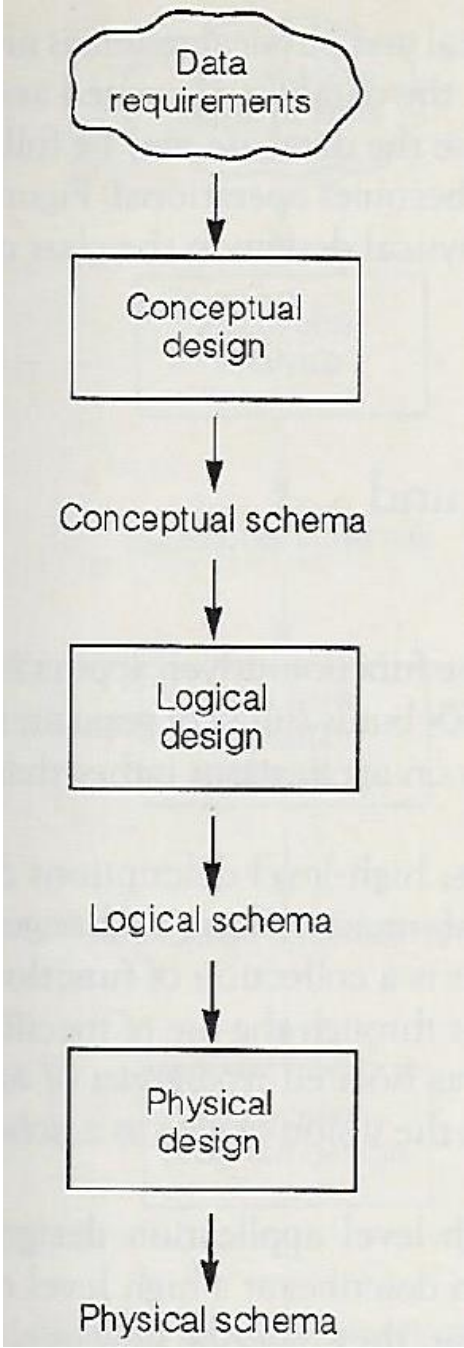






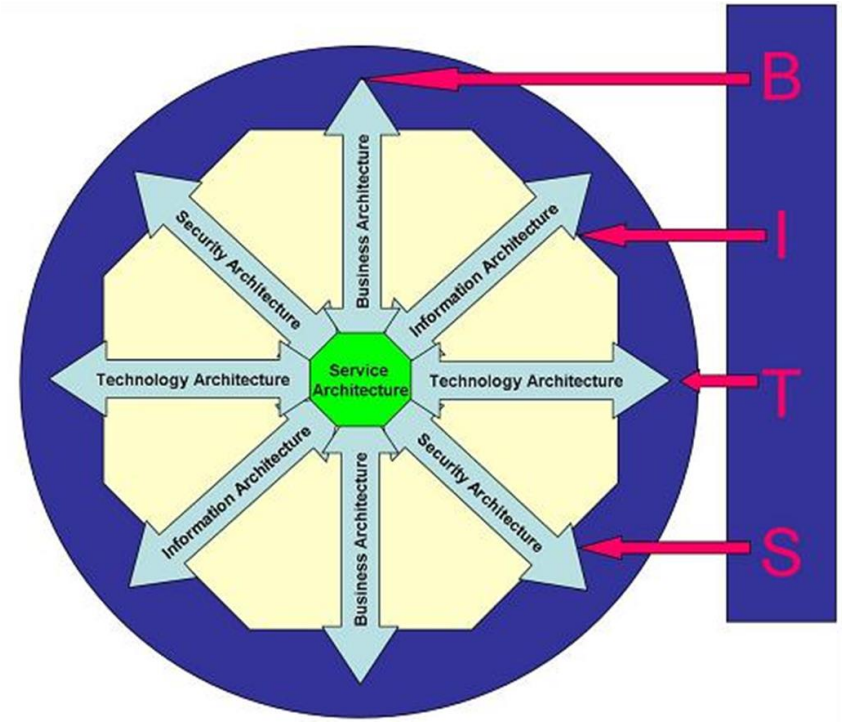
Conceptual models of information system design and development…





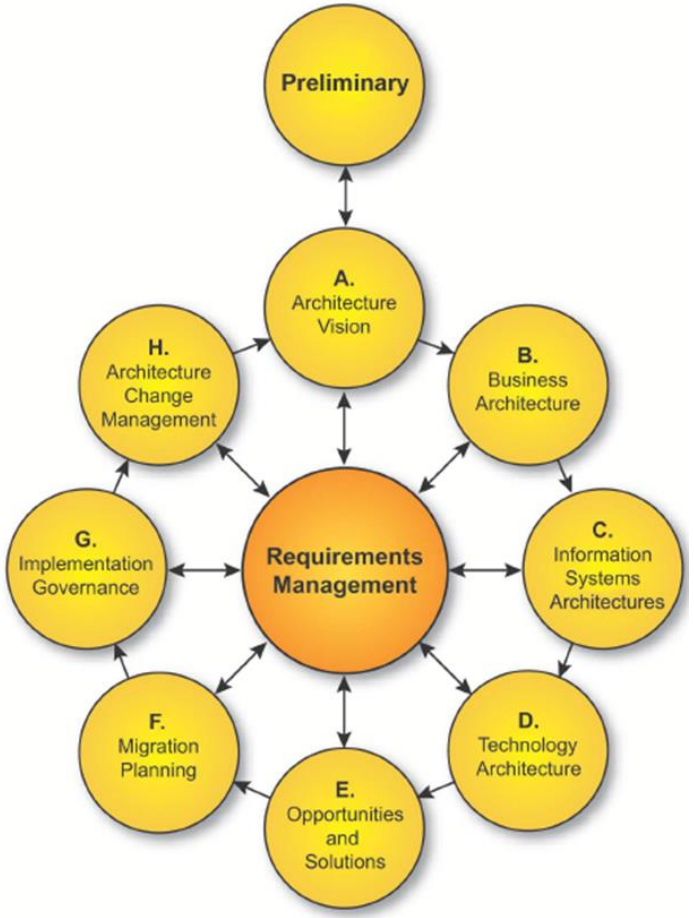
Database design

Models help us understand enterprise information systems and their security



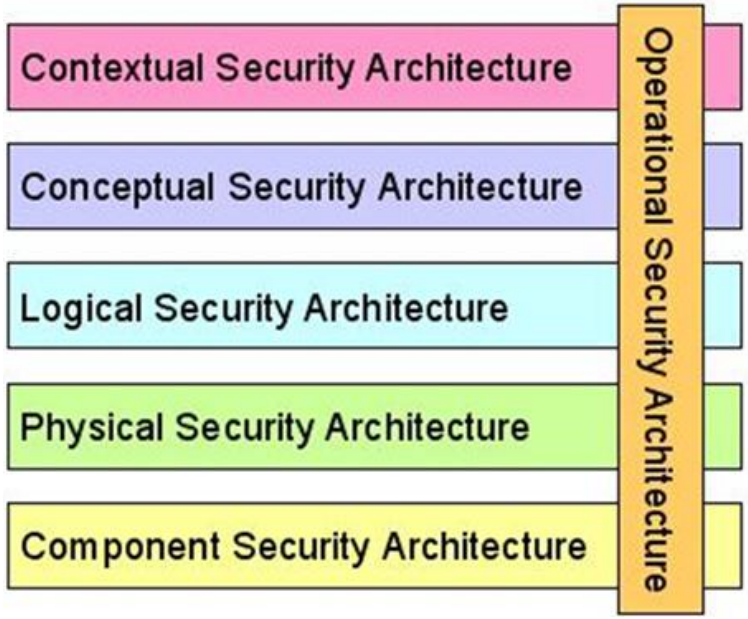
Horatio Huxham's BITS

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



The Open Data Group Architecture Framework (TOGAF) Version 9.1

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



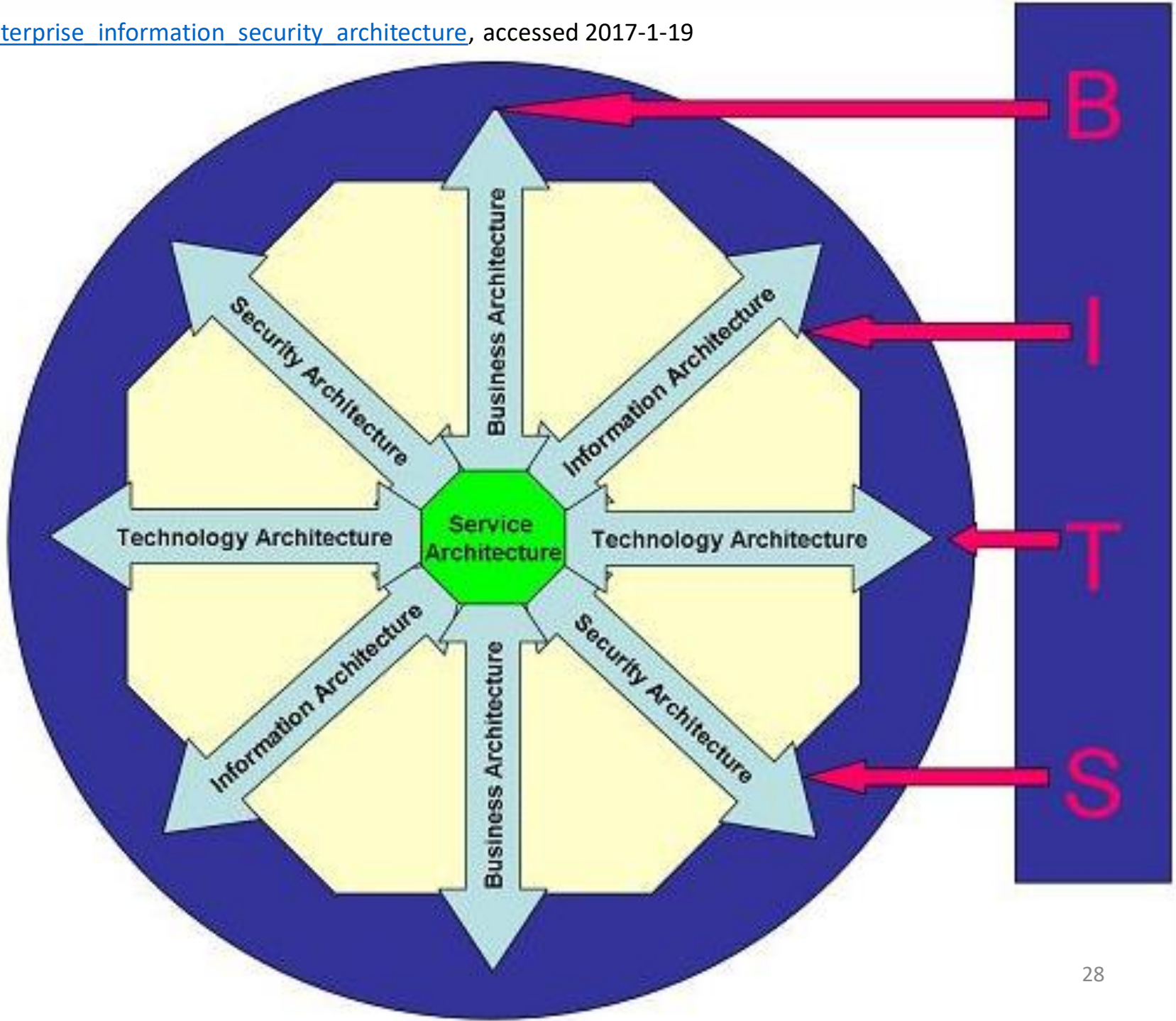
Sherwood Applied Business Security Architecture (SABSA)

http://www.sabsa.org/white_paper

Wikipedia: https://en.wikipedia.org/wiki/Enterprise_information_security_architecture, accessed 2017-1-19

Enterprise architecture consists of:

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

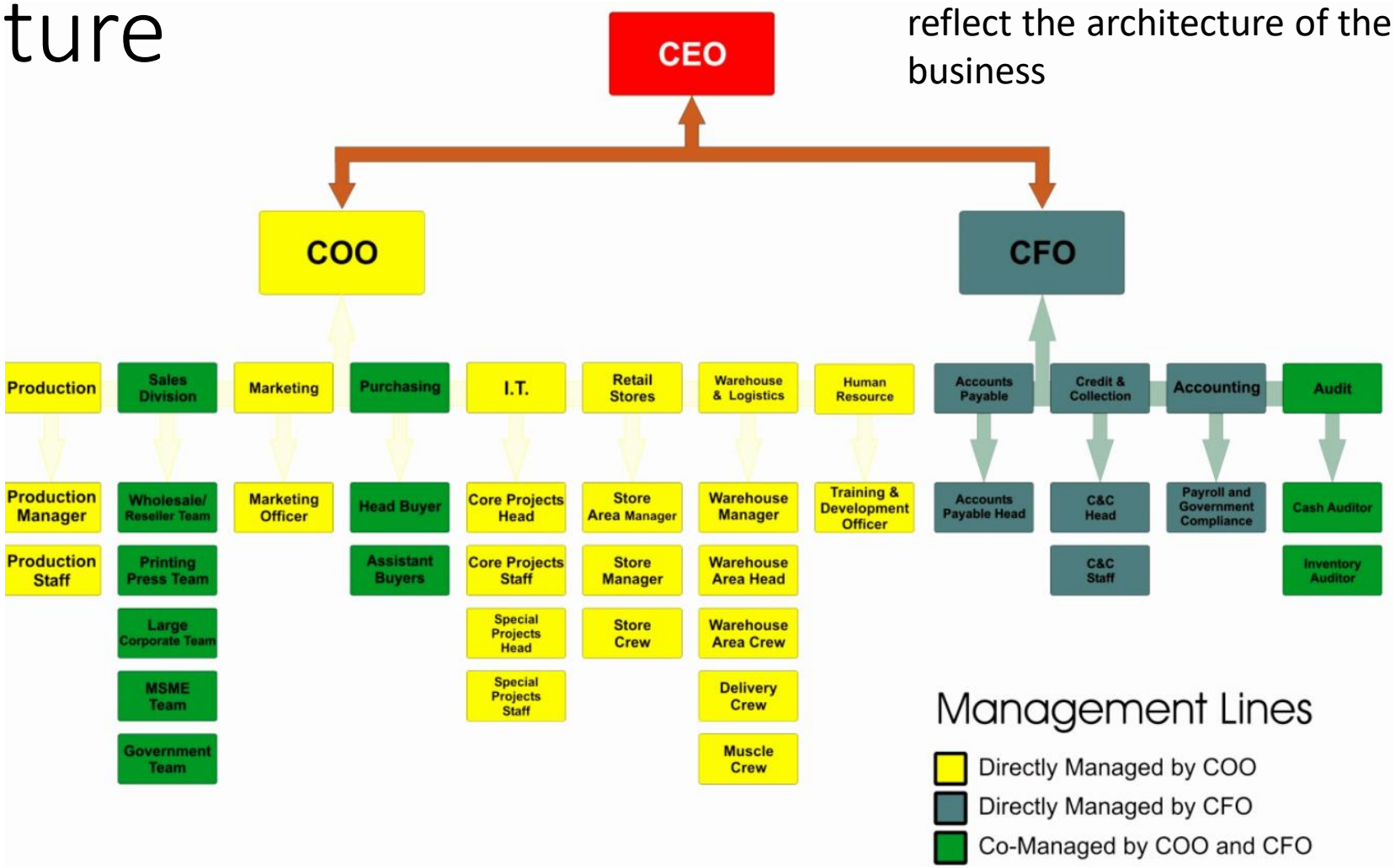


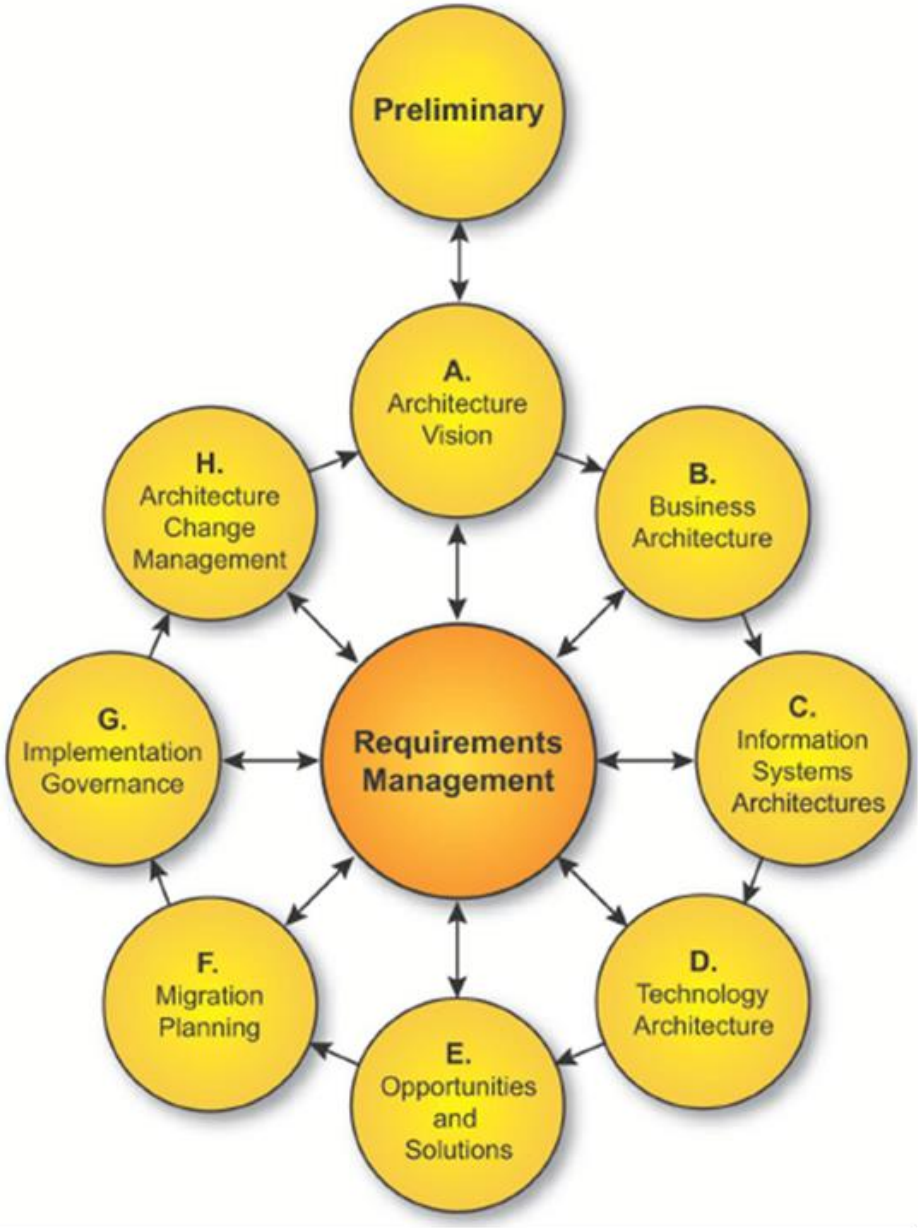
Horatio Huxham's BITS

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

Business Architecture

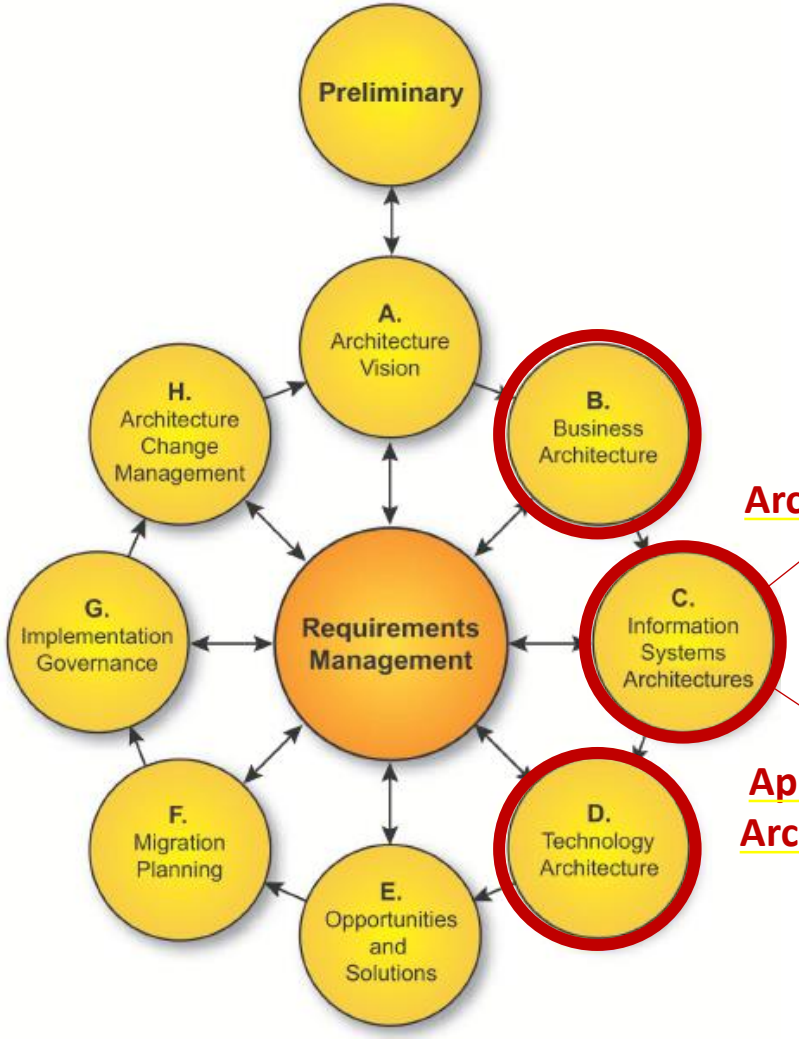
An organization chart may reflect the architecture of the business





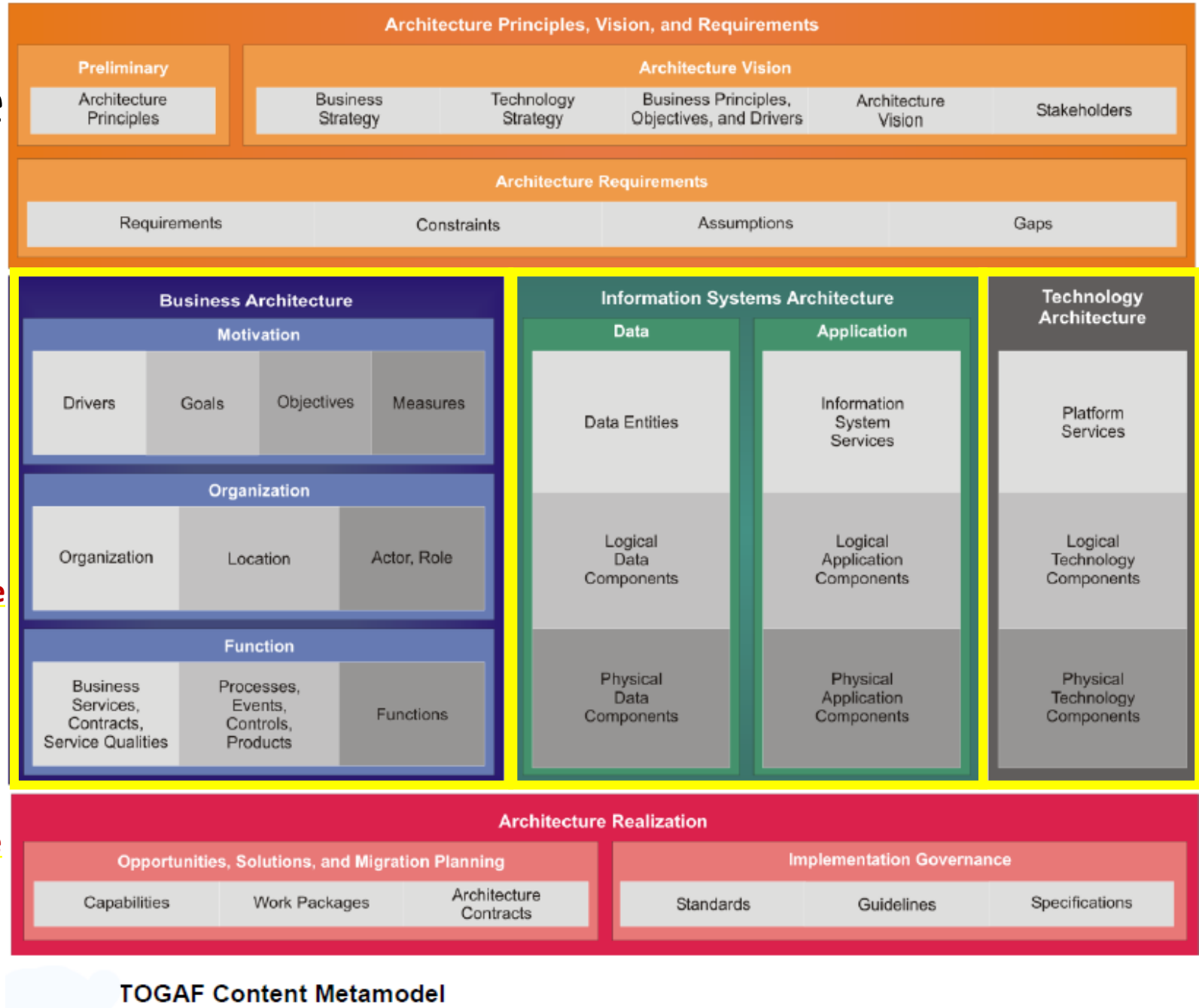
The Open Data Group Architecture Framework (TOGAF) Version 9.1

Information Architecture



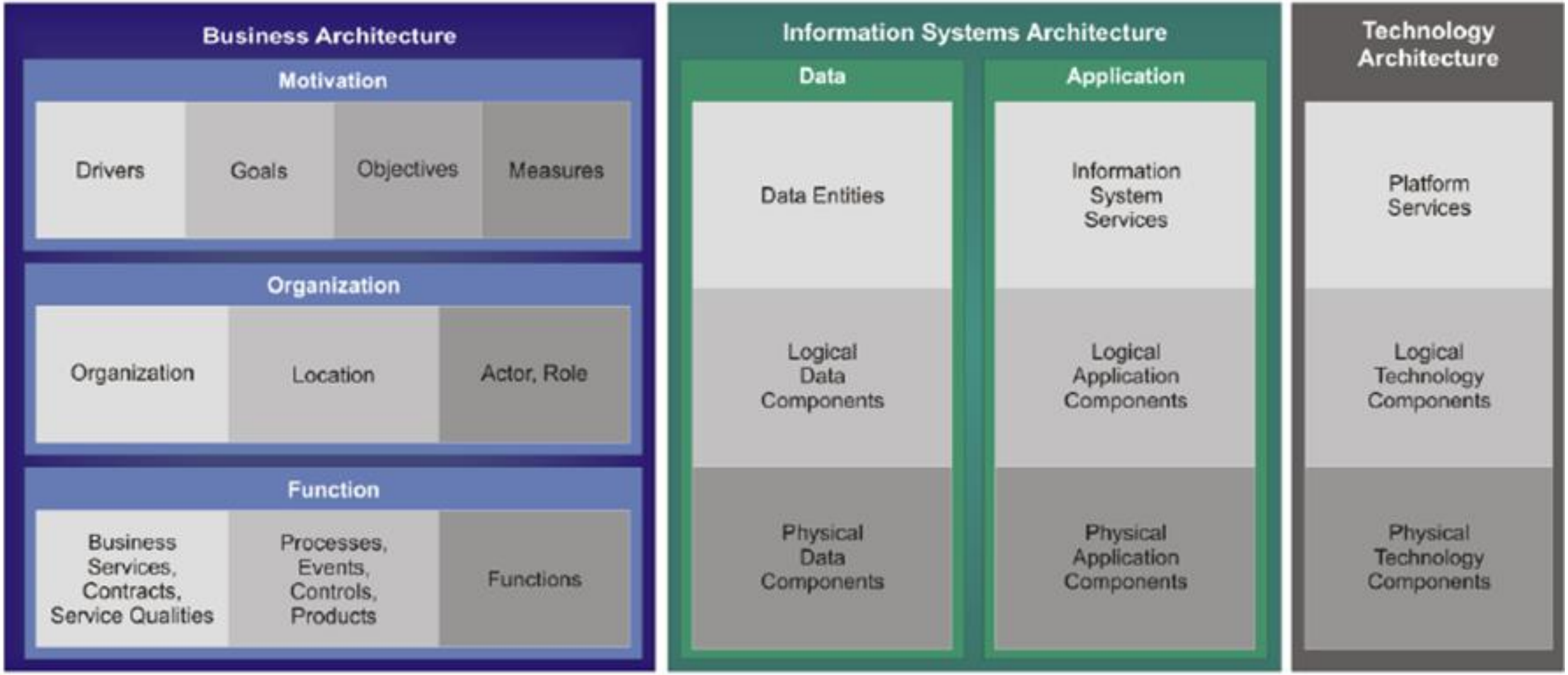
Data Architecture

Application Architecture

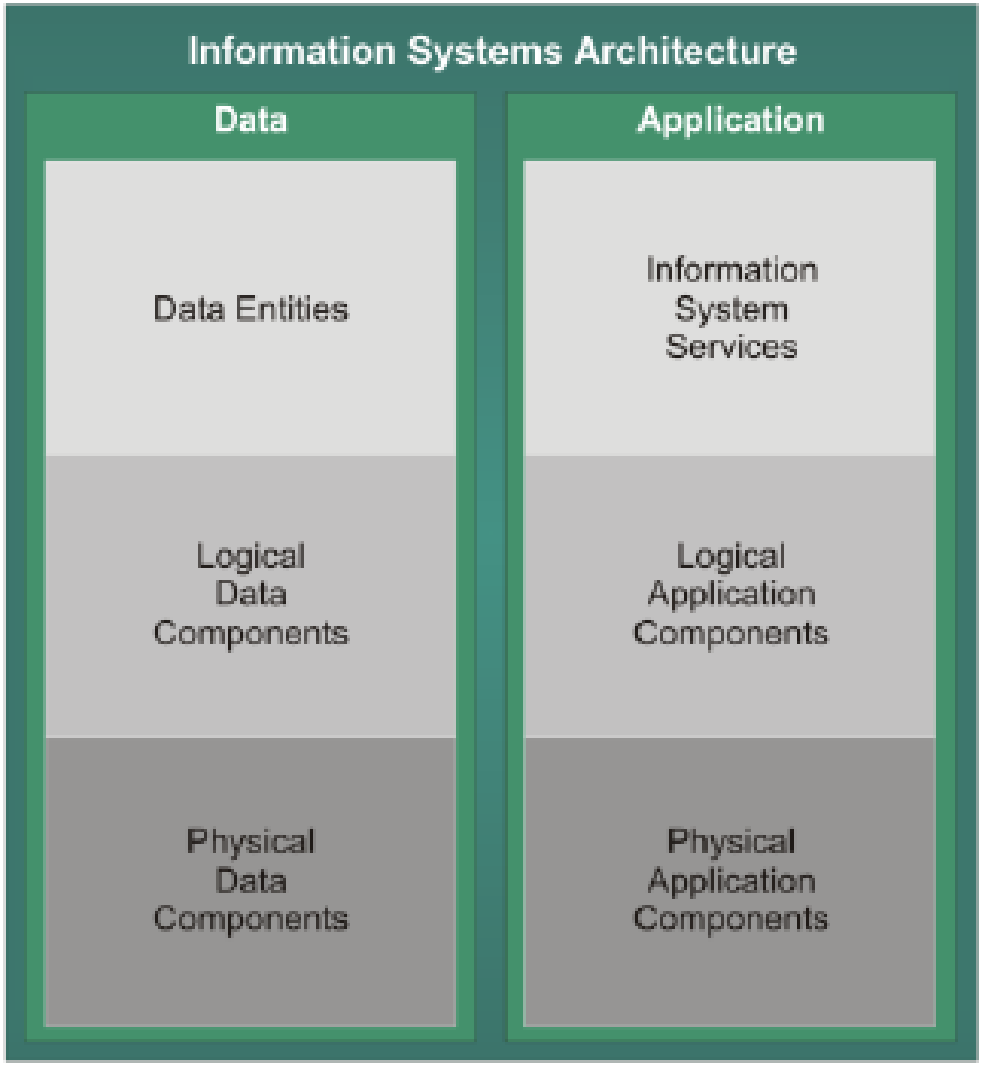


TOGAF Content Metamodel

Information Architecture

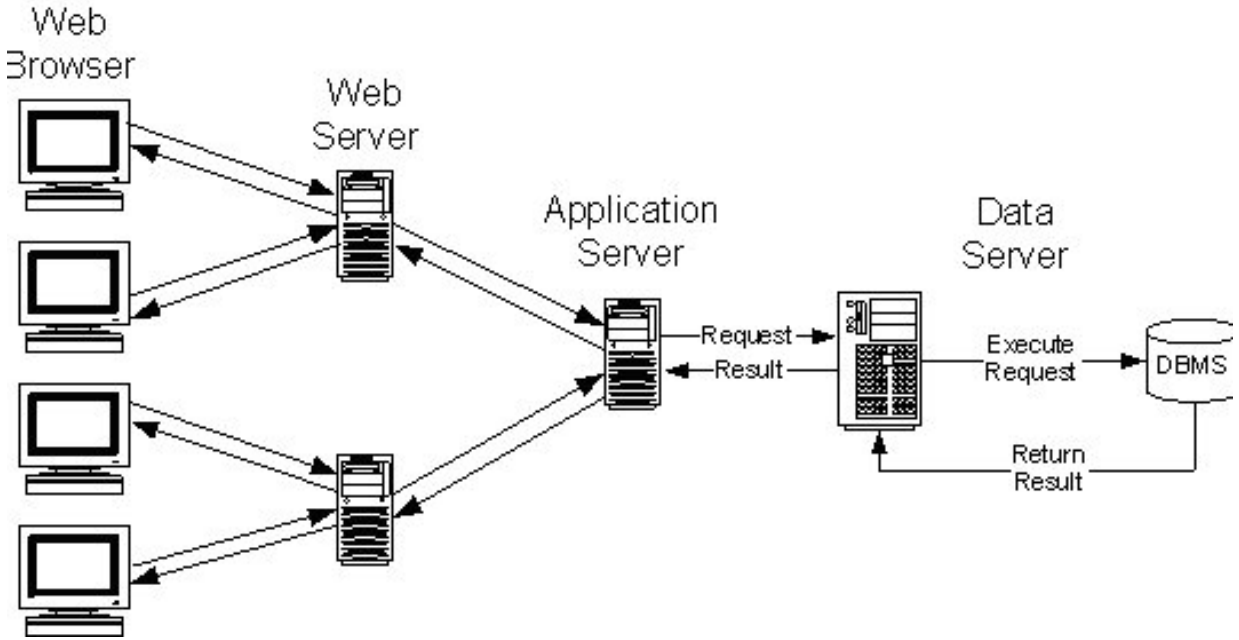


Conceptual models of Information Systems

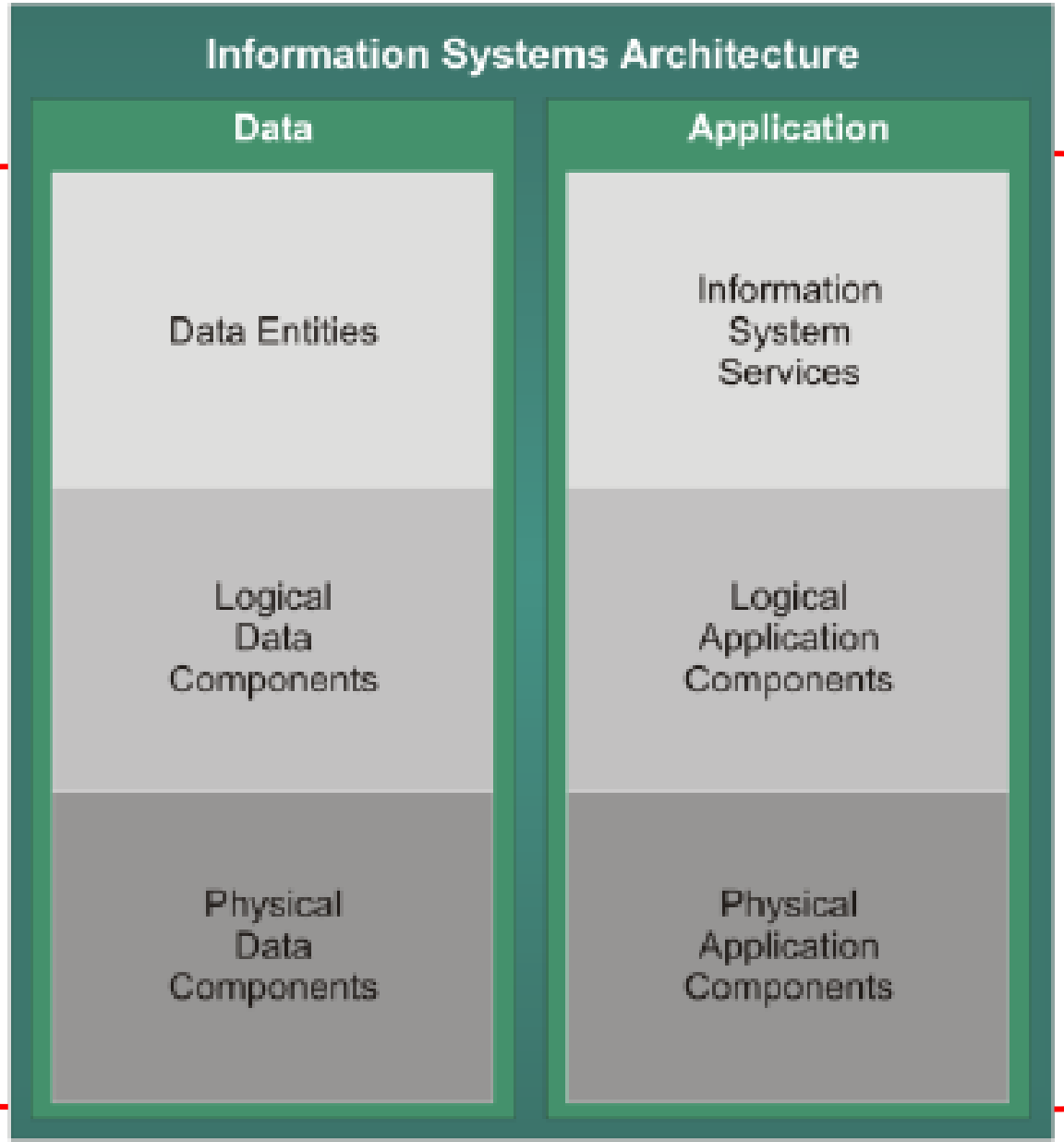


Content & Structure

Function & Use



Conceptual models of Information Systems

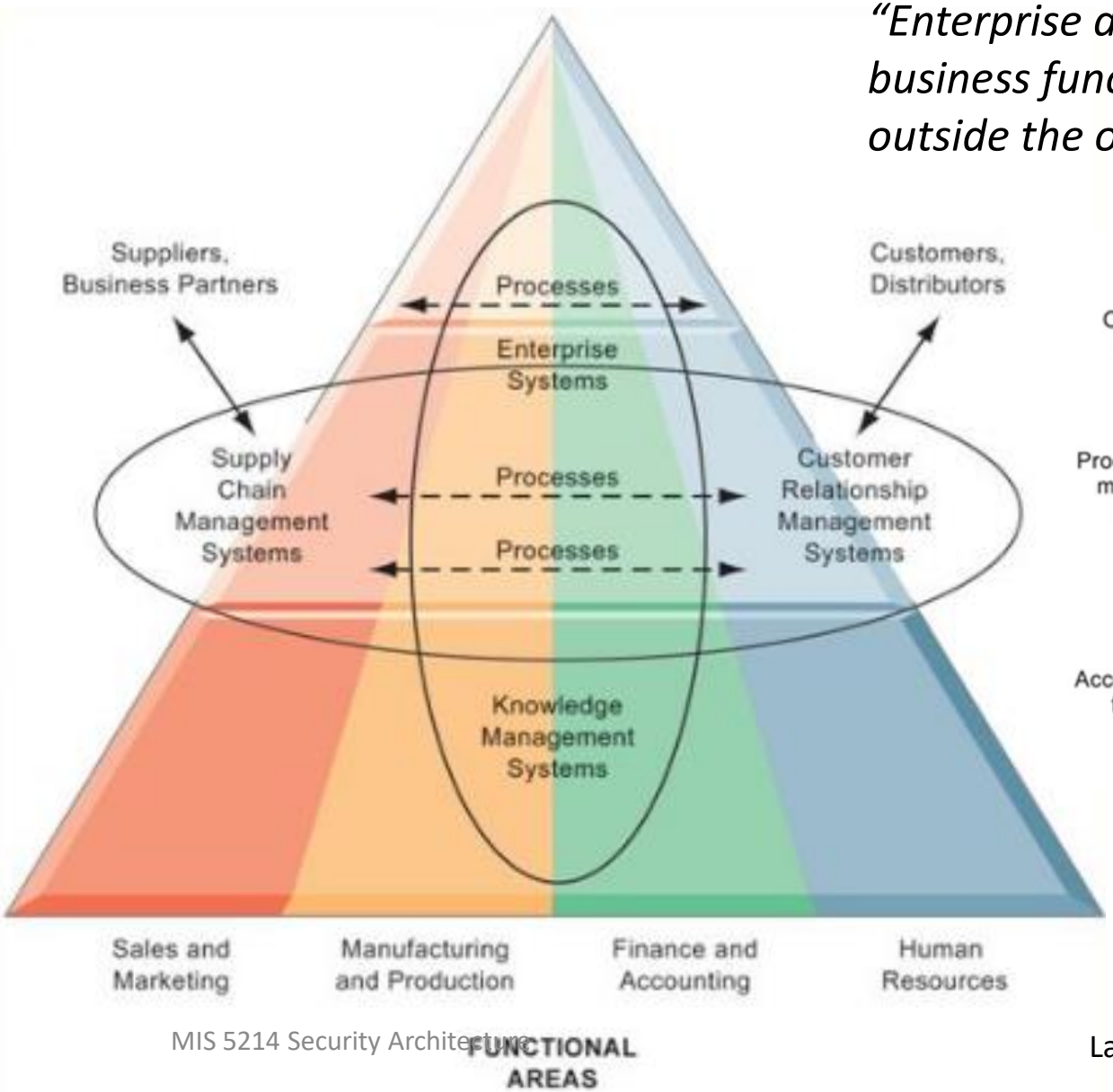


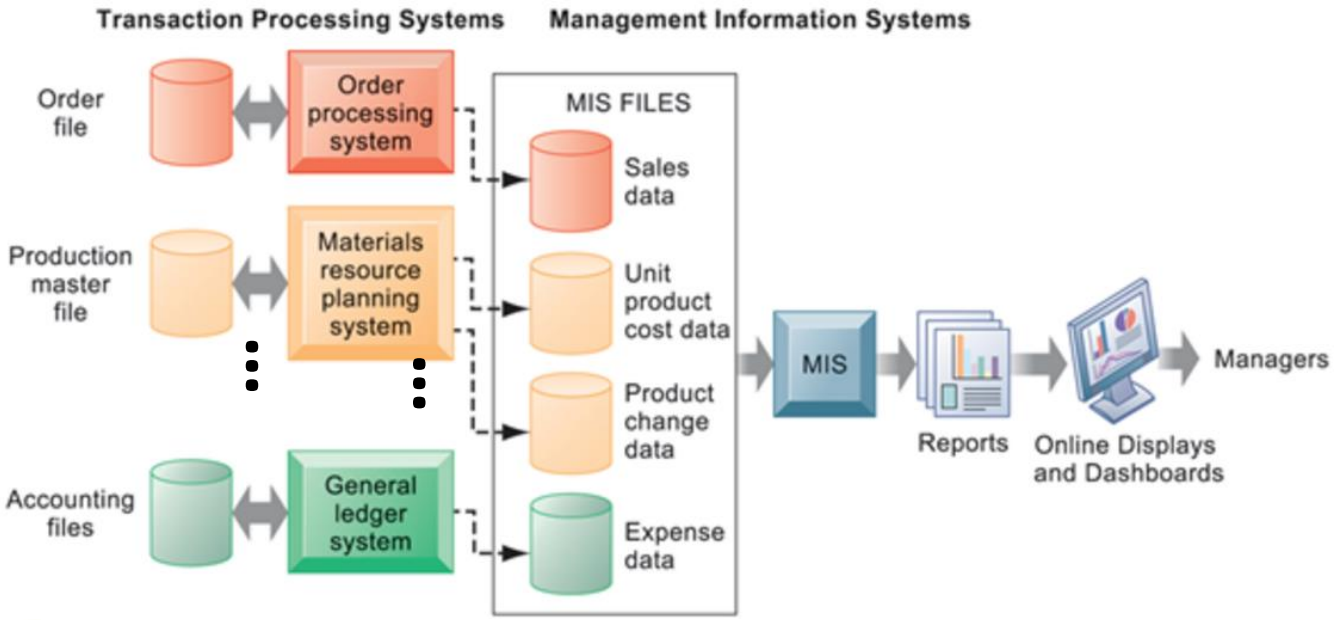
Content & Structure

Function & Use

Information Systems – Models of Information Flows

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





Laudon, K.C. and Traver, C.G. (2011), Management Information Systems, Prentice Hall

An example of an important security architecture model:

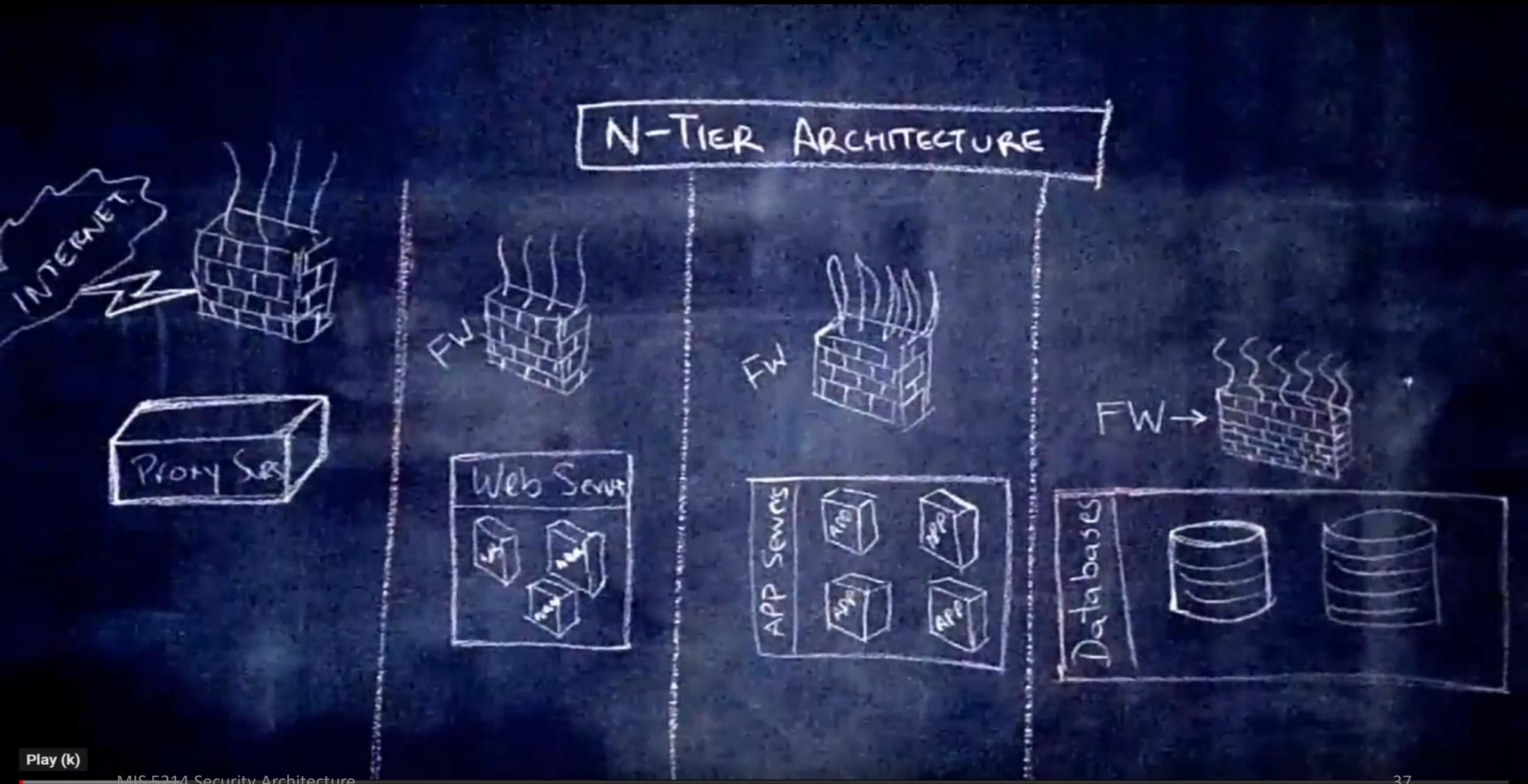
“Defense in Depth”

Also known as:

- *Layered Security*

We will focus our study on elements of layered security moving forward…

N-Tier Architecture for kids



Play (k)

0:01 / 12:20

Scroll for details

In-Class Exercise: Draw a conceptual mode of an N-Tier Architecture for a Web-Based System

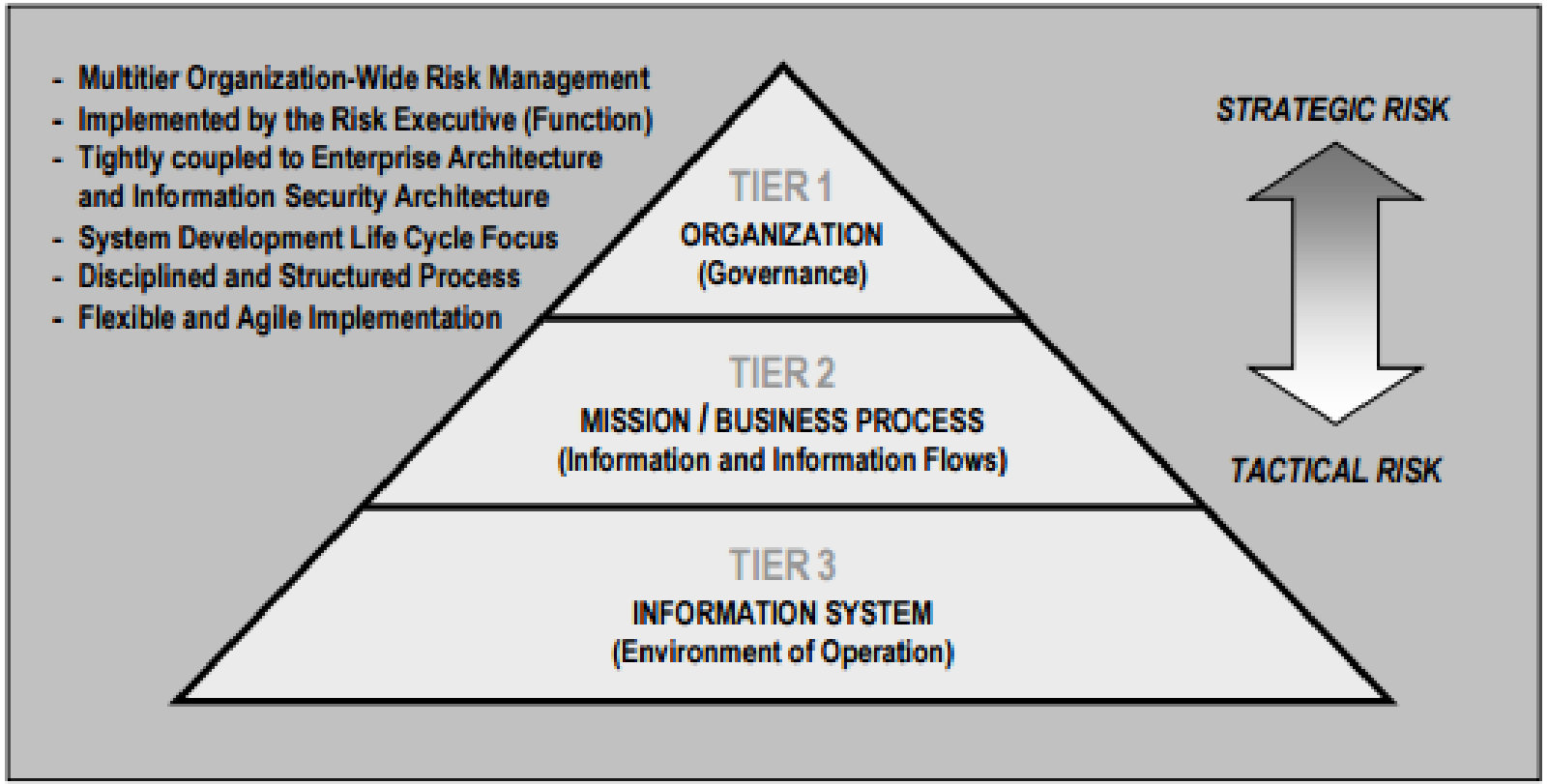
- Consider the purpose and contents of a web-based system for managing the accounts of customers of a public utility for a small town
- Using what you learned in the video, draw an N-Tier Architecture for the web-based system

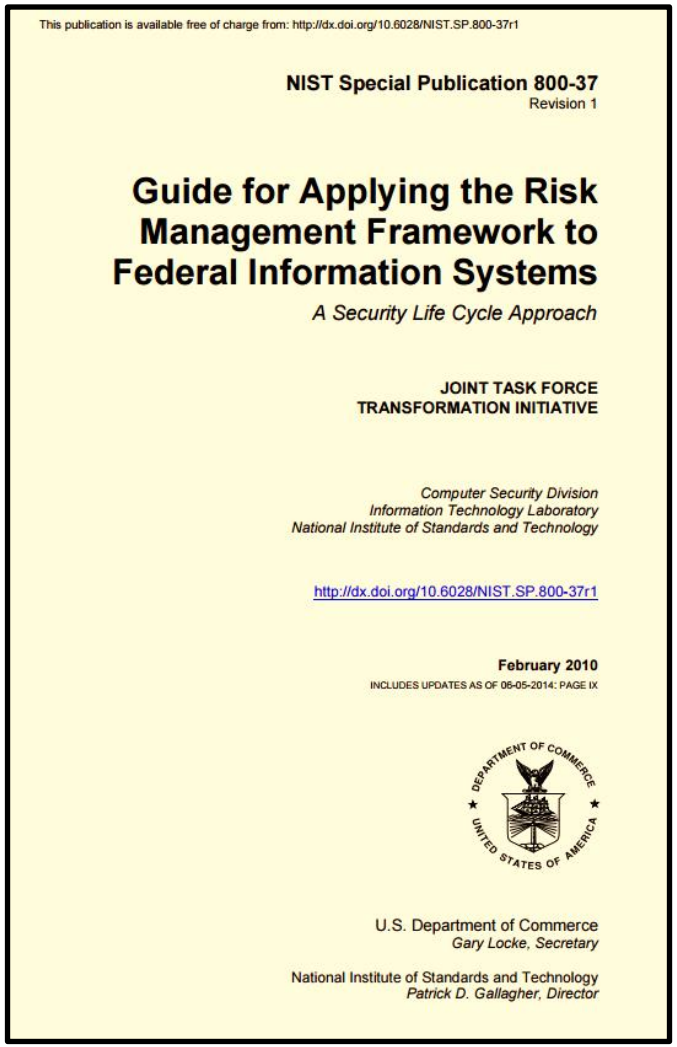
  https://app.diagrams.net/
- Identify in your diagram:
  1. Where the users are
  2. How their data flows through the system as they access and view their billing records

Agenda

- ✓Threat Modeling Exercise
- ✓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

NIST Risk Management Framework





This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-37r1

NIST Special Publication 800-37
Revision 1

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE TRANSFORMATION INITIATIVE

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

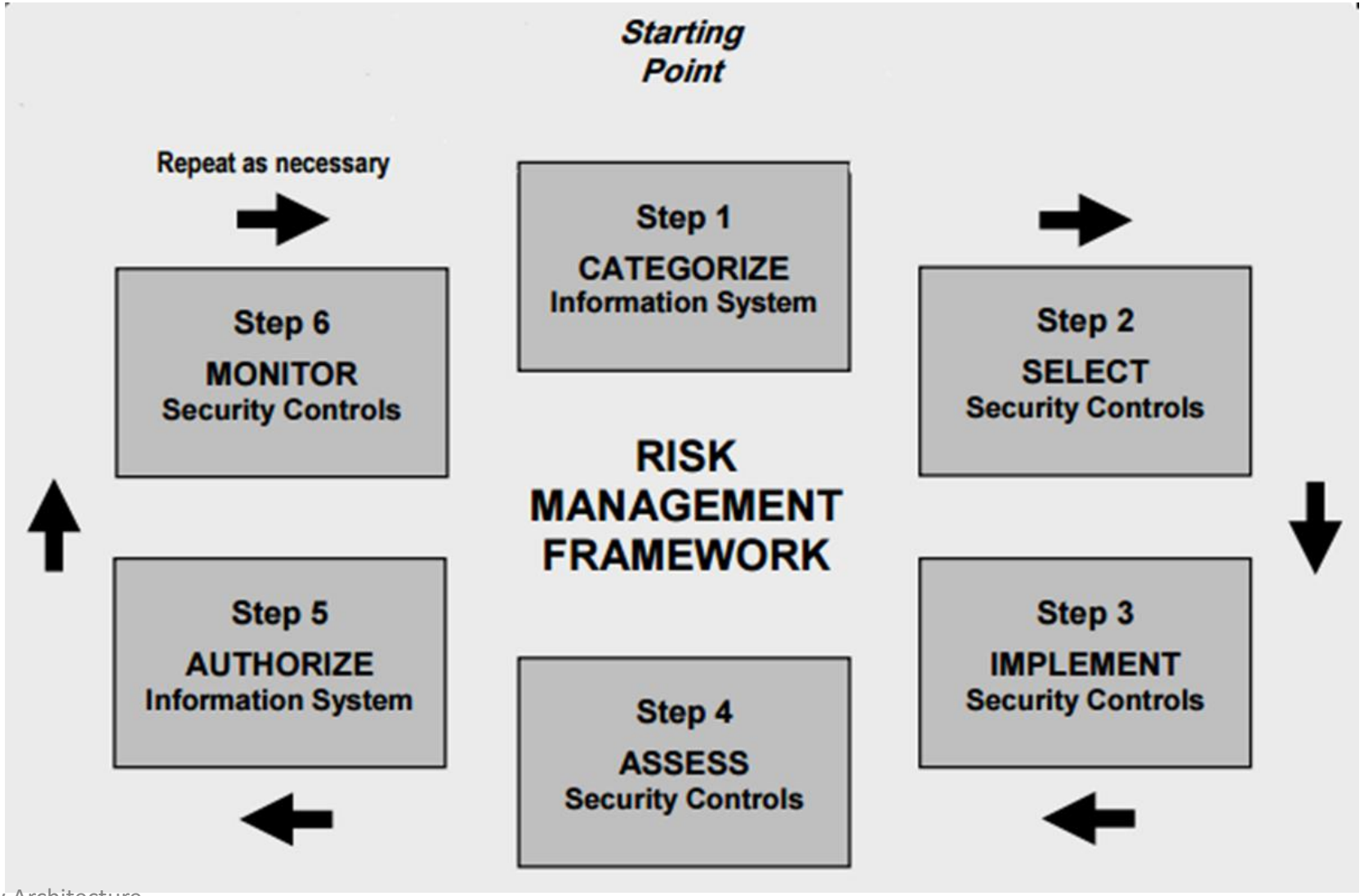
http://dx.doi.org/10.6028/NIST.SP.800-37r1

February 2010
INCLUDES UPDATES AS OF 06-05-2014: PAGE IX

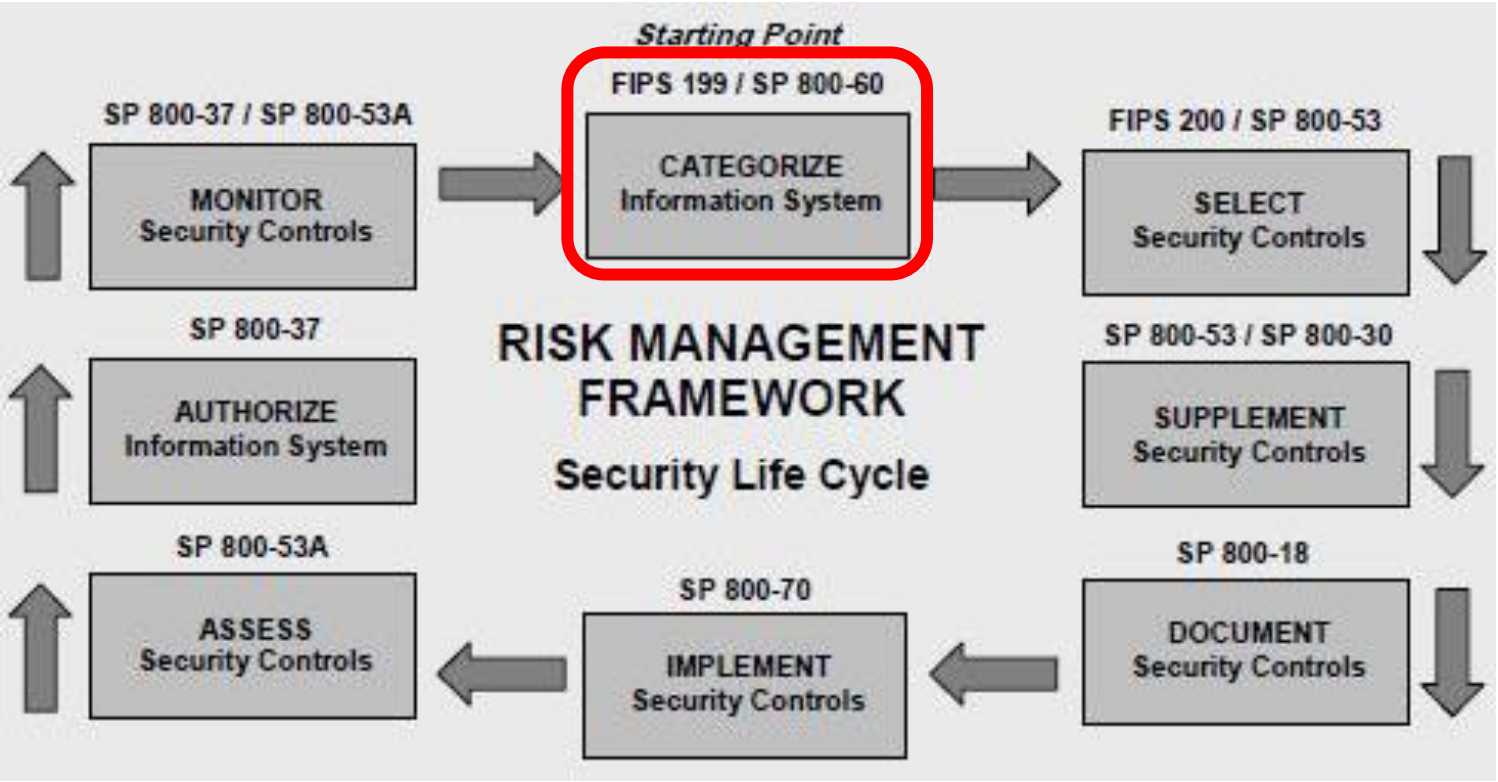
U.S. Department of Commerce
Gary Locke, Secretary

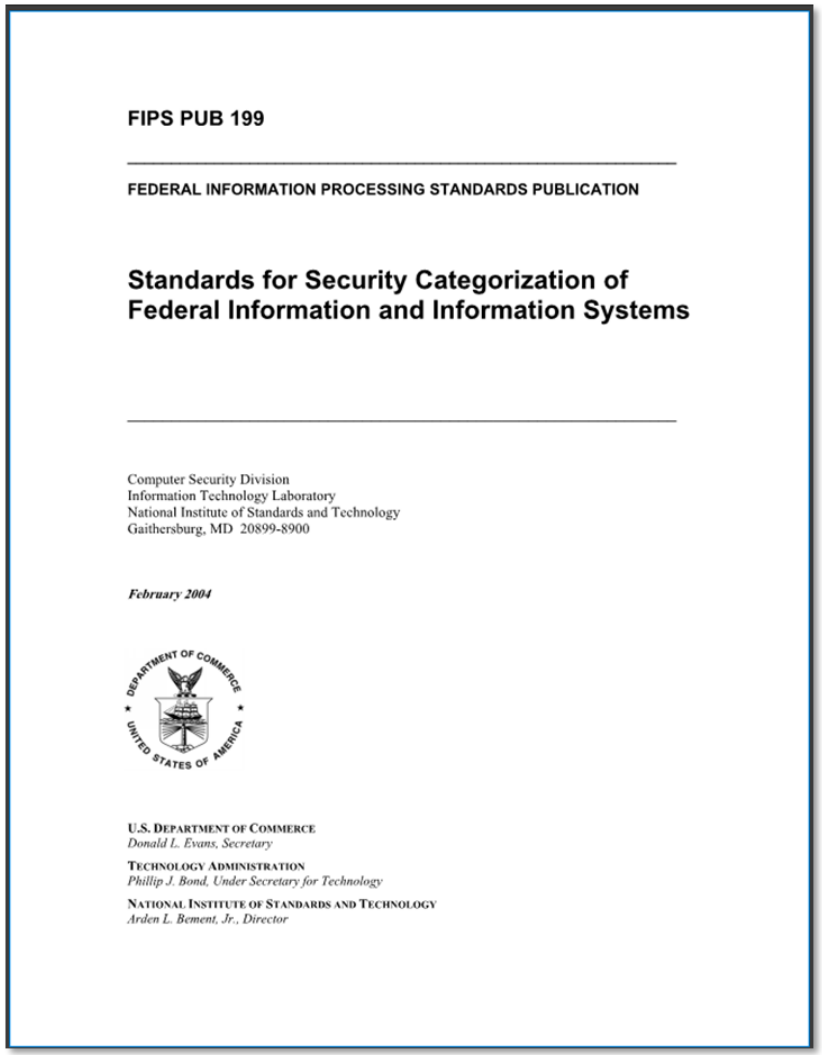
National Institute of Standards and Technology
Patrick D. Gallagher, Director

NIST Risk Management Framework



NIST Risk Management Framework





FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

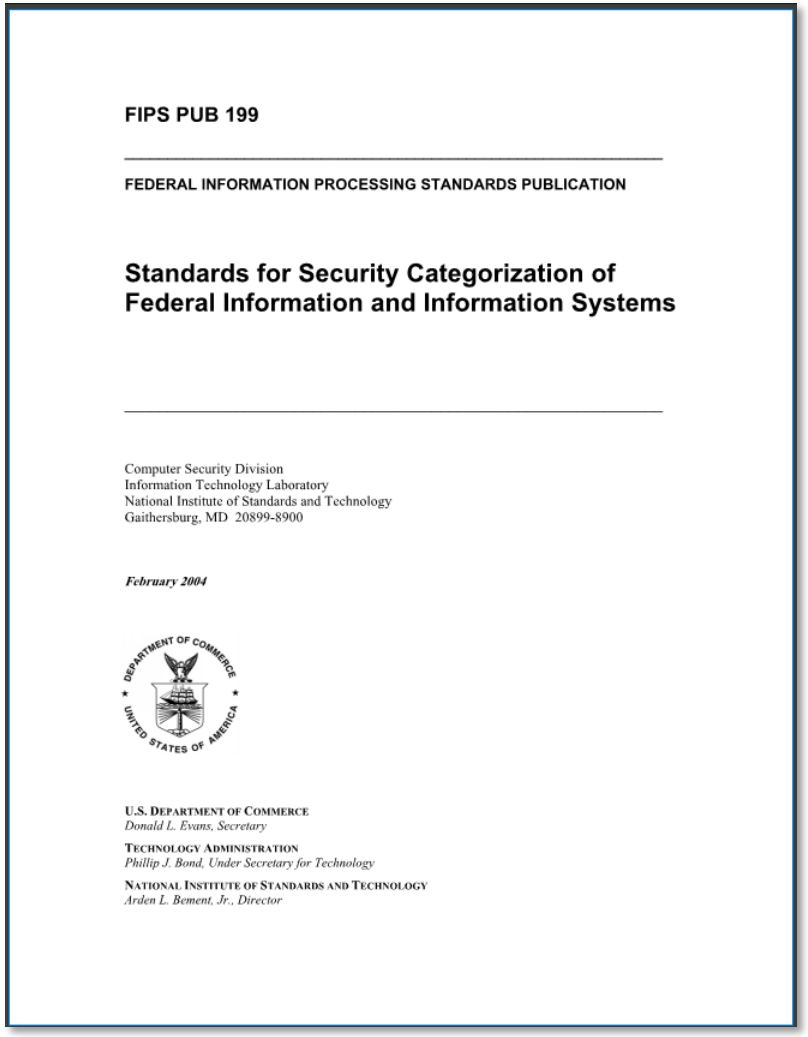
February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

FIPS 199: Qualitative risk assessment based on security objectives



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

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

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 = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

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

Example with multiple information types:

SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}. = LOW rating

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

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

What are the security categorizations of these 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 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 are the security categorizations of the geodatabases?

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	***High***	***Moderate***	***Moderate***	***High***
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	**Moderate**	**Moderate**	**Low**	**Moderate**
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
Comm_Electric Geodatabase	*High*	*Moderate*	*Moderate*	*High*
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	Moderate	Moderate	Low	Moderate
Parcel Boundary Shapefile	Low	Low	Low	Low

High

How would you transform these ordinal impact ratings into quantitative risk measures?

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
Comm_Electric Geodatabase	*High*	*Moderate*	*Moderate*	*High*
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
Water_Sewer Geodatabase	Moderate	Moderate	Low	Moderate
Parcel Boundary Shapefile	Low	Low	Low	Low
				High

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

Overall Risk of CIA Breach

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:

NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

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

INFORMATION SECURITY

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

October 2006

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

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Table 10-1. Risk Level Matrix

	Impact		
Threat Likelihood	**Low (10)**	**Moderate (50)**	**High (100)**
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10) 01527a

Because the determination of risk ratings for impact and threat likelihood is largely subjective, it is best to assign each rating a numeric value for ease of calculation. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For example:

- The probability assigned for each threat likelihood level is 1.0 for high, 0.5 for moderate, and 0.1 for low.
- The value assigned for each impact level is 100 for high, 50 for moderate, and 10 for low.

Table 10-2, below, describes the risk levels shown in the above matrix. This risk scale, with its ratings of high, moderate, and low, represents the degree of risk to which an information system, facility, or procedure might be exposed if a given vulnerability were exploited. It also describes the type of action senior managers must take for each risk level.

Table 10-2. Risk Scale and Necessary Management Action

Risk Level	Risk Description and Necessary Management Action
High	If an observation or finding is evaluated as high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate	If an observation is rated as moderate risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's authorizing official must determine whether corrective actions are still required or decide to accept the risk.

10.1.5 Step 5 – Control Recommendations

The goal of the control recommendations is to reduce the level of risk to the information system and its data to a level the organization deems acceptable. These recommendations are essential input for the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. This step is designed to help agencies identify and select controls appropriate to the organization's operations and mission that could mitigate or eliminate the risks identified in the preceding steps. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility);
- Legislation and regulation;

Transformation of ordinal qualitative risk categories to interval quantitative risk measures

	Impact		
Threat Likelihood	**Low (10)**	**Moderate (50)**	**High (100)**
High (1.0)	10 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

01527a

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

Requires the risk analyst to contribute additional knowledge to transform ordinal scale into an interval scale…

NIST SP 800-100 “Information Security Handbook: A Guide for Managers”, page 90

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 x 1.0 = 10	50 x 1.0 = 50	100 x 1.0 = 100
Moderate (0.5)	10 x 0.5 = 5	50 x 0.5 = 25	100 x 0.5 = 50
Low (0.1)	10 x 0.1 = 1	50 x 0.1 = 5	100 x 0.1 = 10

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

01527a

= ?

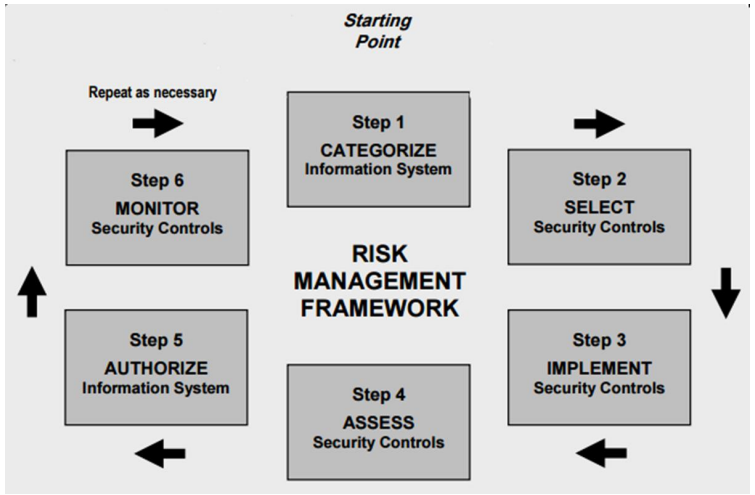
Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Traffic control	10	0.1	1
Comm_Electric Geodatabase	***High***		
			0
Water Distribution System	50	0.1	5
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1
Water_Sewer Geodatabase	**Moderate**	0.1	
			0
Parcel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

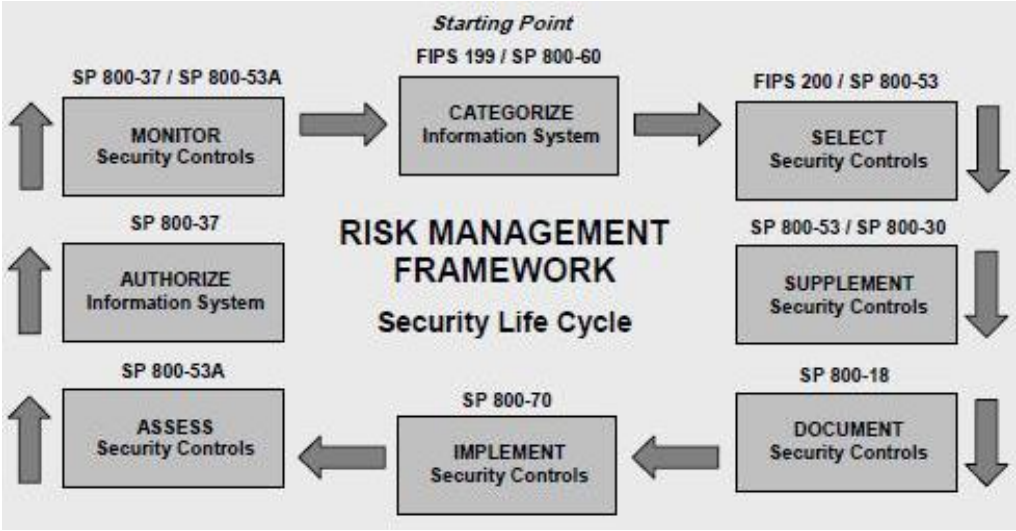
Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Water Distribution System	50	0.1	5
Parcel Boundary Shapefile	10	0.5	5
Traffic control	10	0.1	1
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1

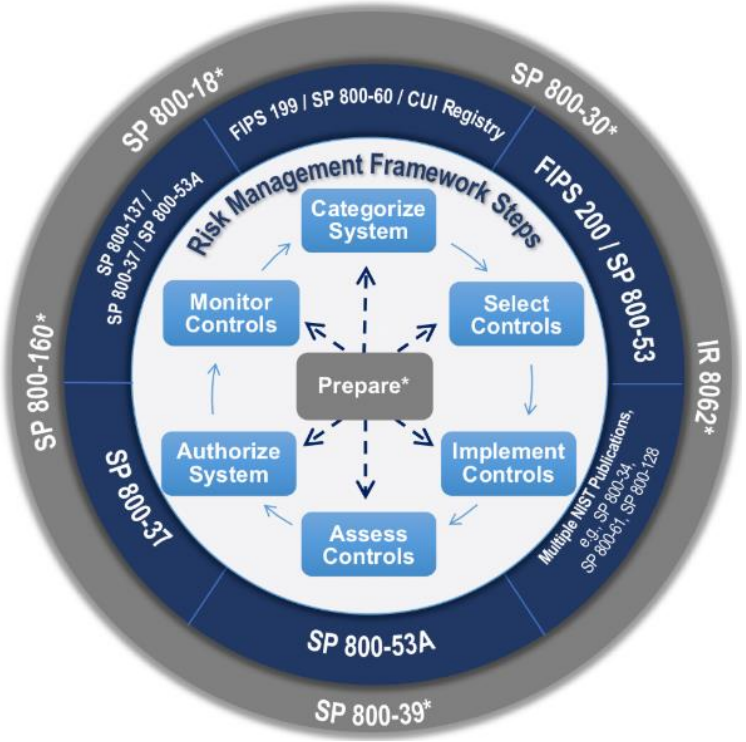
Agenda

- ✓Threat Modeling Exercise
- ✓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

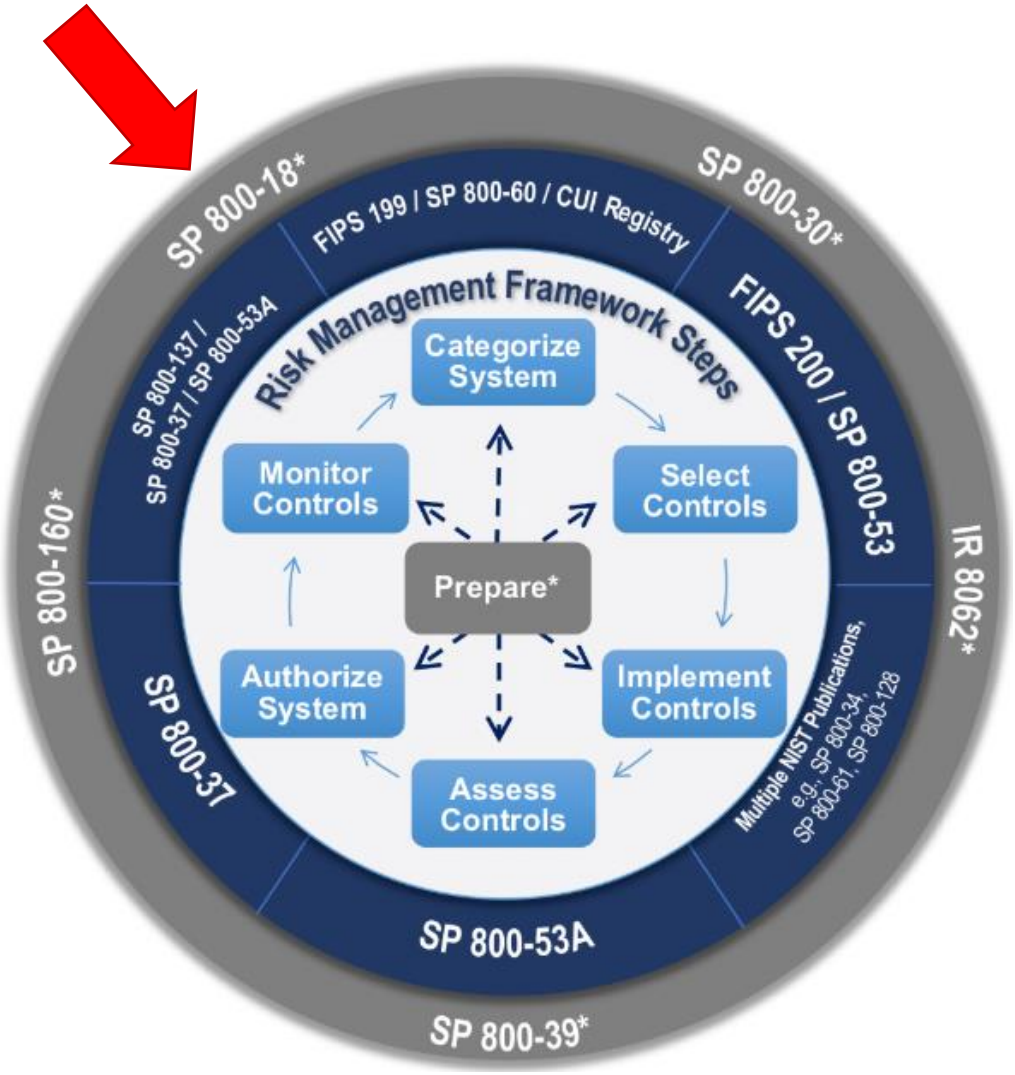
Conceptual Views of NIST Risk Management Framework

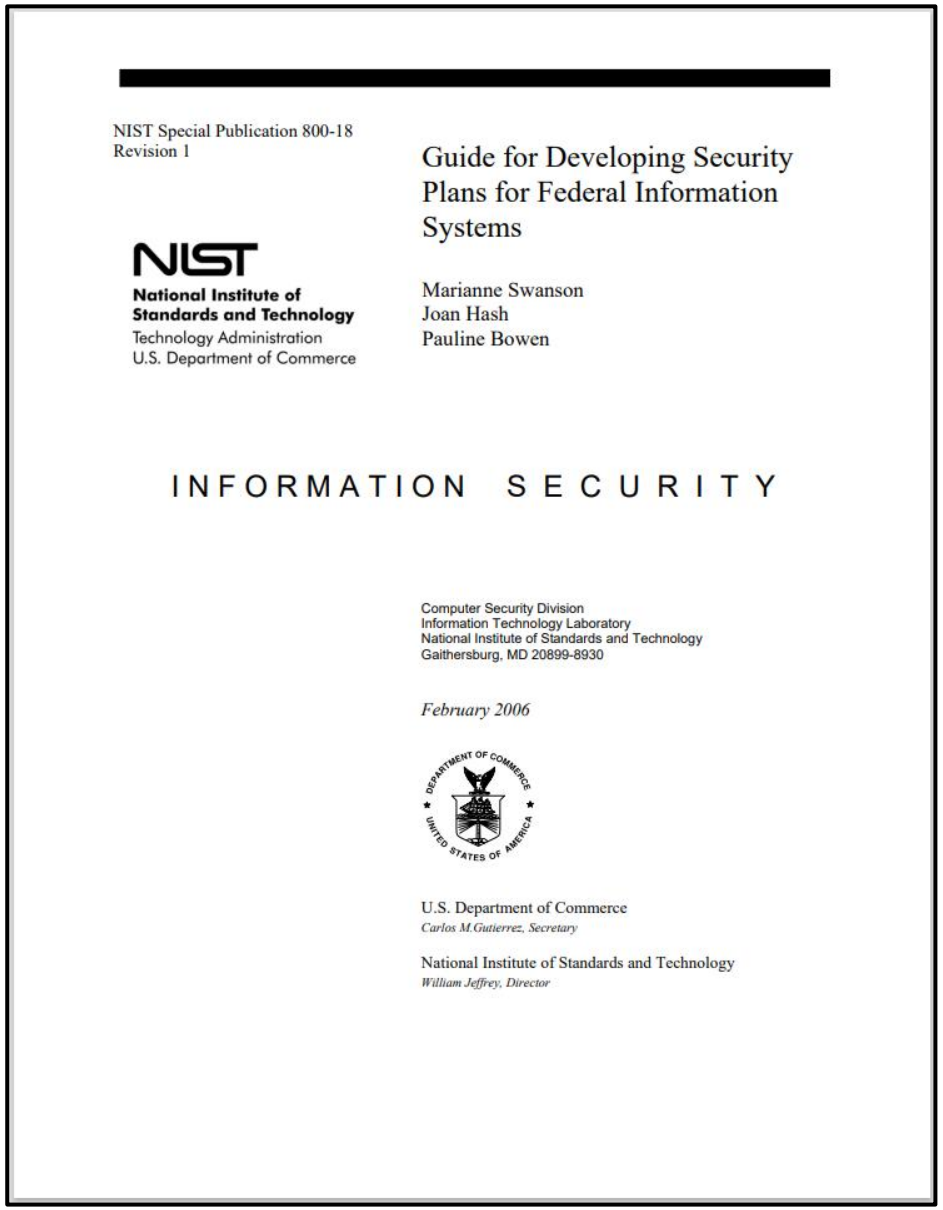






Documenting Information System Security Categorization in a System Security Plan





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

INFORMATION SECURITY

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

February 2006

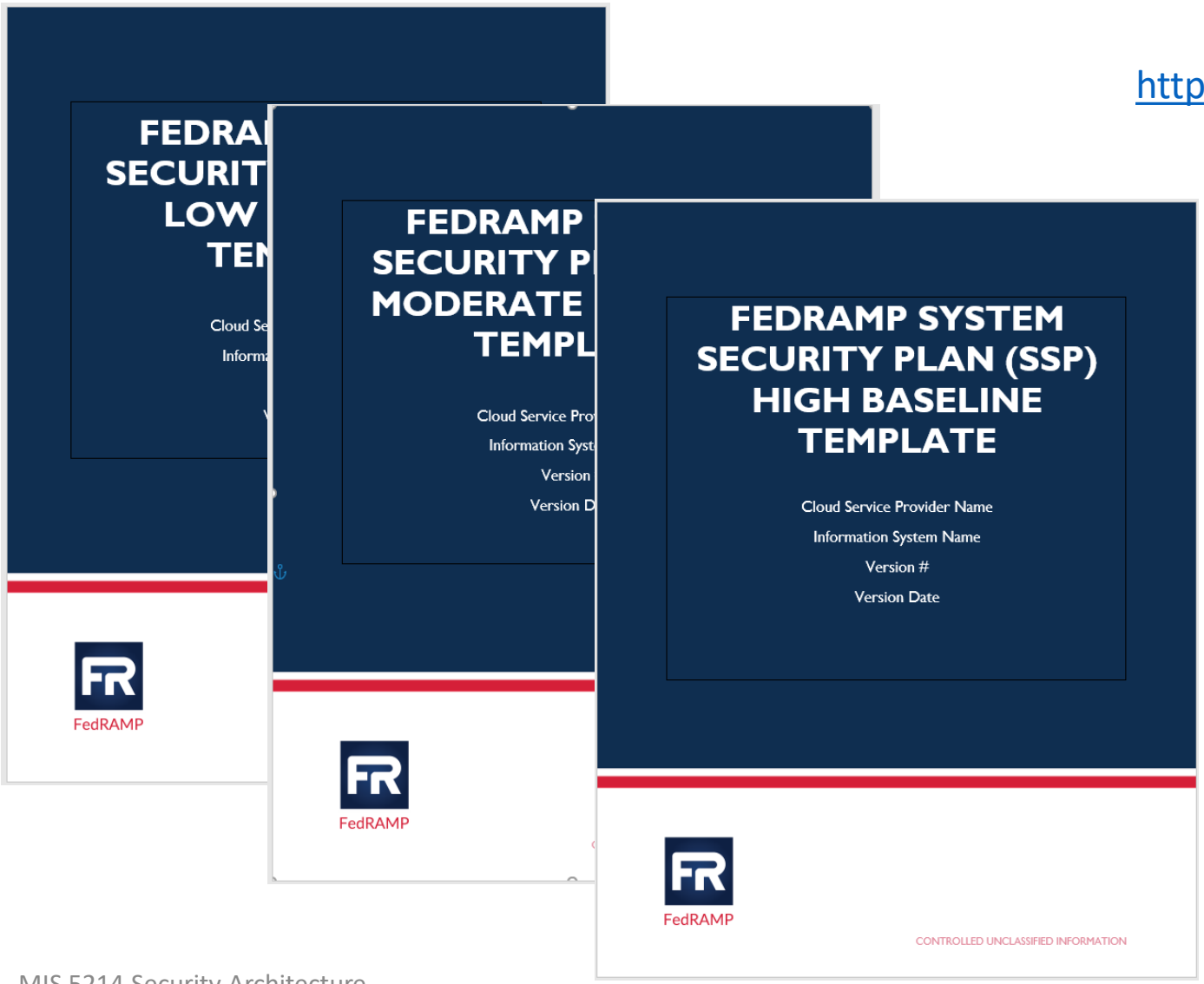
U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

System Security Plan (SSP)

FedRAMP = Federal Risk and Authorization Management Program

https://www.fedramp.gov/documents-templates/



Information System Security Plan (SSP)

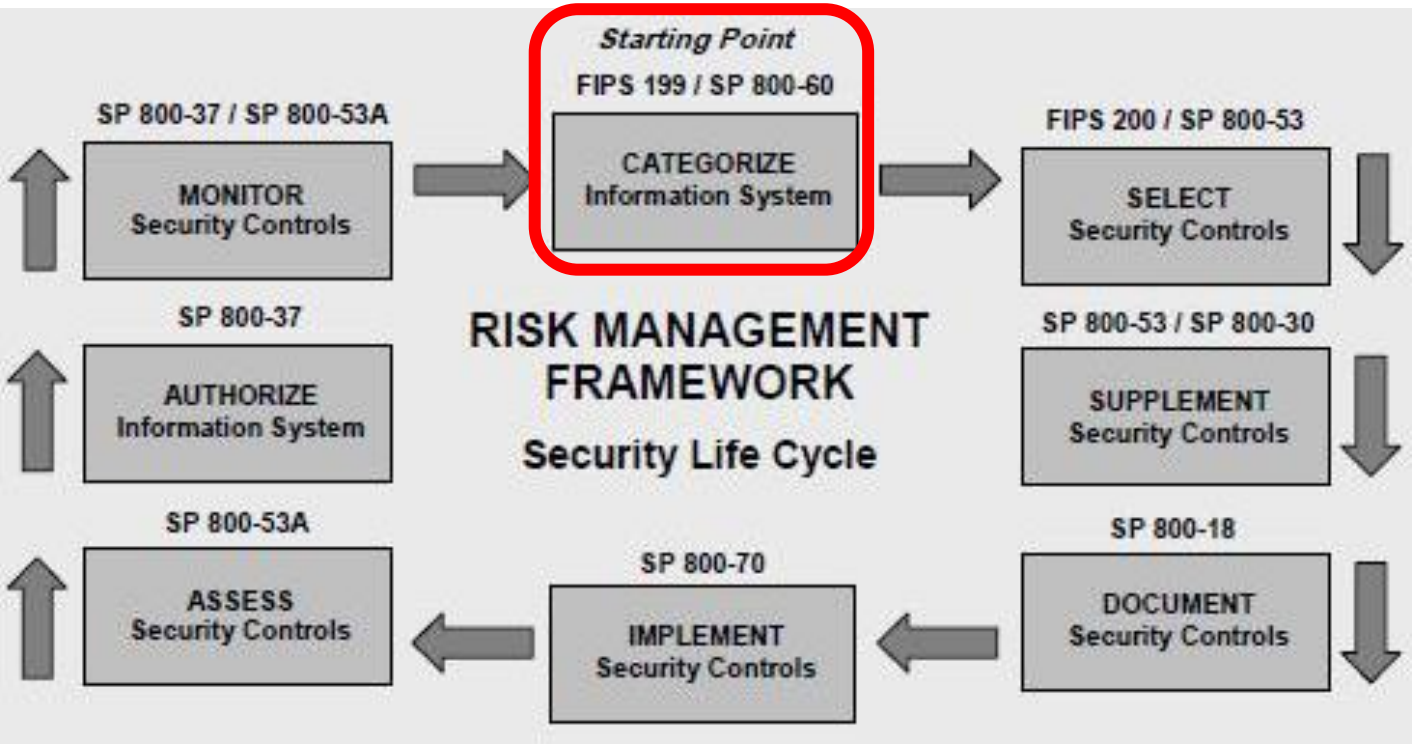


TABLE OF CONTENTS

Where to document information system categorization within a System Security Plan

Information System Security Plan (SSP)

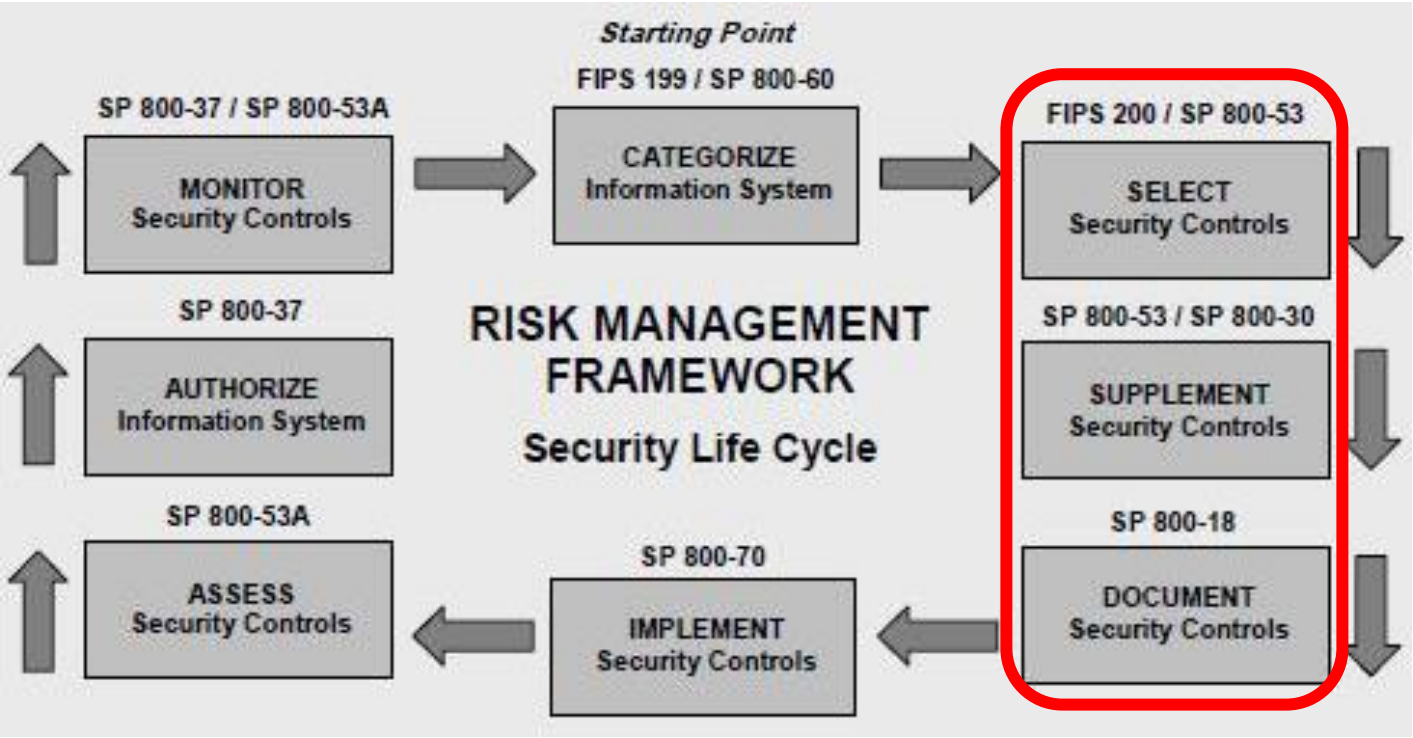


TABLE OF CONTENTS

FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

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

March 2006

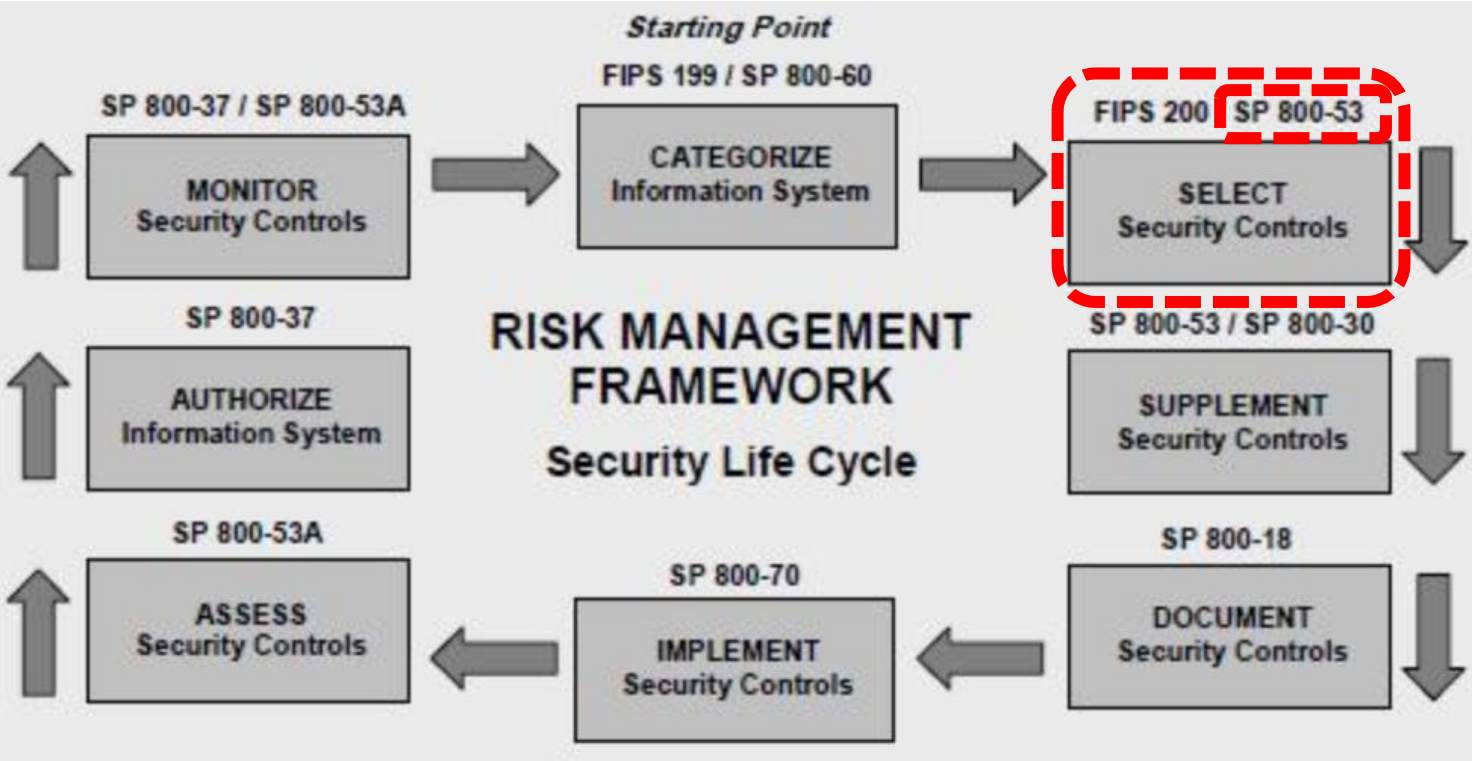
U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

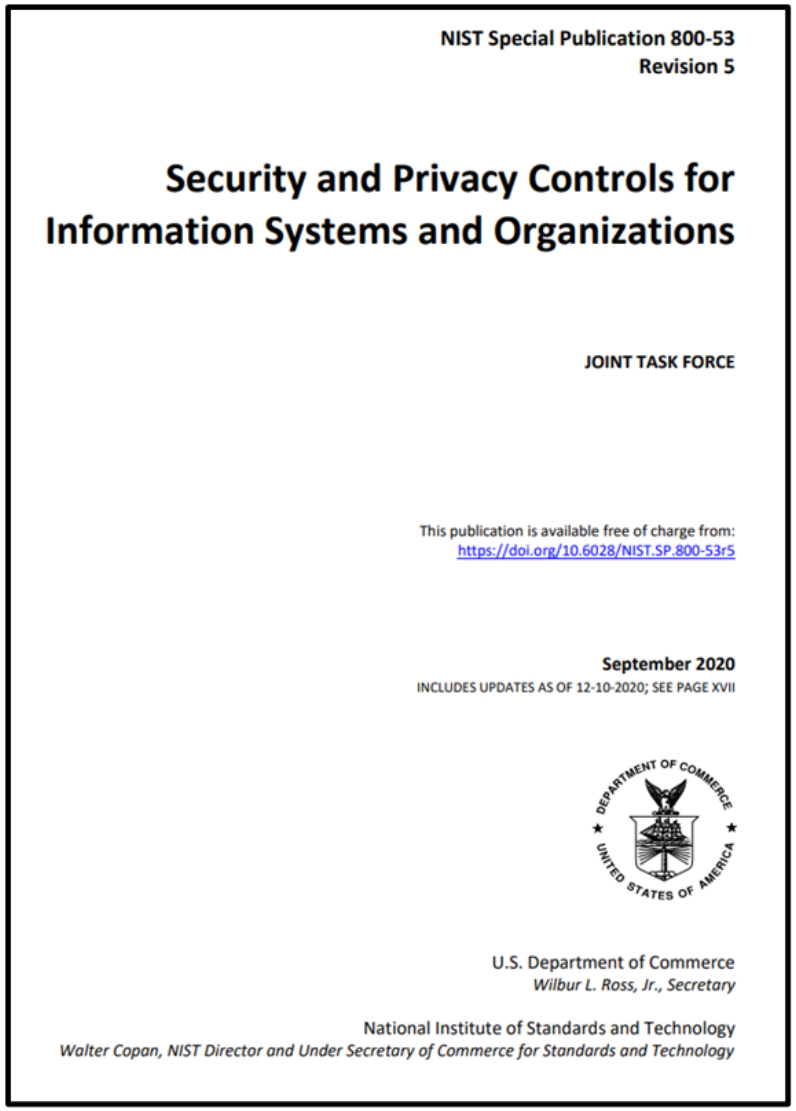
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

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 RMF





NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

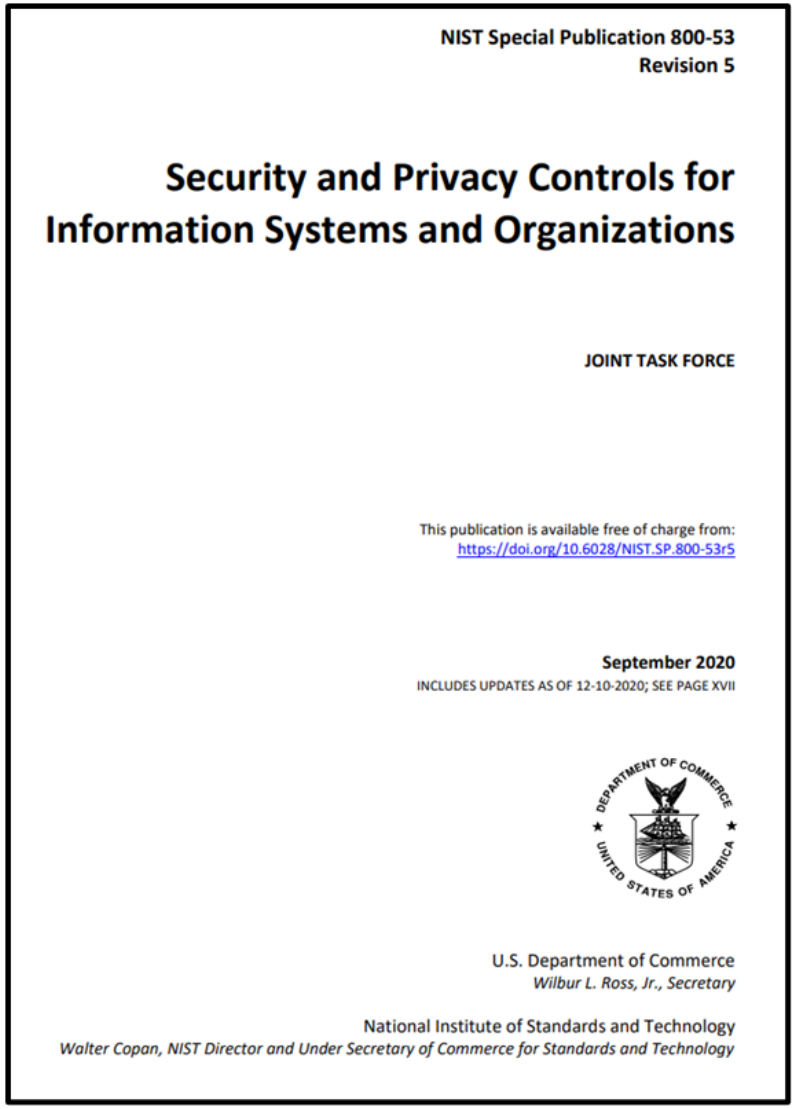
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Minimum Security Controls have evolved



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Since FIPS 200 was written in 2006, 3 more control families have been added

How we use FIPS 199 security categorization to select security controls…

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020

INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

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
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
Planning					

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)

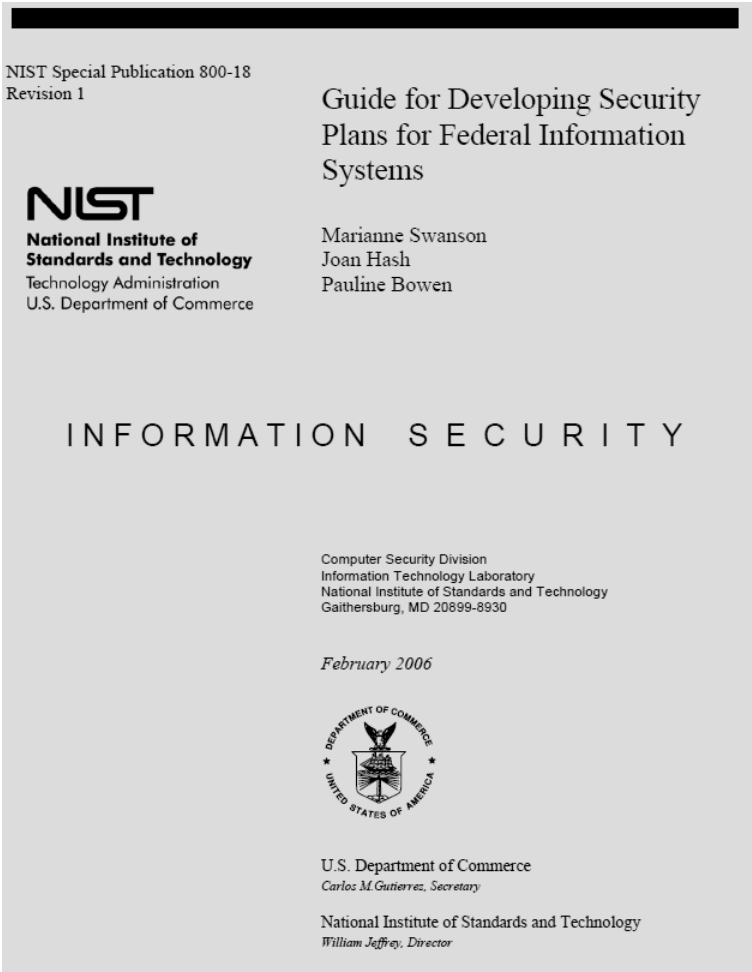
CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
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) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
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)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)

NIST 800-53 risk controls are typically presented alphabetically

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

NIST 800-53 Controls can be 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

INFORMATION SECURITY

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

3.16 RISK ASSESSMENT FAMILY

Table 3-16 provides a summary of the controls and control enhancements assigned to the Risk Assessment Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-1	**Policy and Procedures**	x	x	x	x
RA-2	**Security Categorization**		x	x	x
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	**Risk Assessment**	x	x	x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		x	x	x
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	Risk Assessment Update	W: Incorporated into RA-3.			
RA-5	**Vulnerability Monitoring and Scanning**		x	x	x
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		x	x	x
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				x
RA-5(5)	PRIVILEGED ACCESS			x	x
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		x	x	x
RA-6	**Technical Surveillance Countermeasures Survey**				
RA-7	**Risk Response**	x	x	x	x
RA-8	**Privacy Impact Assessments**	x			
RA-9	**Criticality Analysis**			x	x
RA-10	**Threat Hunting**				

How do you determine which RA controls are relevant to the web-based system you began designing for managing the utility's customers' billing records for the small town ?

TABLE 3-16: RISK ASSESSMENT FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
RA-1	**Policy and Procedures**	x	x	x	x
RA-2	**Security Categorization**		x	x	x
RA-2(1)	IMPACT-LEVEL PRIORITIZATION				
RA-3	**Risk Assessment**	x	x	x	x
RA-3(1)	SUPPLY CHAIN RISK ASSESSMENT		x	x	x
RA-3(2)	USE OF ALL-SOURCE INTELLIGENCE				
RA-3(3)	DYNAMIC THREAT AWARENESS				
RA-3(4)	PREDICTIVE CYBER ANALYTICS				
RA-4	Risk Assessment Update	W: Incorporated into RA-3.			
RA-5	**Vulnerability Monitoring and Scanning**		x	x	x
RA-5(1)	UPDATE TOOL CAPABILITY	W: Incorporated into RA-5.			
RA-5(2)	UPDATE VULNERABILITIES TO BE SCANNED		x	x	x
RA-5(3)	BREADTH AND DEPTH OF COVERAGE				
RA-5(4)	DISCOVERABLE INFORMATION				x
RA-5(5)	PRIVILEGED ACCESS			x	x
RA-5(6)	AUTOMATED TREND ANALYSES				
RA-5(7)	AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	W: Incorporated into CM-8.			
RA-5(8)	REVIEW HISTORIC AUDIT LOGS				
RA-5(9)	PENETRATION TESTING AND ANALYSES	W: Incorporated into CA-8.			
RA-5(10)	CORRELATE SCANNING INFORMATION				
RA-5(11)	PUBLIC DISCLOSURE PROGRAM		x	x	x
RA-6	**Technical Surveillance Countermeasures Survey**				
RA-7	**Risk Response**	x	x	x	x
RA-8	**Privacy Impact Assessments**	x			
RA-9	**Criticality Analysis**			x	x
RA-10	**Threat Hunting**				

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*].

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

of the risk assessment policy and associated

ization-defined frequency]; and

organization-defined frequency].

tablishment of policy and procedures for the
ls and control enhancements in the RA family.
s, Executive Orders, directives, regulations,
policies and procedures at the organization
s and procedures unnecessary. The policy can
ty policy for organizations or conversely, can
mplex nature of certain organizations. The
am in general and for particular information
ment 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

SSP – Control Inventory Example

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:

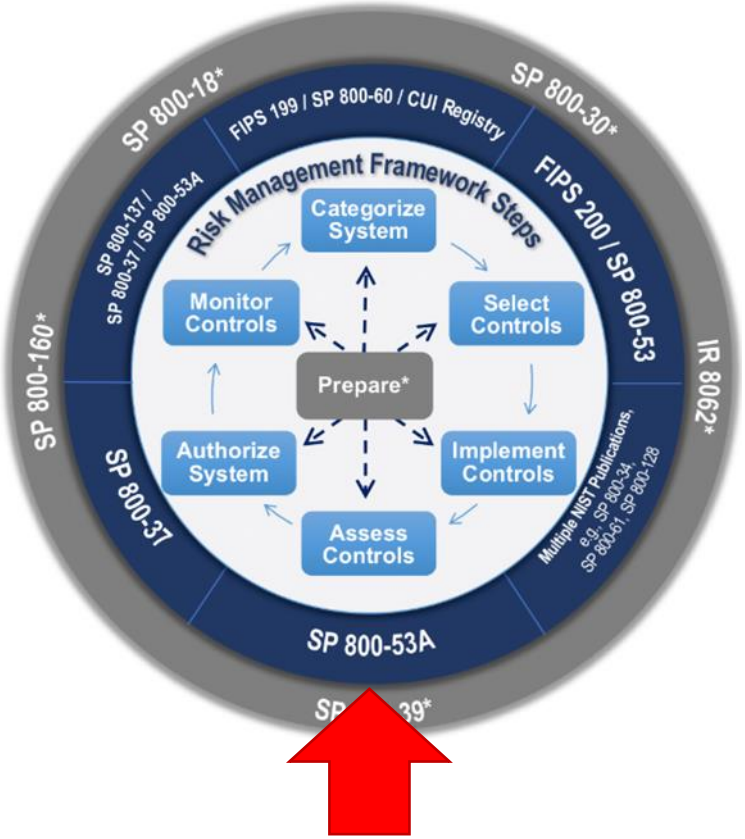
   1. Risk assessment policy [*Assignment: organization-defined frequency*]; and

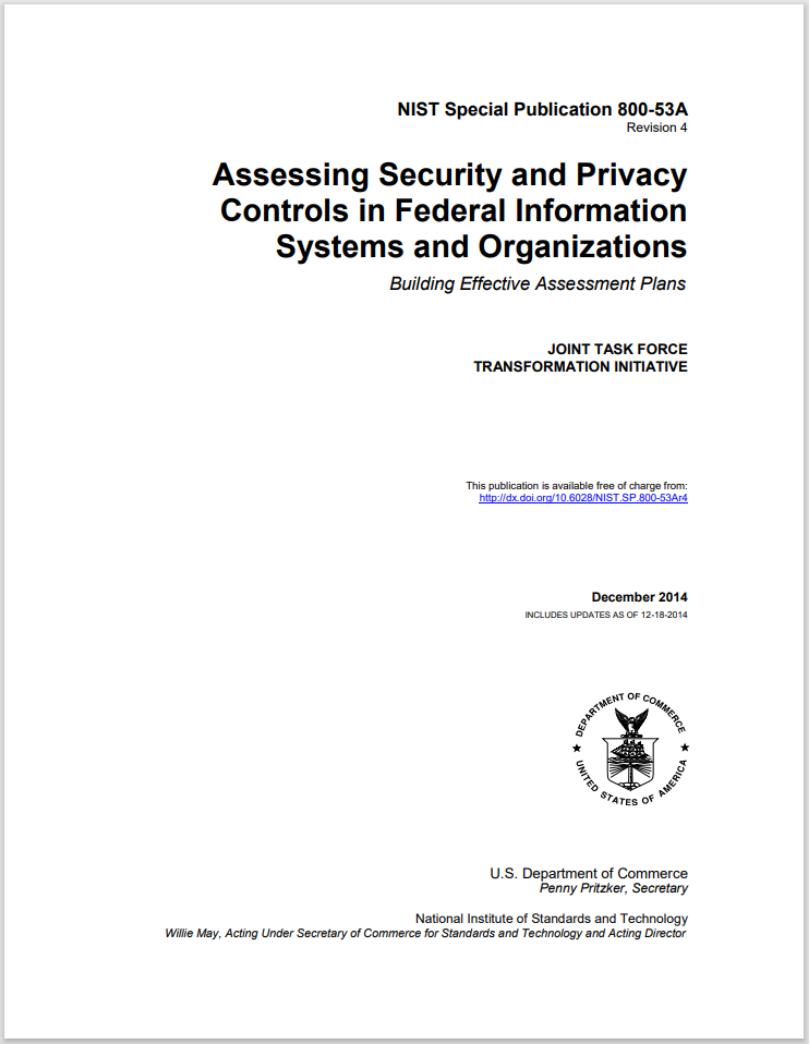
   2. Risk assessment procedures [*Assignment: organization-defined frequency*].

RA-1	Control Summary Information
Responsible Role:	
Parameter RA-1(a):	
Parameter RA-1(b)(1):	
Parameter RA-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

RA-1 What is the solution and how is it implemented?	
Part a	
Part b	

How to assess an InfoSec Control ?





NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

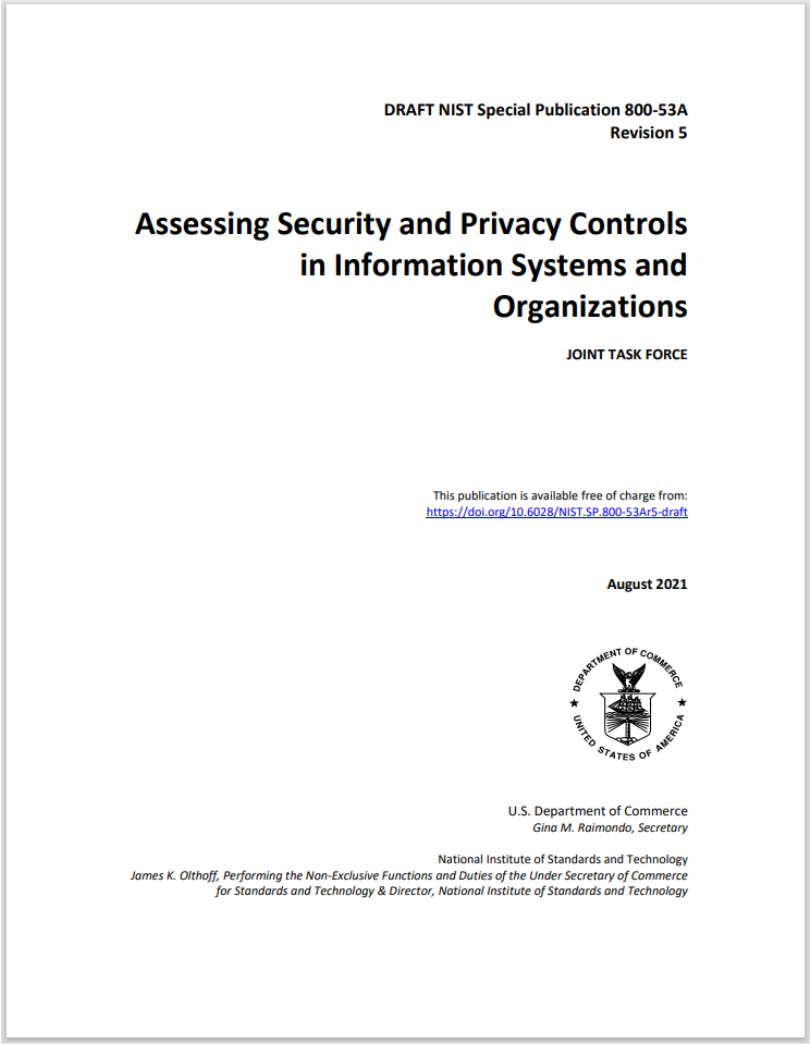
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

December 2014
INCLUDES UPDATES AS OF 12-18-2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director



DRAFT NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5-draft

August 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Assessing InfoSec control

FAMILY: RISK ASSESSMENT

RA-1	RISK ASSESSMENT POLICY AND PROCEDURES		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	RA-1(a)(1)	RA-1(a)(1)[1]	*develops and documents a risk assessment policy that addresses:*
			RA-1(a)(1)[1][a] *purpose;*
			RA-1(a)(1)[1][b] *scope;*
			RA-1(a)(1)[1][c] *roles;*
			RA-1(a)(1)[1][d] *responsibilities;*
			RA-1(a)(1)[1][e] *management commitment;*
			RA-1(a)(1)[1][f] *coordination among organizational entities;*
			RA-1(a)(1)[1][g] *compliance;*
		RA-1(a)(1)[2]	*defines personnel or roles to whom the risk assessment policy is to be disseminated;*
		RA-1(a)(1)[3]	*disseminates the risk assessment policy to organization-defined personnel or roles;*
	RA-1(a)(2)	RA-1(a)(2)[1]	*develops and documents procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls;*
		RA-1(a)(2)[2]	*defines personnel or roles to whom the procedures are to be disseminated;*
		RA-1(a)(2)[3]	*disseminates the procedures to organization-defined personnel or roles;*
	RA-1(b)(1)	RA-1(b)(1)[1]	*defines the frequency to review and update the current risk assessment policy;*
		RA-1(b)(1)[2]	*reviews and updates the current risk assessment policy with the organization-defined frequency;*
	RA-1(b)(2)	RA-1(b)(2)[1]	*defines the frequency to review and update the current risk assessment procedures; and*
		RA-1(b)(2)[2]	*reviews and updates the current risk assessment procedures with the organization-defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* risk assessment policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with risk assessment responsibilities; organizational personnel with information security responsibilities].		

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.

ntative reviews

for effective
e impacts to
information and
availability.
activity with
information
nizations also
ith 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

SSP – Control Inventory Example (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

c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-2	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	

Assessing InfoSec control

RA-2	SECURITY CATEGORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if the organization:*	
	RA-2(a)	*categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;*
	RA-2(b)	*documents the security categorization results (including supporting rationale) in the security plan for the information system; and*
	RA-2(c)	*ensures the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and information systems; security plan; security categorization documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for security categorization].	

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

SSP – Control Inventory Example

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.

RA-3	Control Summary Information
Responsible Role:	
Parameter RA-3(b):	
Parameter RA-3(c):	
Parameter RA-3(d):	
Parameter RA-3(e):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply):	
☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

RA-3 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	

Assessing InfoSec control

RA-3	RISK ASSESSMENT		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	RA-3(a)	*conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of:*	
		RA-3(a)[1]	*the information system;*
		RA-3(a)[2]	*the information the system processes, stores, or transmits;*
	RA-3(b)	RA-3(b)[1]	*defines a document in which risk assessment results are to be documented (if not documented in the security plan or risk assessment report);*
		RA-3(b)[2]	*documents risk assessment results in one of the following:*
		RA-3(b)[2][a]	*the security plan;*
		RA-3(b)[2][b]	*the risk assessment report; or*
		RA-3(b)[2][c]	*the organization-defined document;*
	RA-3(c)	RA-3(c)[1]	*defines the frequency to review risk assessment results;*
		RA-3(c)[2]	*reviews risk assessment results with the organization-defined frequency;*
	RA-3(d)	RA-3(d)[1]	*defines personnel or roles to whom risk assessment results are to be disseminated;*
		RA-3(d)[2]	*disseminates risk assessment results to organization-defined personnel or roles;*
	RA-3(e)	RA-3(e)[1]	*defines the frequency to update the risk assessment;*
		RA-3(e)[2]	*updates the risk assessment:*

TABLE OF CONTENTS

System Security Plan based on RMF including FIPS 199, FIPS 200 and SP800-53…

SSP Contains & Documents the status of the System's Control Inventory

	Control Summary Information
Responsible Role:	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	

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

Agenda

- ✓Threat Modeling Exercise
- ✓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