

# Unit #1a

MIS5214

## System Security Plan

# Agenda

- Threat Modeling and STRIDE
- 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.

## What is Threat Modeling?

Threat modeling is a structured process used in cybersecurity and software development to identify, analyze, and mitigate potential security threats in a system before they can be exploited.

### Key Goals of Threat Modeling:

- 1. Identify Threats** – Understand what could go wrong in a system.
- 2. Assess Risks** – Analyze how severe and likely each threat is.
- 3. Mitigate Vulnerabilities** – Implement security controls to prevent attacks.
- 4. Improve Security Posture** – Ensure secure system design from the start.

### Steps in Threat Modeling:

- 1. Define the System** – Understand components (e.g., servers, databases, users).
- 2. Identify Threats** – Use models like **STRIDE**, **DREAD**, or **PASTA** to categorize threats.
- 3. Analyze Risks** – Evaluate threat impact and likelihood.
- 4. Prioritize and Mitigate** – Apply **security solutions** (e.g., encryption, MFA, firewall).
- 5. Review and Update** – Continuously monitor and improve security



# STRIDE

**STRIDE** is a threat modeling framework developed by **Microsoft** to help identify and mitigate security threats in software systems. It categorizes threats into six types:

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

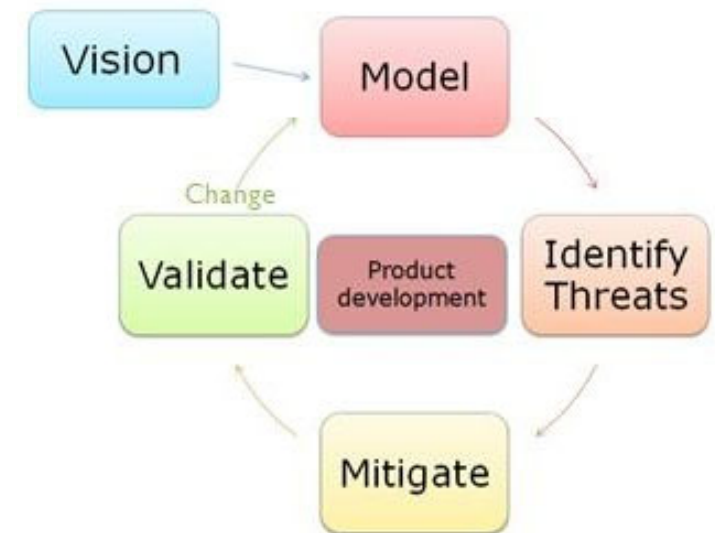
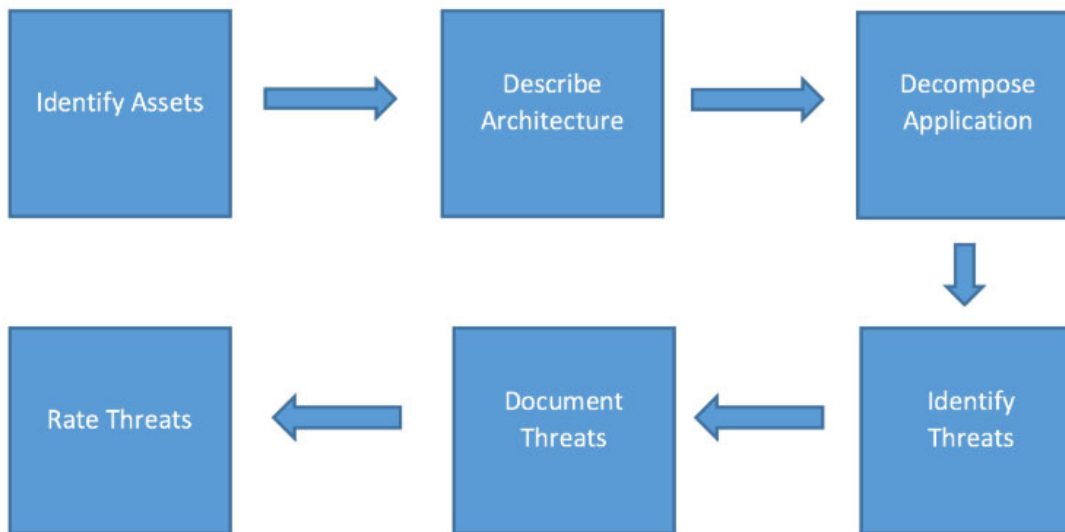
A security threat brainstorming activity

- 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

**Information Systems (IS)** refers to the structured arrangement of technology, people, processes, and data used to collect, process, store, and distribute information. It helps organizations make decisions, coordinate activities, analyze data, and create efficiencies in business operations.

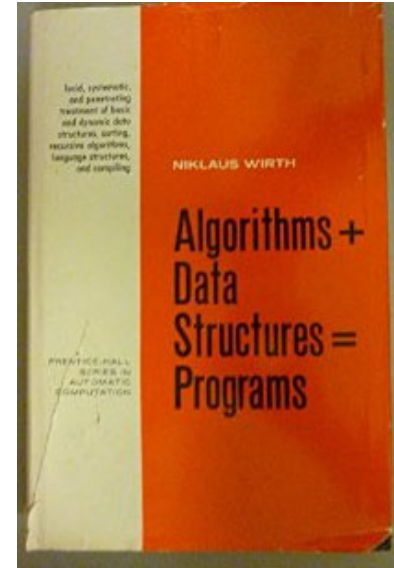
## **Key Components of an Information System**

An information system consists of five main components:

- 1.Hardware** – Physical devices such as computers, servers, storage devices, networking equipment, and peripherals.
- 2.Software** – Applications and operating systems that process data and perform specific tasks.
- 3.Data** – Raw facts and figures that are processed into meaningful information.
- 4.People** – Users who interact with the system, including IT professionals, analysts, and business users.
- 5.Processes** – Procedures and rules governing how data is collected, processed, and used.

# 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



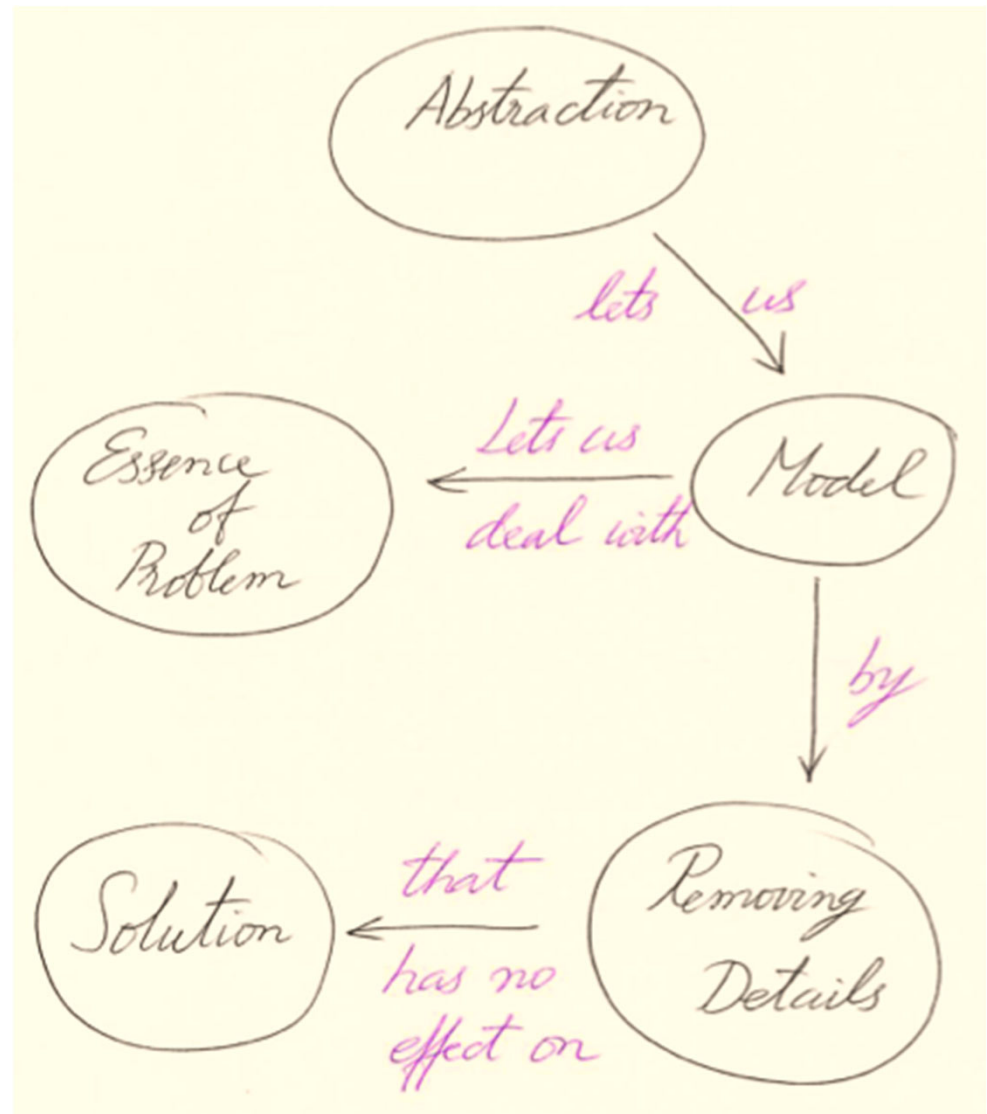
# Information System Architecture

**Information Systems Architecture (ISA)** is a structured framework that defines how an organization's information systems, data, processes, and technology components are organized and interact to support business operations and decision-making. It provides a blueprint for developing, managing, and integrating IT resources efficiently.

Abstraction in **Information System Architecture** refers to the process of **hiding complex implementation details** while exposing only the necessary and relevant aspects of a system. It simplifies the design and understanding of large, intricate systems by breaking them down into manageable components with well-defined interfaces.

ISA is an **abstraction** that provides the “big picture” goals for the system

- Guides the development process, answering questions including:
  - How s 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?





# 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

A **conceptual model** is a high-level representation of an information system that defines the structure, key components, and relationships between elements **without detailing implementation specifics**. It serves as an **abstract framework** to understand how different parts of a system interact and supports decision-making during system design and development.

## Key Characteristics of a Conceptual Model

### 1.High-Level Abstraction

1. Focuses on **what** the system should do rather than **how** it will be implemented.
2. Ignores low-level technical details like programming languages, databases, or hardware.

### 2.Graphical or Descriptive Representation

1. Often depicted using diagrams such as **Entity-Relationship Diagrams (ERD)**, **Unified Modeling Language (UML)** diagrams, or **flowcharts**.
2. Can also be described in textual form.

### 3.Defines System Scope and Boundaries

1. Helps stakeholders understand system functionality and **interactions between components**.
2. Defines **actors, entities, processes, and data flows**.

### 4.Guides System Development

1. Acts as a **blueprint** for creating detailed logical and physical models.
2. Helps developers and engineers design databases, software modules, and workflows.

The **conceptual model** and **abstraction** are closely related in **Information System Architecture**, as both aim to simplify complex systems by focusing on high-level representations and hiding unnecessary details

A **conceptual model** is a structured form of **abstraction** that provides a **blueprint for system design** before moving into **detailed implementation**.

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

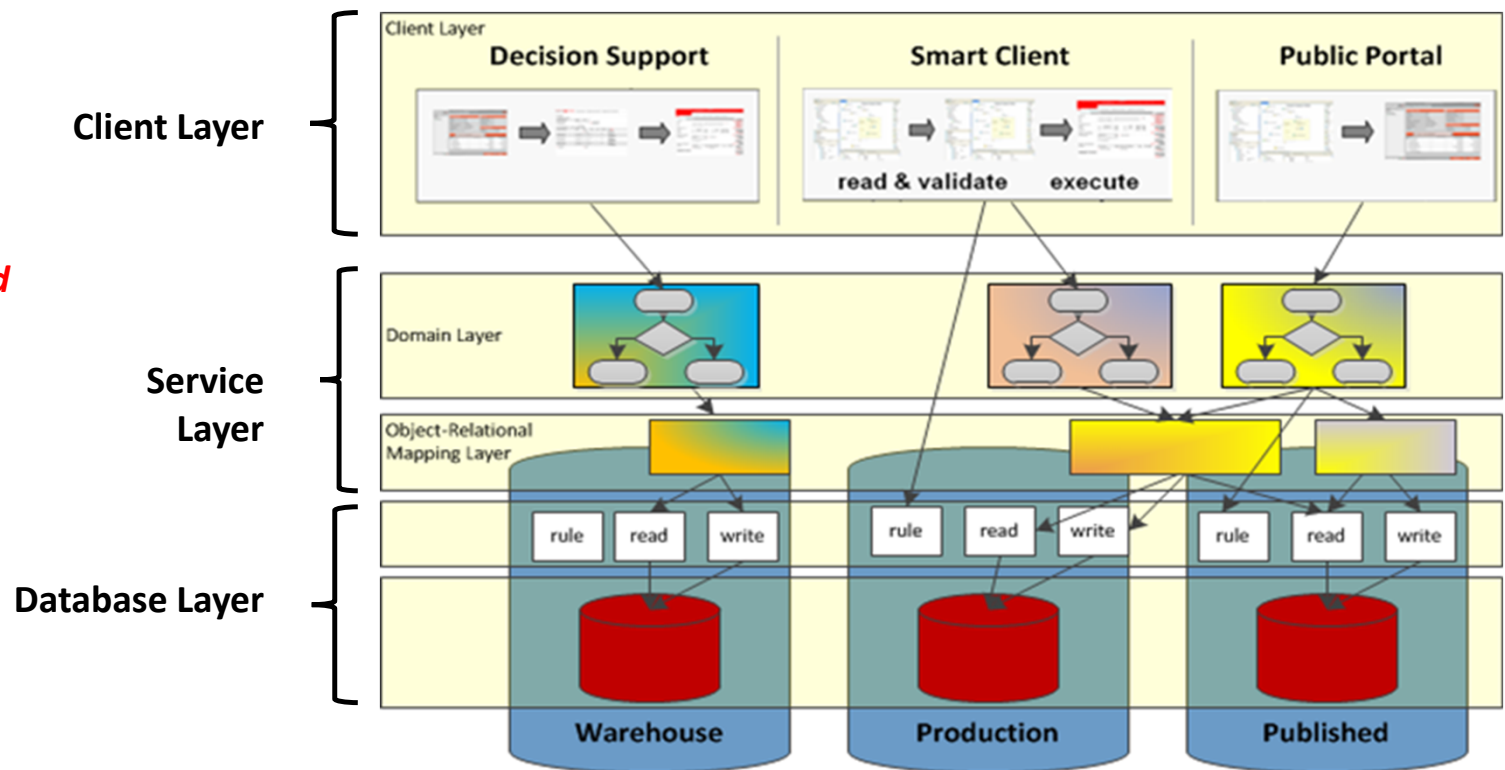
These three abstraction mechanisms complement each other in Information System Architecture:

Mechanism	Purpose	Example in a University System
Classification	Groups similar entities	Students, Professors, Courses as distinct classes
Aggregation	Represents whole-part relationships	University → Departments → Courses
Generalization	Defines hierarchy and inheritance	Person → Student, Professor, Staff

# Classification

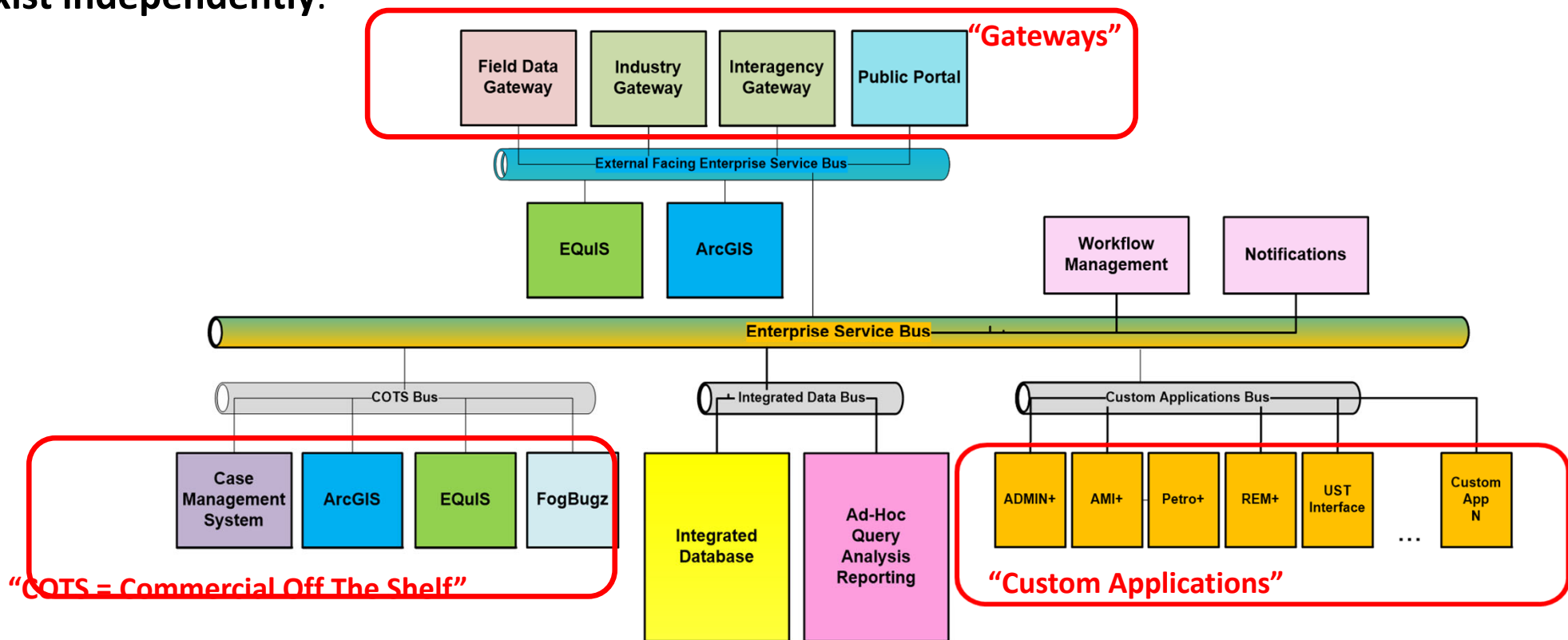
Classification is the process of **grouping objects with similar characteristics into categories (classes)**. It helps in structuring the system by defining **objects/entities** and their **attributes**.

*Example: Classes of software types within an enterprise service-oriented architecture*



# Aggregation

Aggregation is a **"whole-part" relationship** where a **higher-level entity** is composed of multiple **lower-level entities**. It represents a **structural hierarchy** where components **can exist independently**.

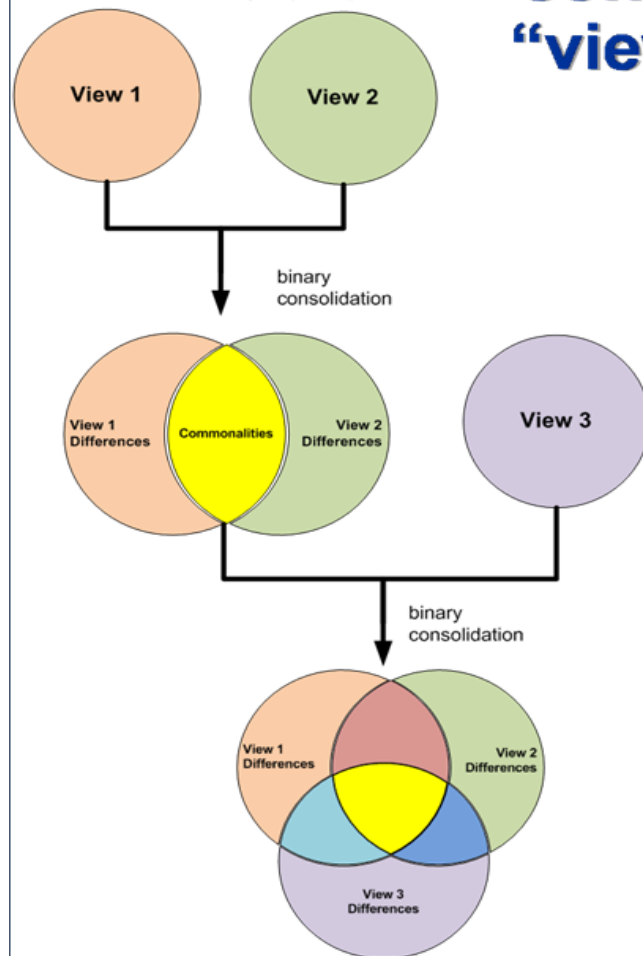


# Classification and Aggregation

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”

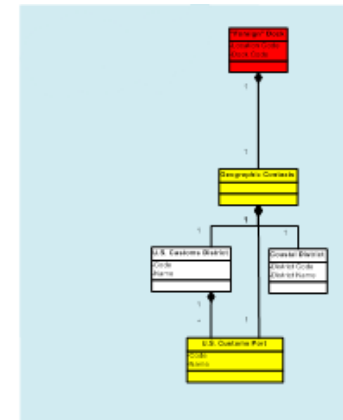
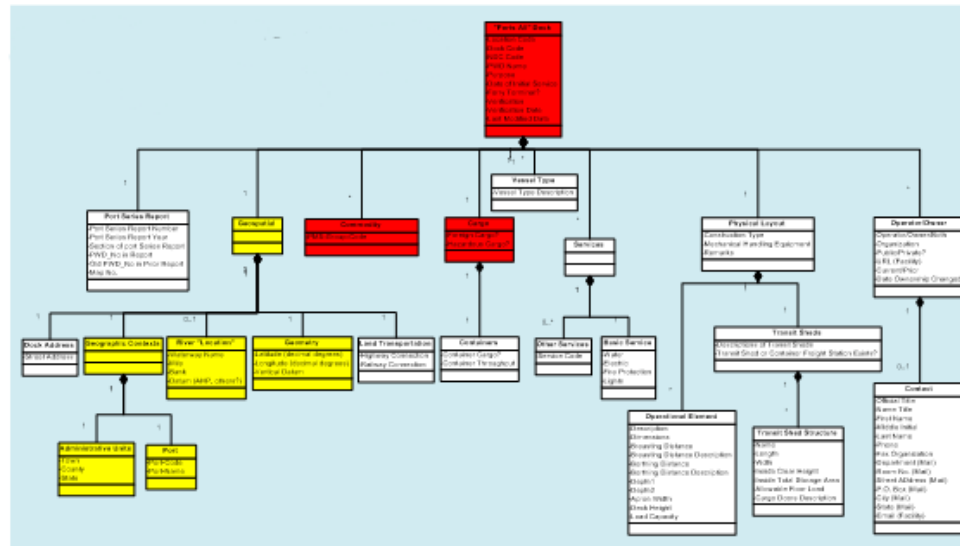
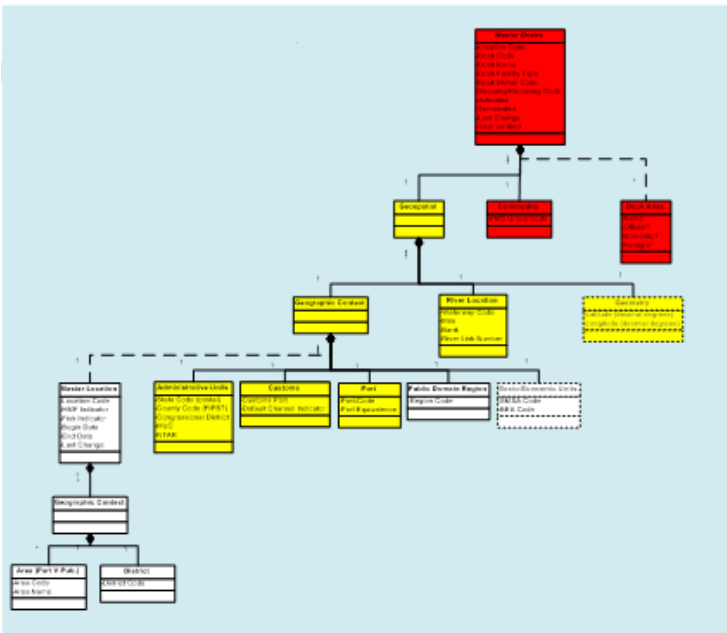


model integration achieved by:

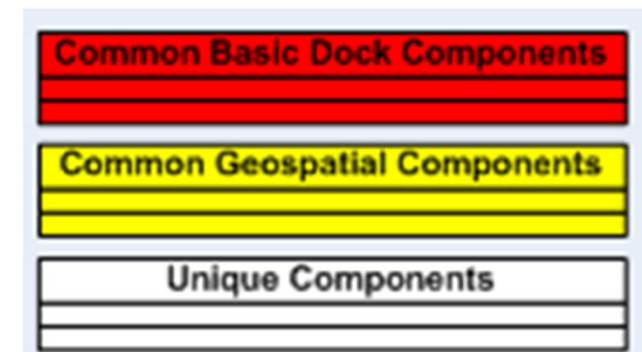
1. Identifying,
2. Resolving, and
3. Consolidating

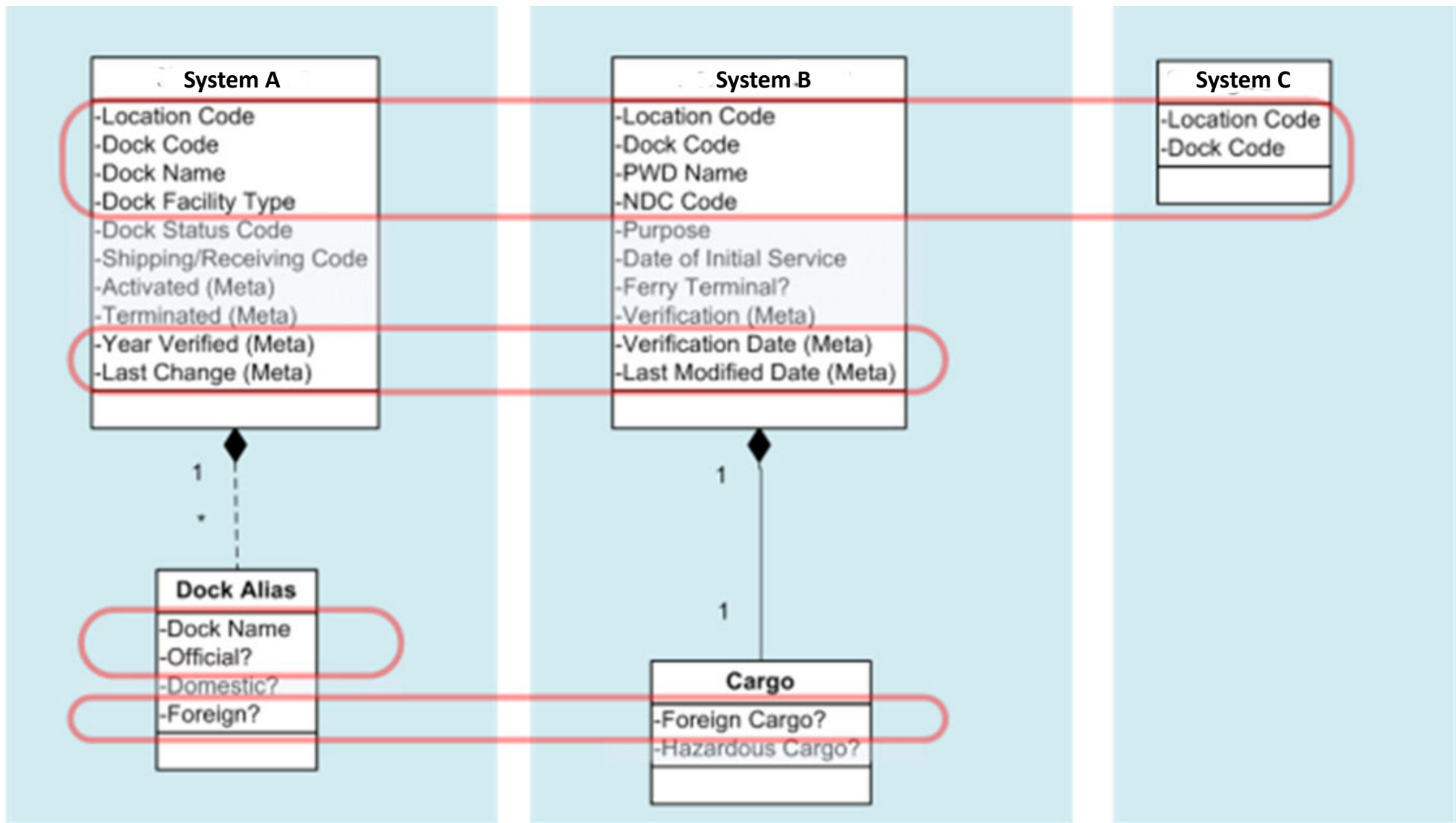
- **Commonalities** (and synonyms)
- and
- **Differences** (and homonyms)

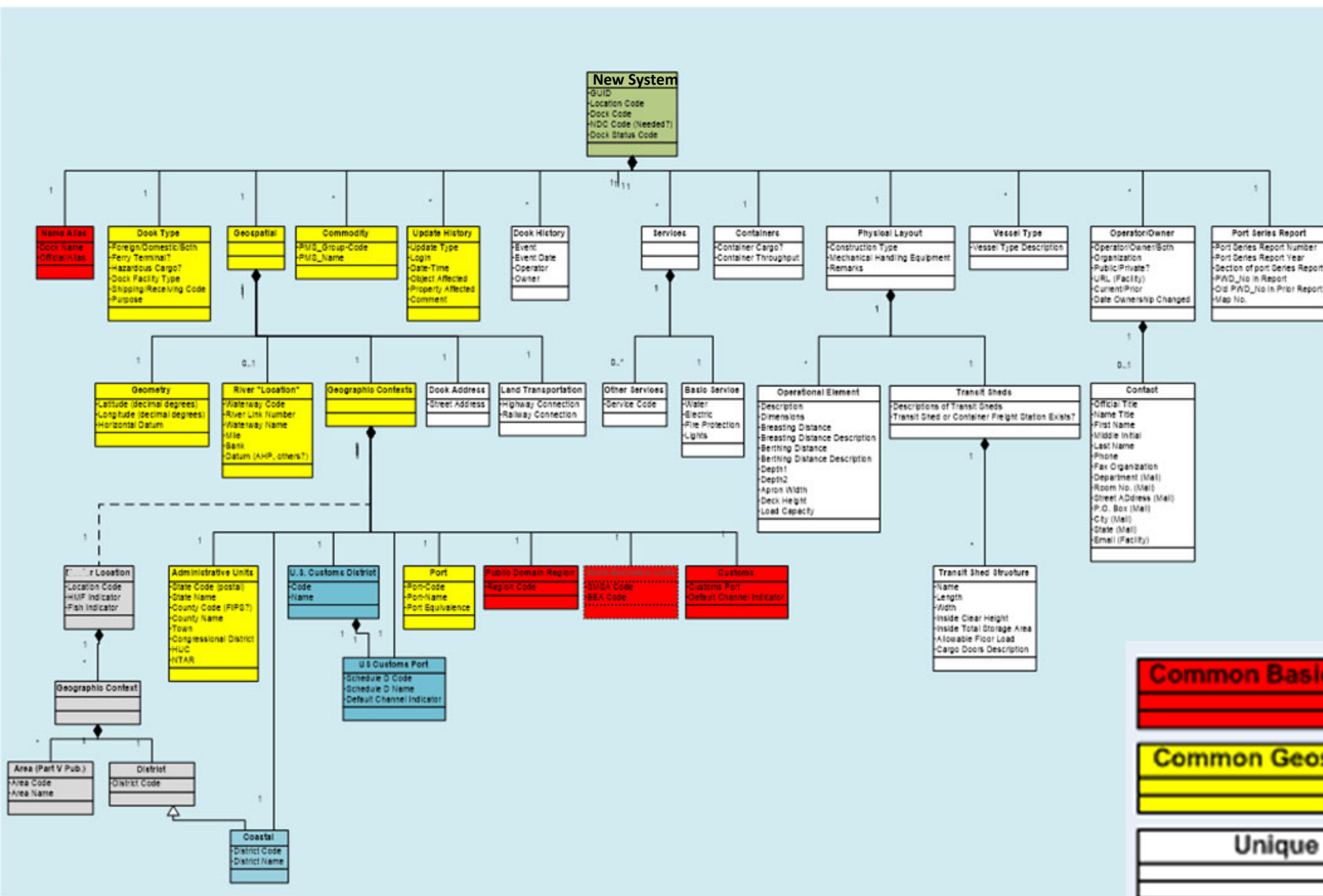




*Information models from disparate business units*







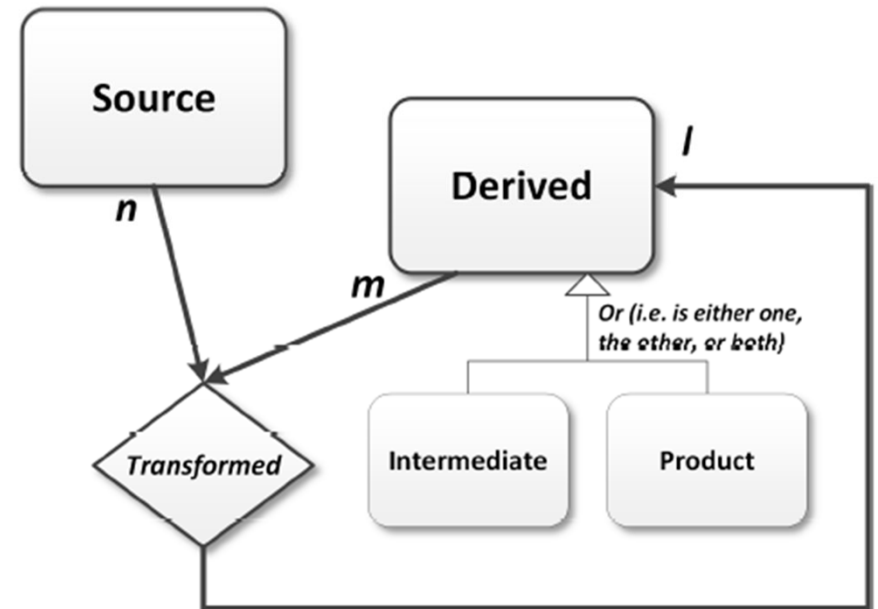
# Generalization

- A generalization abstraction defines a subset relationship between elements of two more classes

Generalization is a **hierarchical abstraction** where **similar entities share common properties** in a **parent (superclass)** and extend them in **child (subclass)** entities.

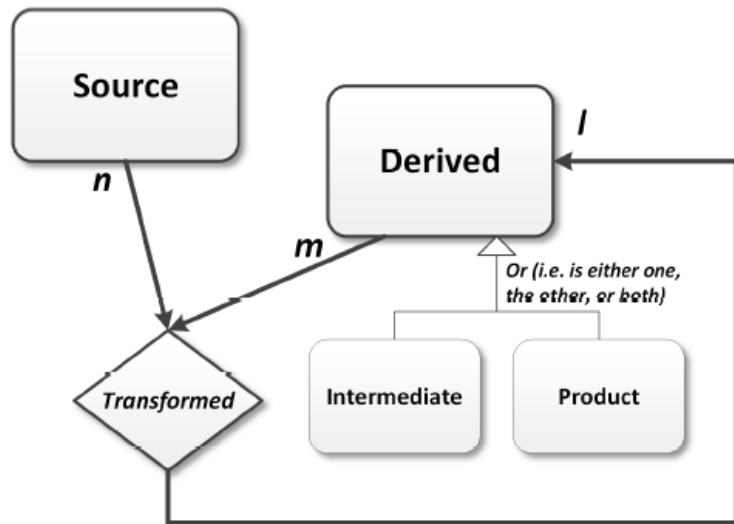
$Datasets = \{Dataset_i : i = source, derived\},$

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

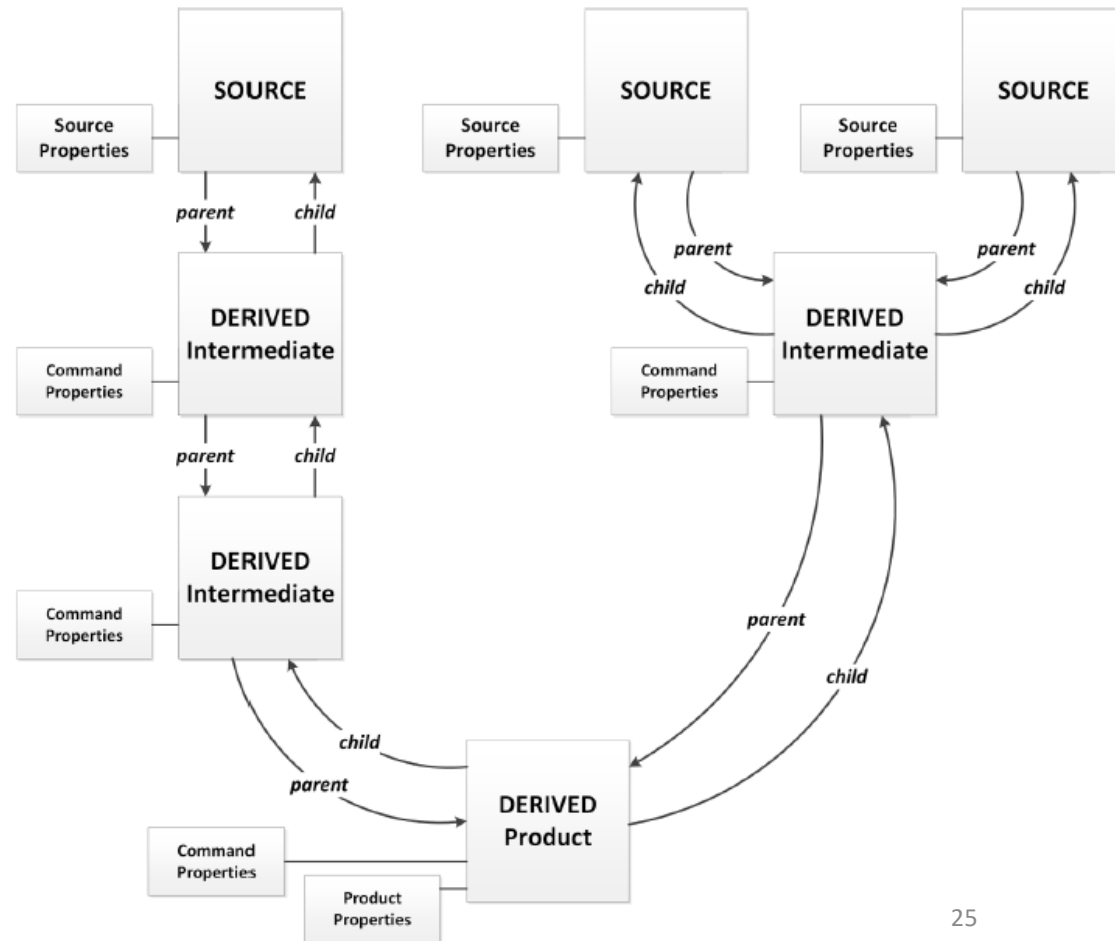


*Data lineage metadata model*

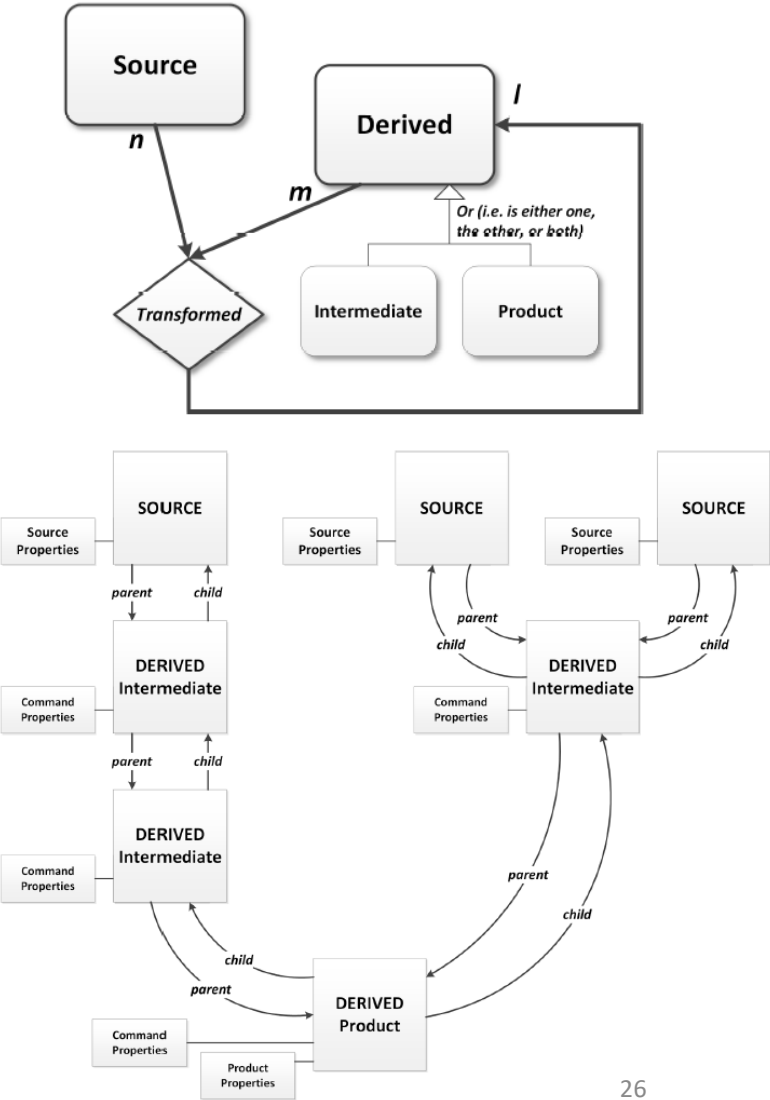
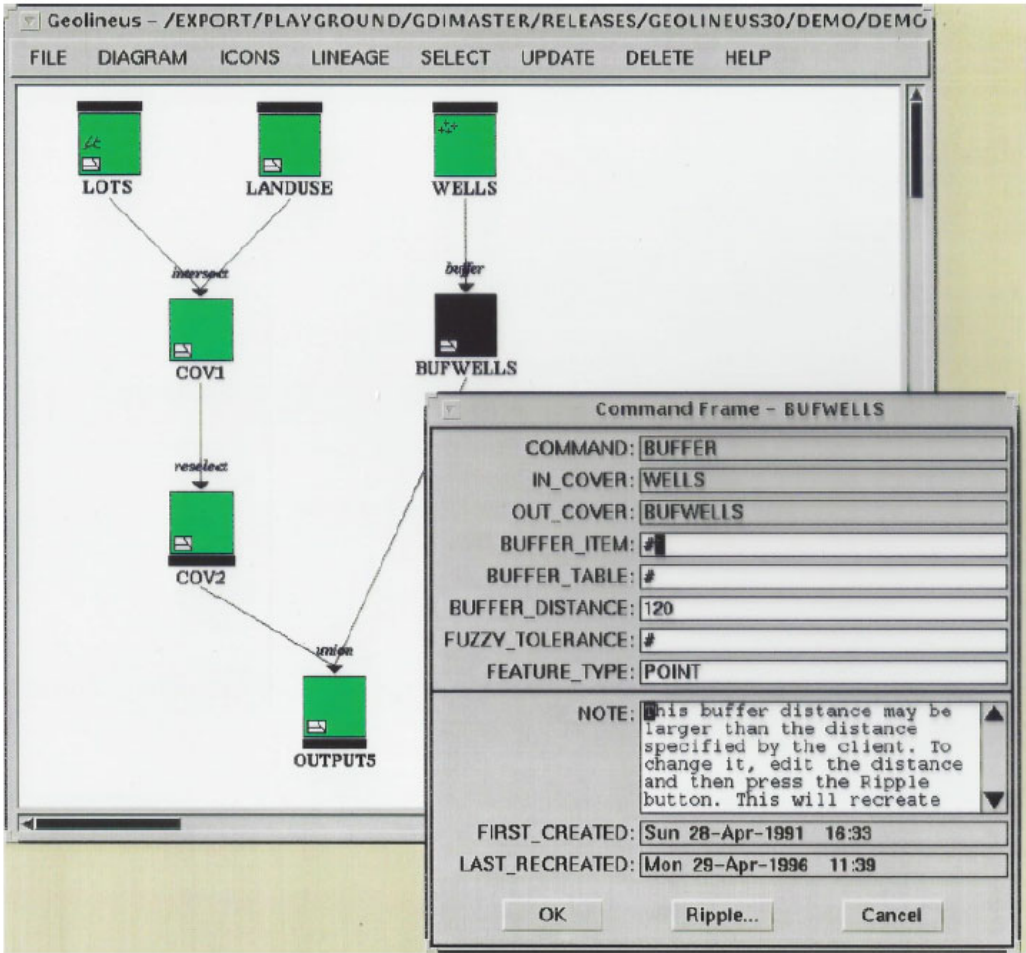
# Generalization enables partitioning objects and structuring common properties and methods



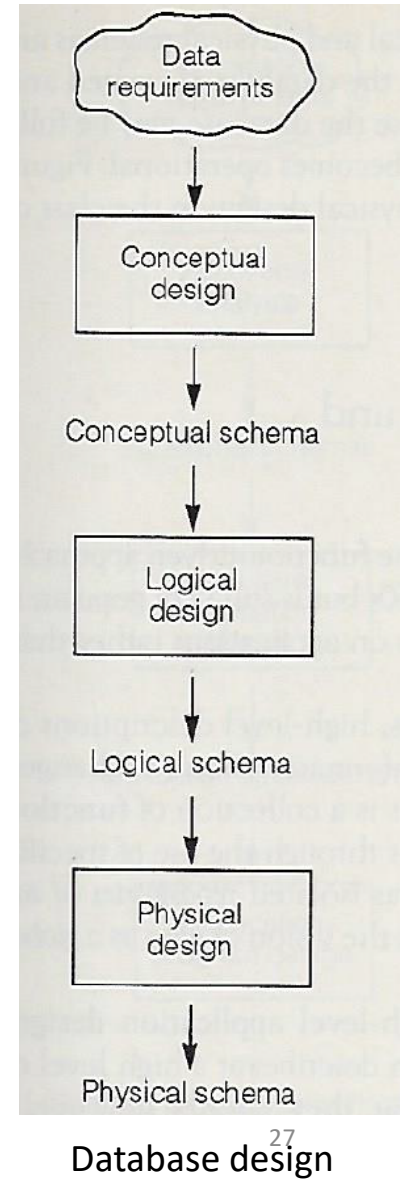
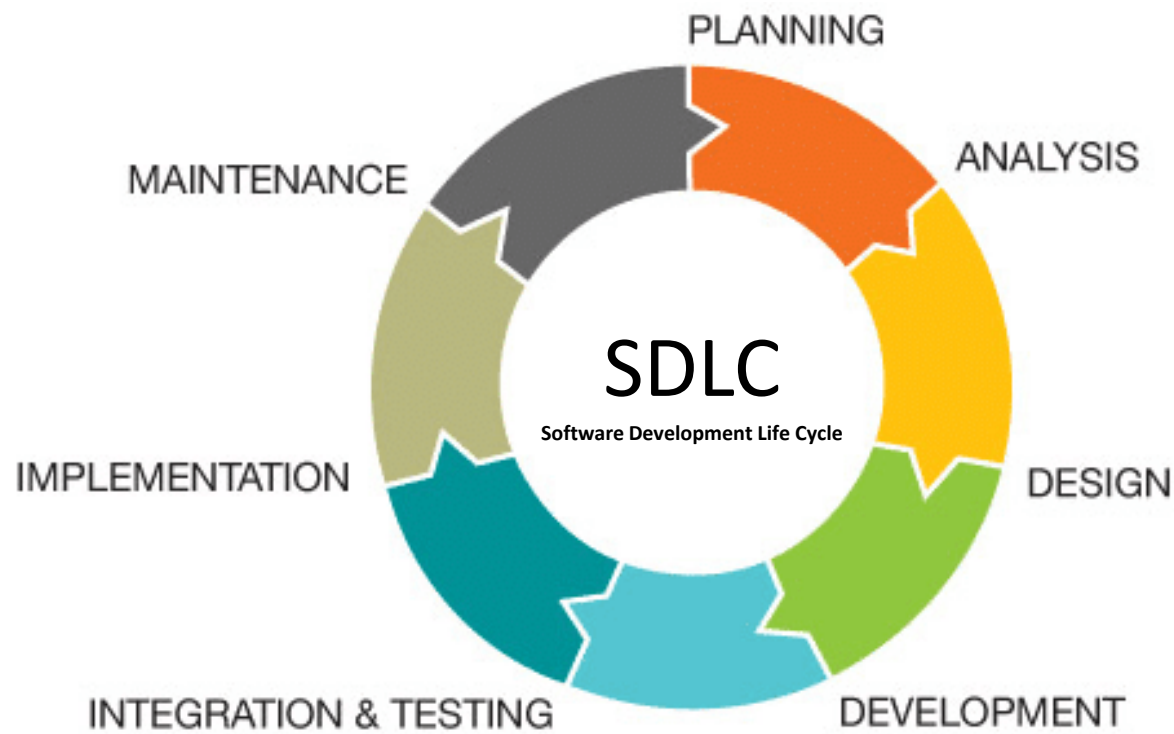
Example of generalizations of different types of datasets



# Data Provenance Metadata System

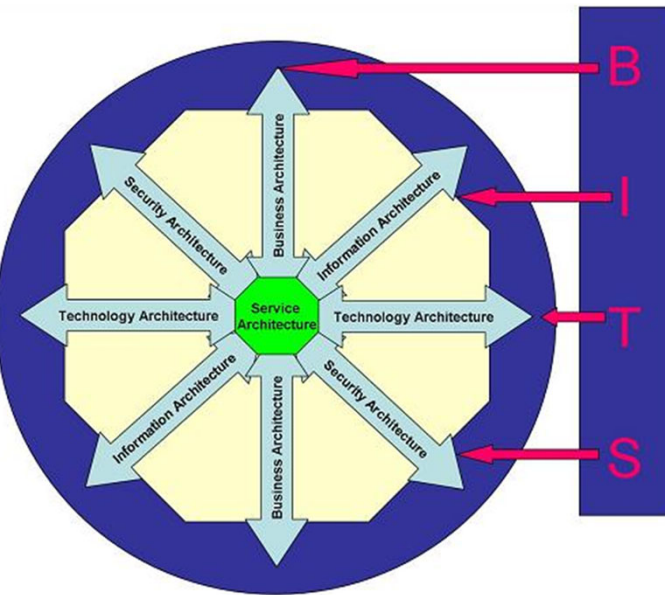


# *Conceptual models of information system design and development...*



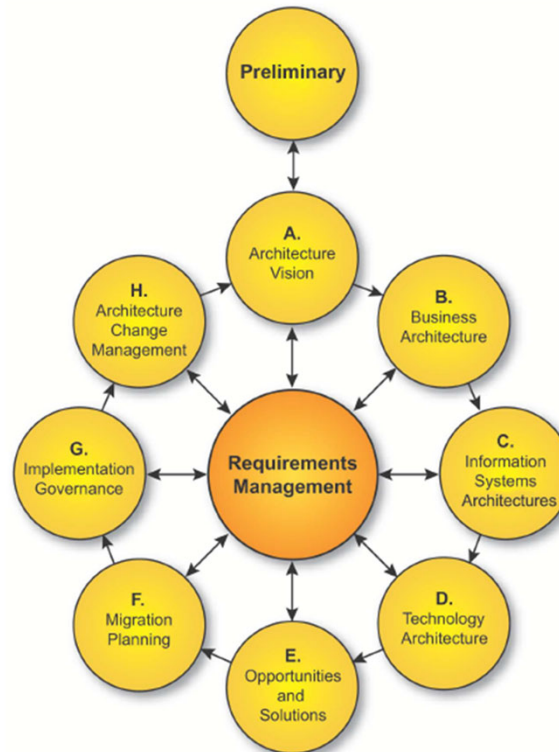


# Models help us understand enterprise information systems and their security



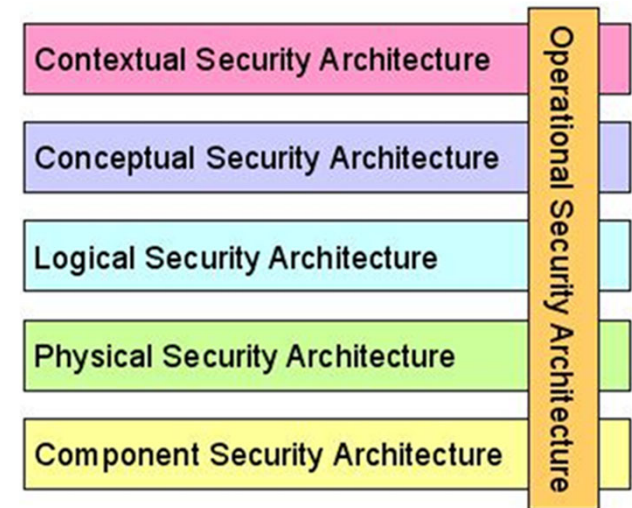
Horatio Huxham's BITS

[https://en.wikipedia.org/wiki/Enterprise\\_information\\_security\\_architecture](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](http://www.sabsa.org/white_paper)



Each of these frameworks—**BITS**, **TOGAF**, and **SABSA**—plays a crucial role in different aspects of enterprise architecture

The **BITS Security Framework** (BITS, or The Bank Policy Institute's BITS) is a set of security best practices specifically designed for financial institutions. It provides guidance on risk management, cybersecurity, fraud prevention, and information security governance.

**TOGAF** is an enterprise architecture framework that provides a structured approach for designing, implementing, and managing an organization's IT architecture. It consists of the **Architecture Development Method (ADM)** to help organizations align their IT infrastructure with business goals.

**SABSA** is a risk-driven enterprise security architecture framework that integrates security into business processes. It ensures security is built into IT systems from the start rather than added later.

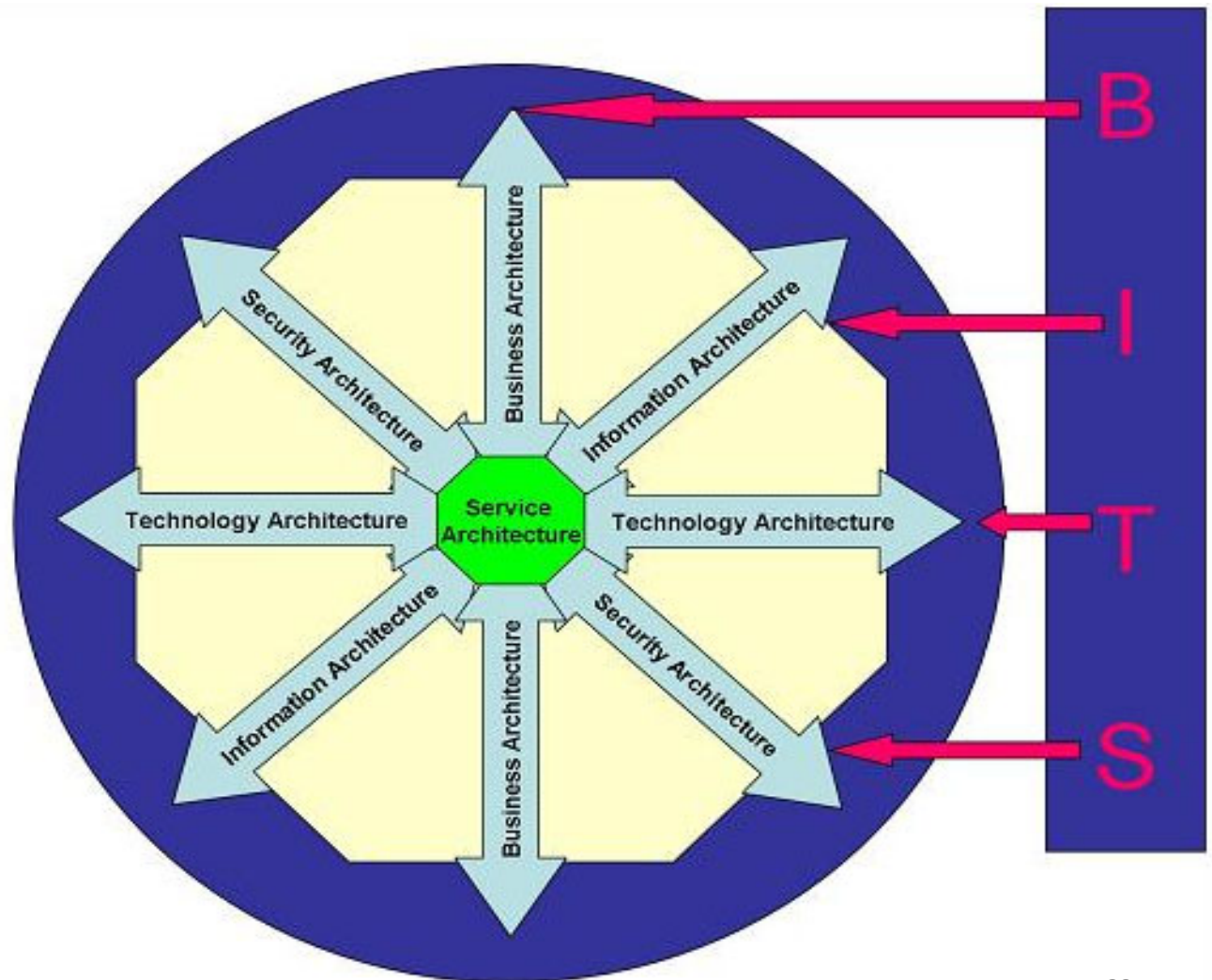
Wikipedia: [https://en.wikipedia.org/wiki/Enterprise\\_information\\_security\\_architecture](https://en.wikipedia.org/wiki/Enterprise_information_security_architecture), accessed 2017-1-19

## 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](https://en.wikipedia.org/wiki/Enterprise_information_security_architecture)

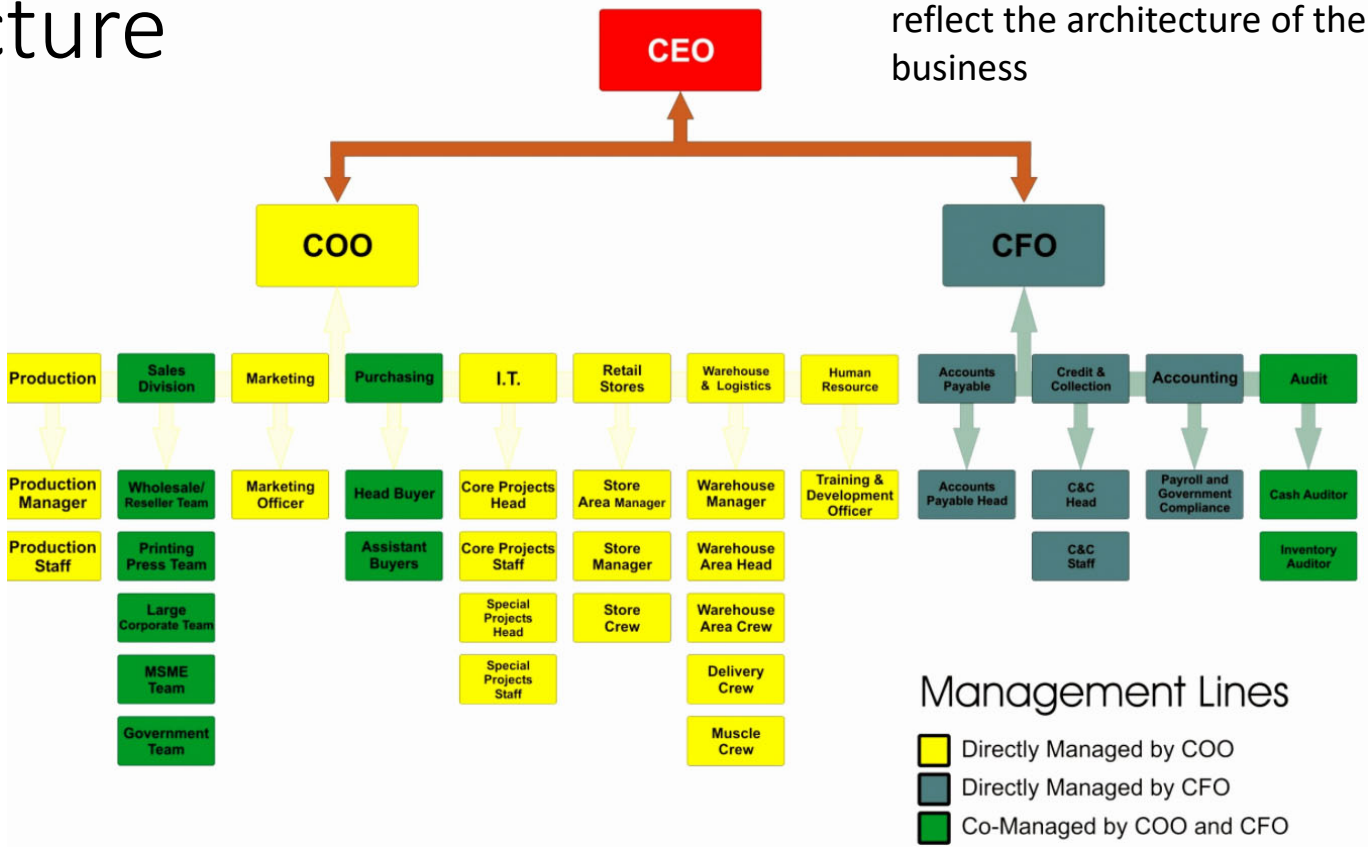


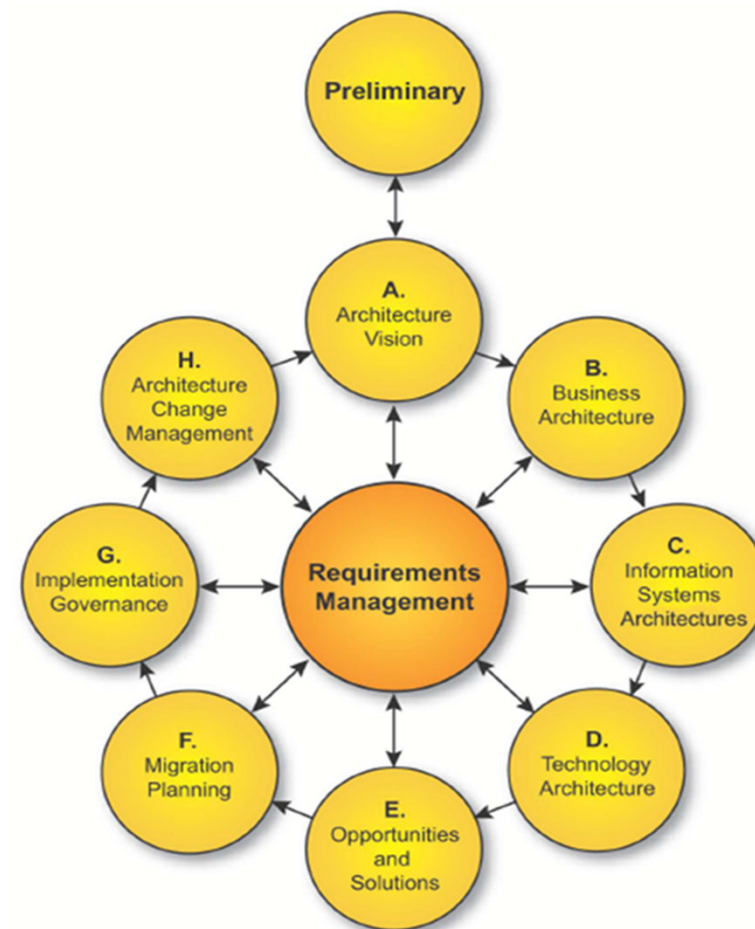
Framework	Business Architecture	Information Architecture	Technology Architecture	Security Architecture
<b>TOGAF</b>	Business process modeling, aligning IT with business	Defines data models, integration	Defines technology stack, system design	Provides general security considerations
<b>SABSA</b>	Aligns security with business goals	Implements data security policies	Embeds security in IT systems	<b>Main security architecture framework</b>
<b>BITS</b>	Ensures compliance with banking regulations	Covers financial data security	Defines security for financial IT systems	Enforces security controls in finance

# Business Architecture



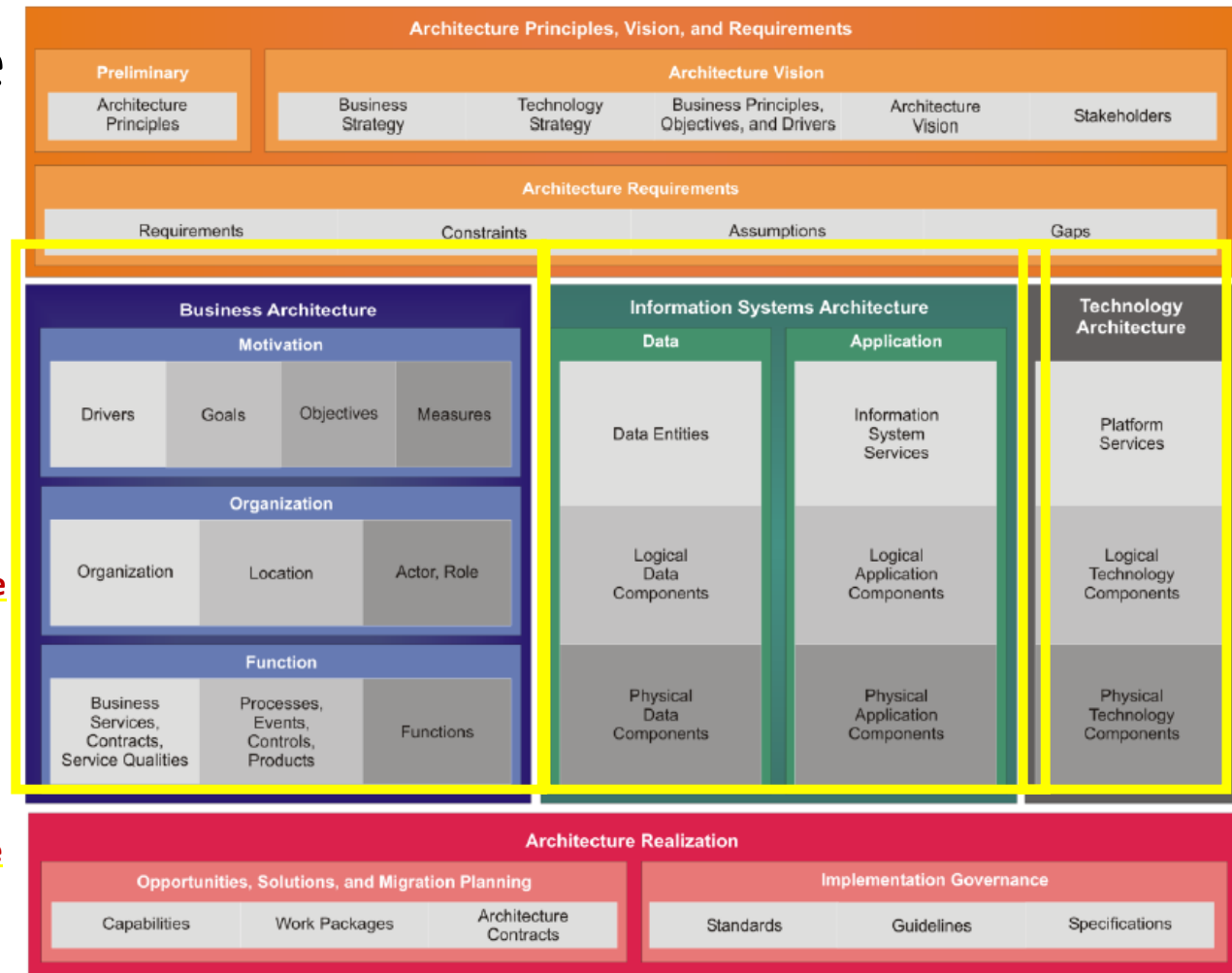
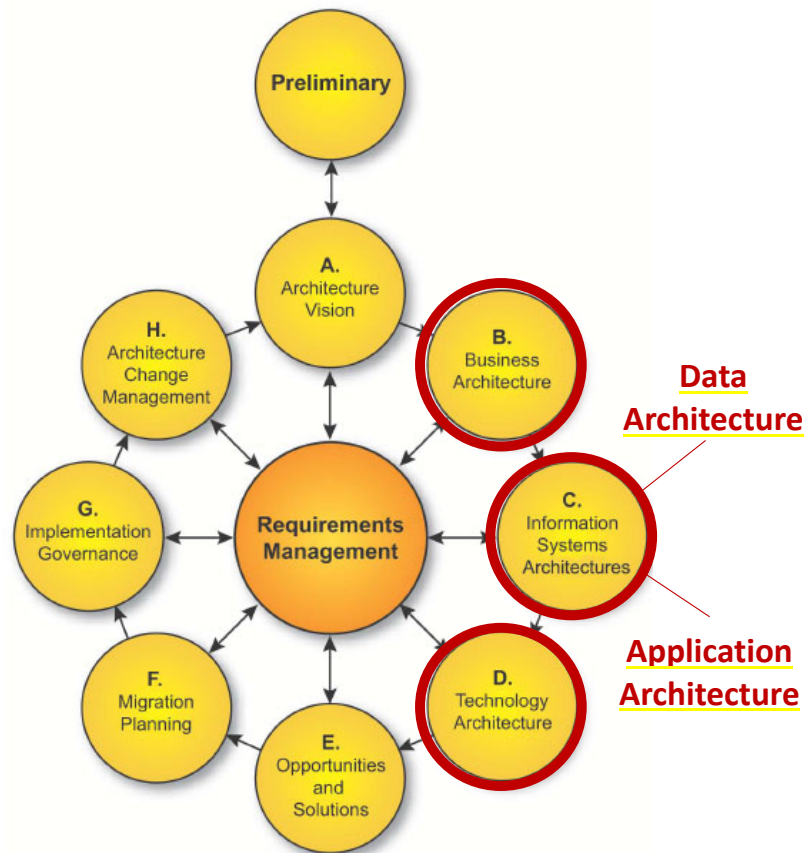
An organization chart may reflect the architecture of the business





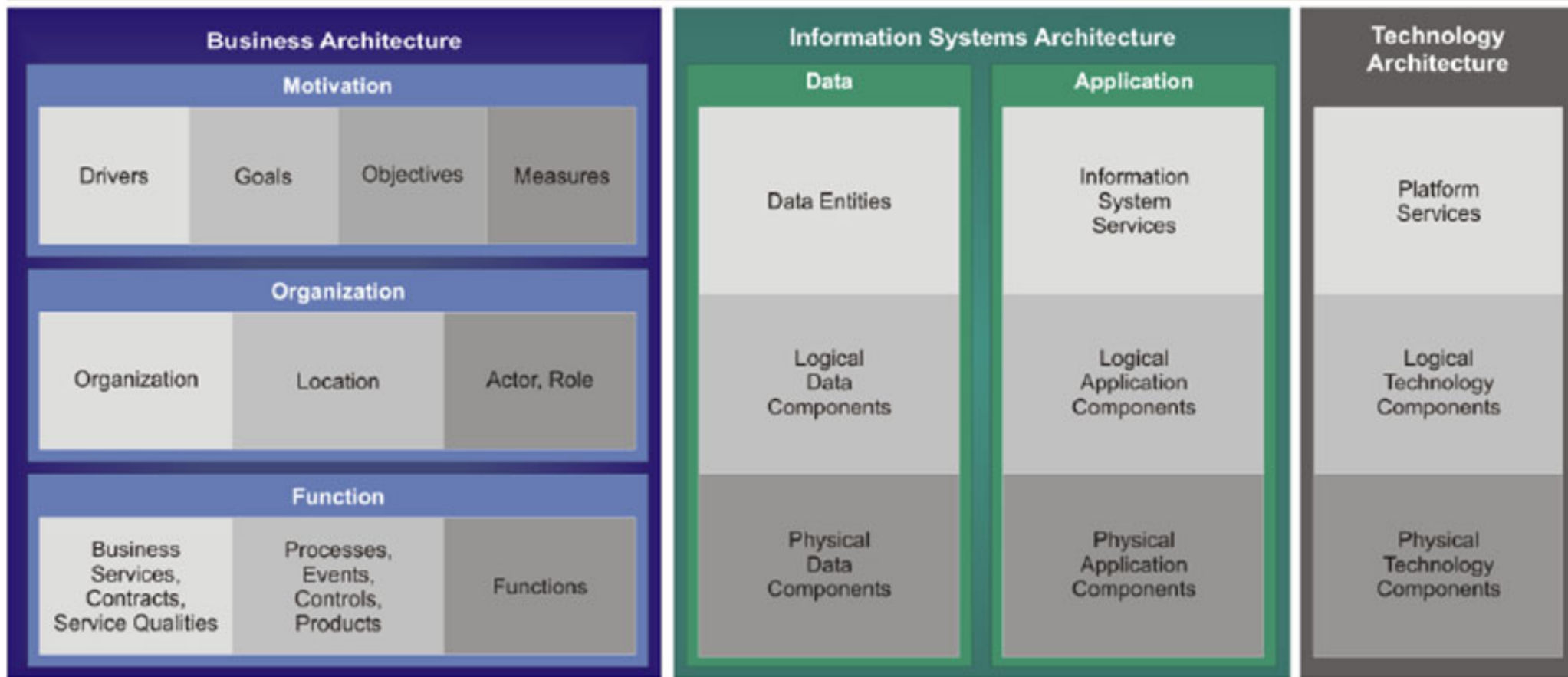
The Open Data Group Architecture Framework  
(TOGAF) Version 9.1

# Information Architecture



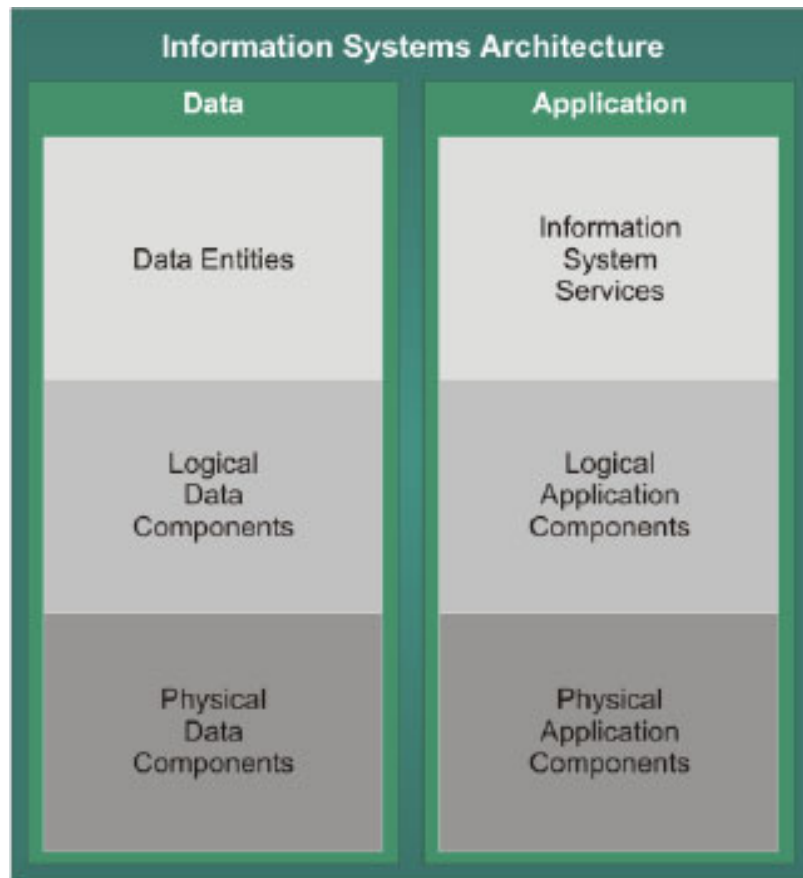
TOGAF Content Metamodel

# Information Architecture



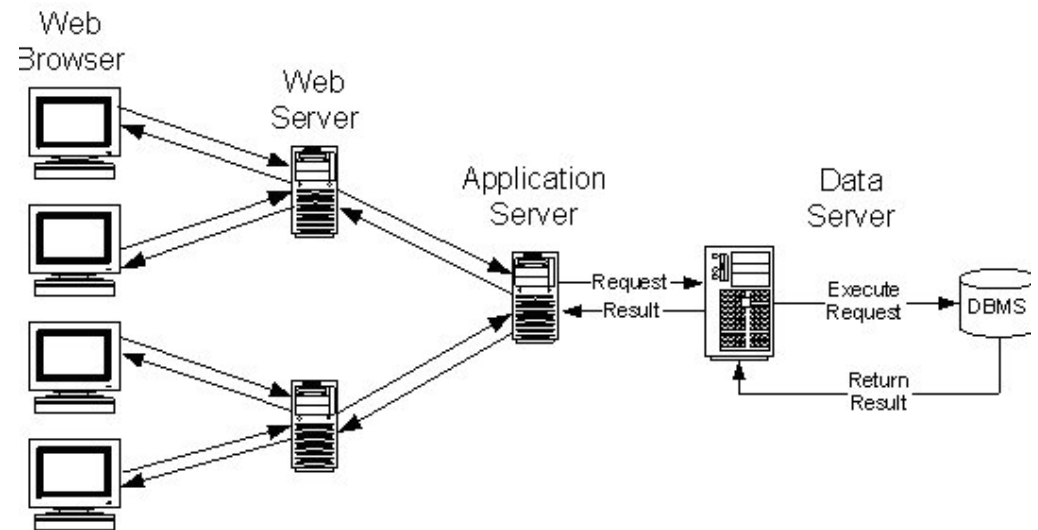


# Conceptual models of Information Systems



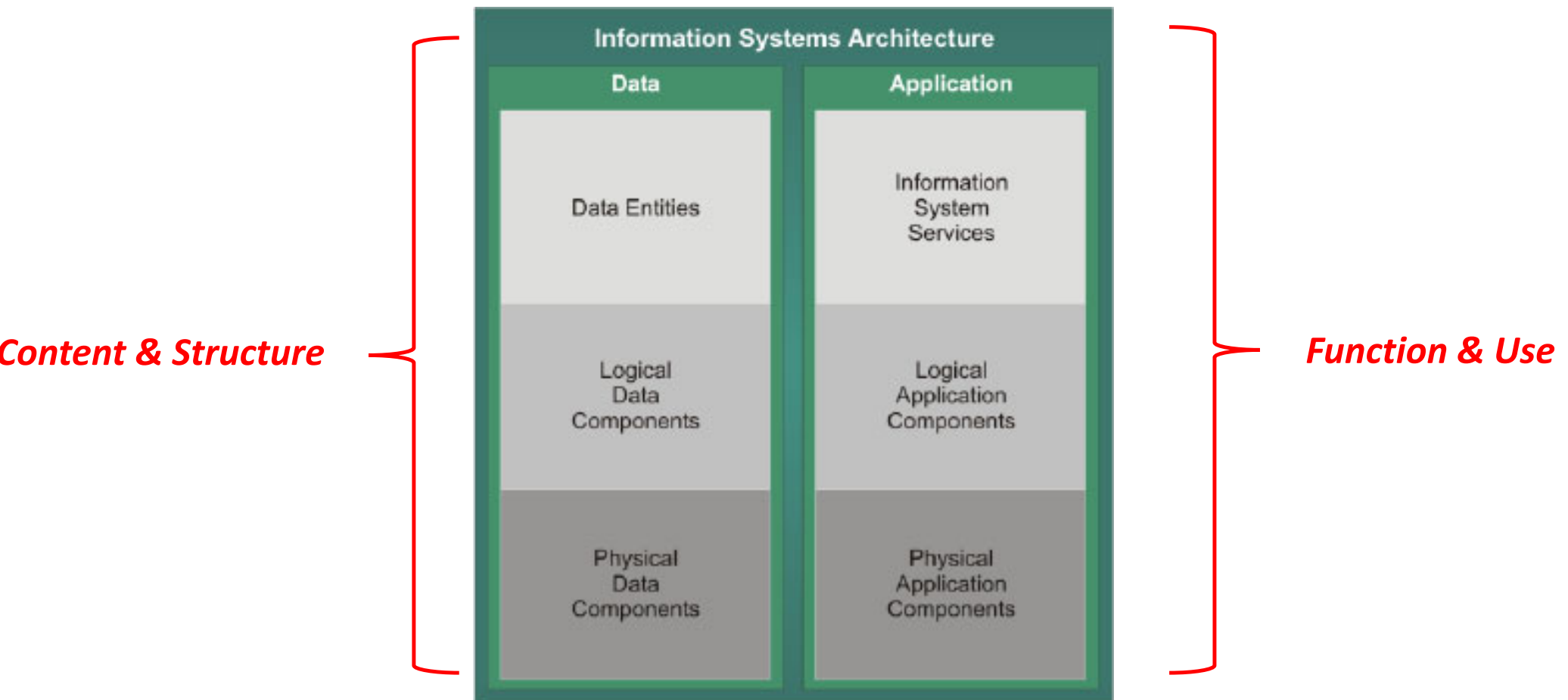
Content &  
Structure

Function &  
Use



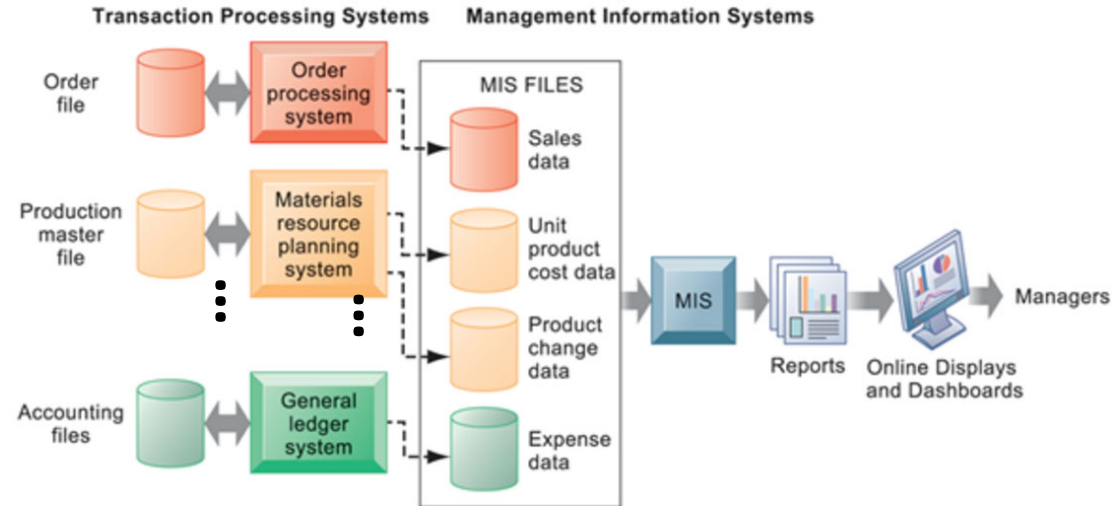
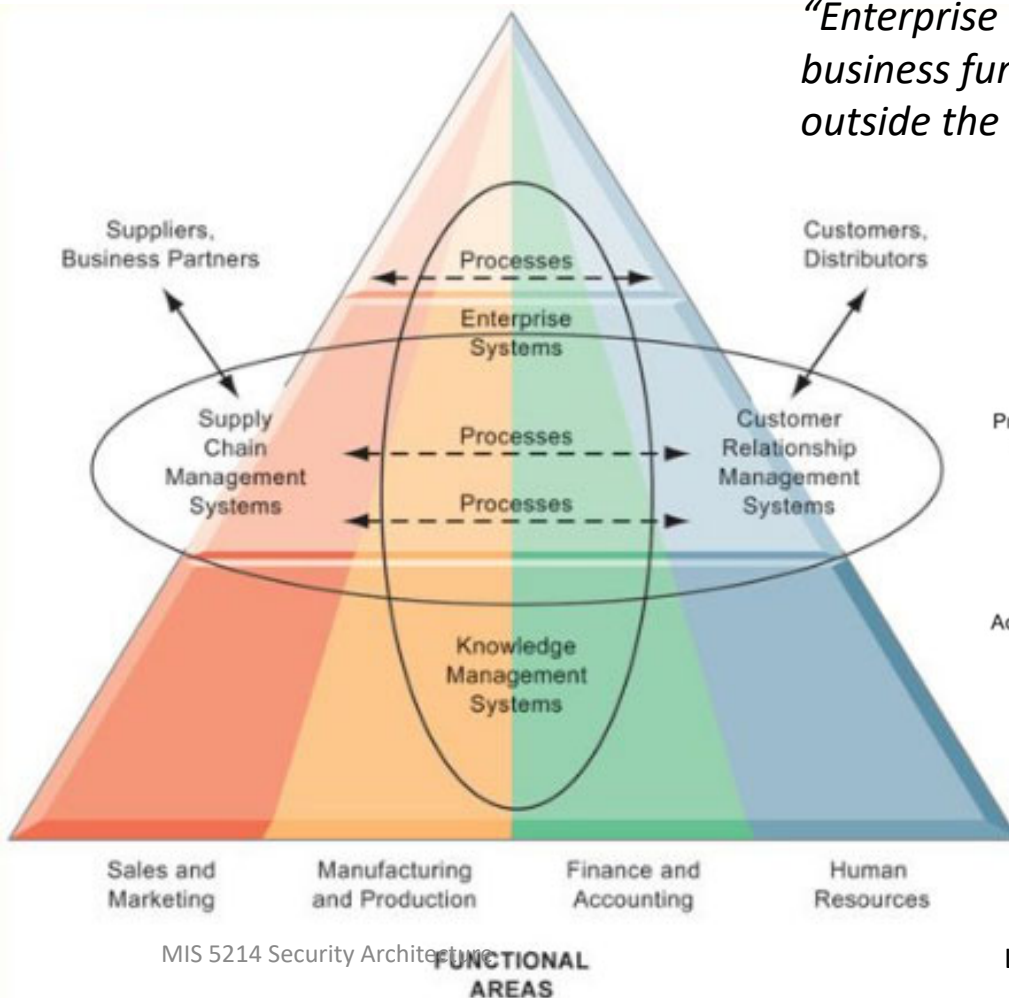


# Conceptual models of Information Systems



# Information Systems – Models of Information Flows

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



An example of an  
important security  
architecture model:

## “Defense in Depth”

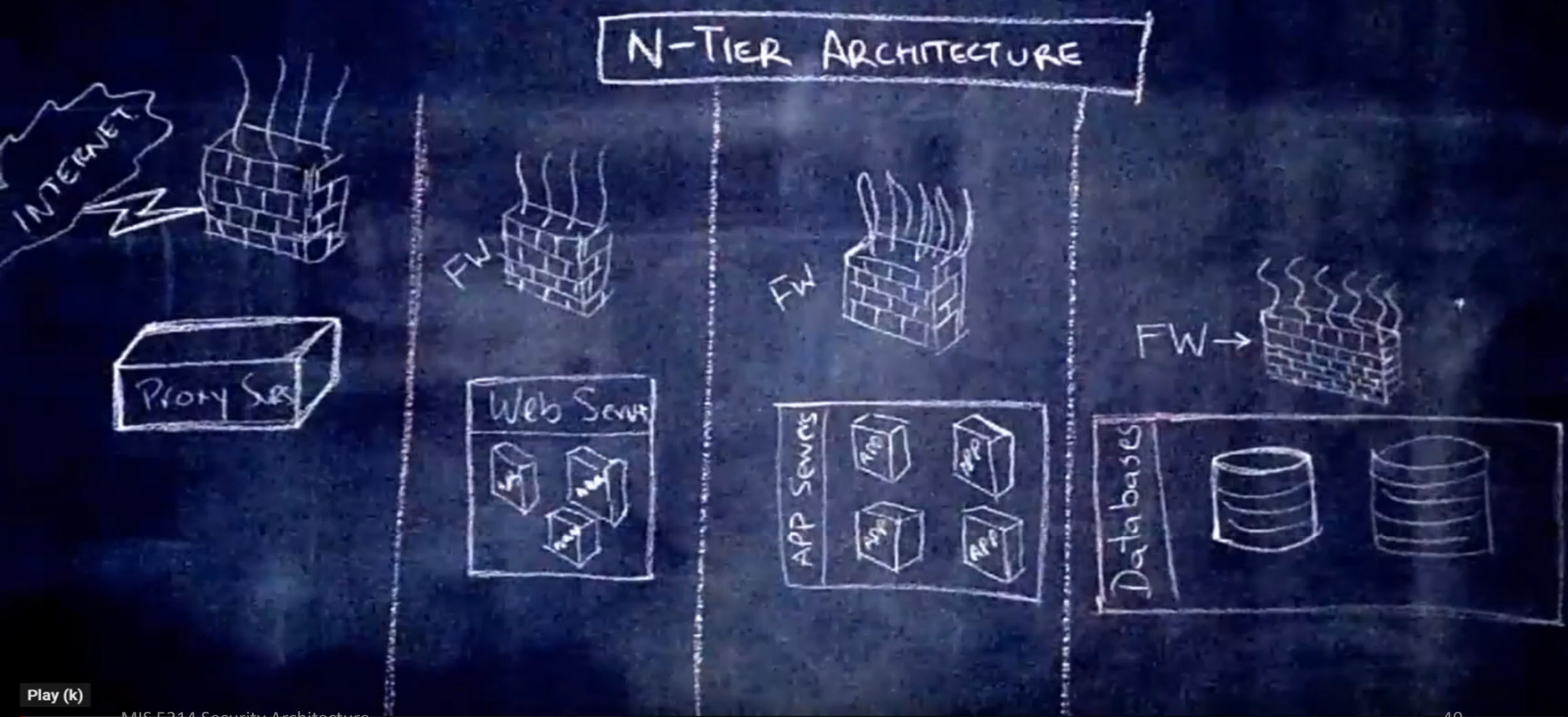
Also known as:

- *Layered Security*

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







Play (k)

MIS 5214 Security Architecture

0:01 / 12:20

Scroll for details

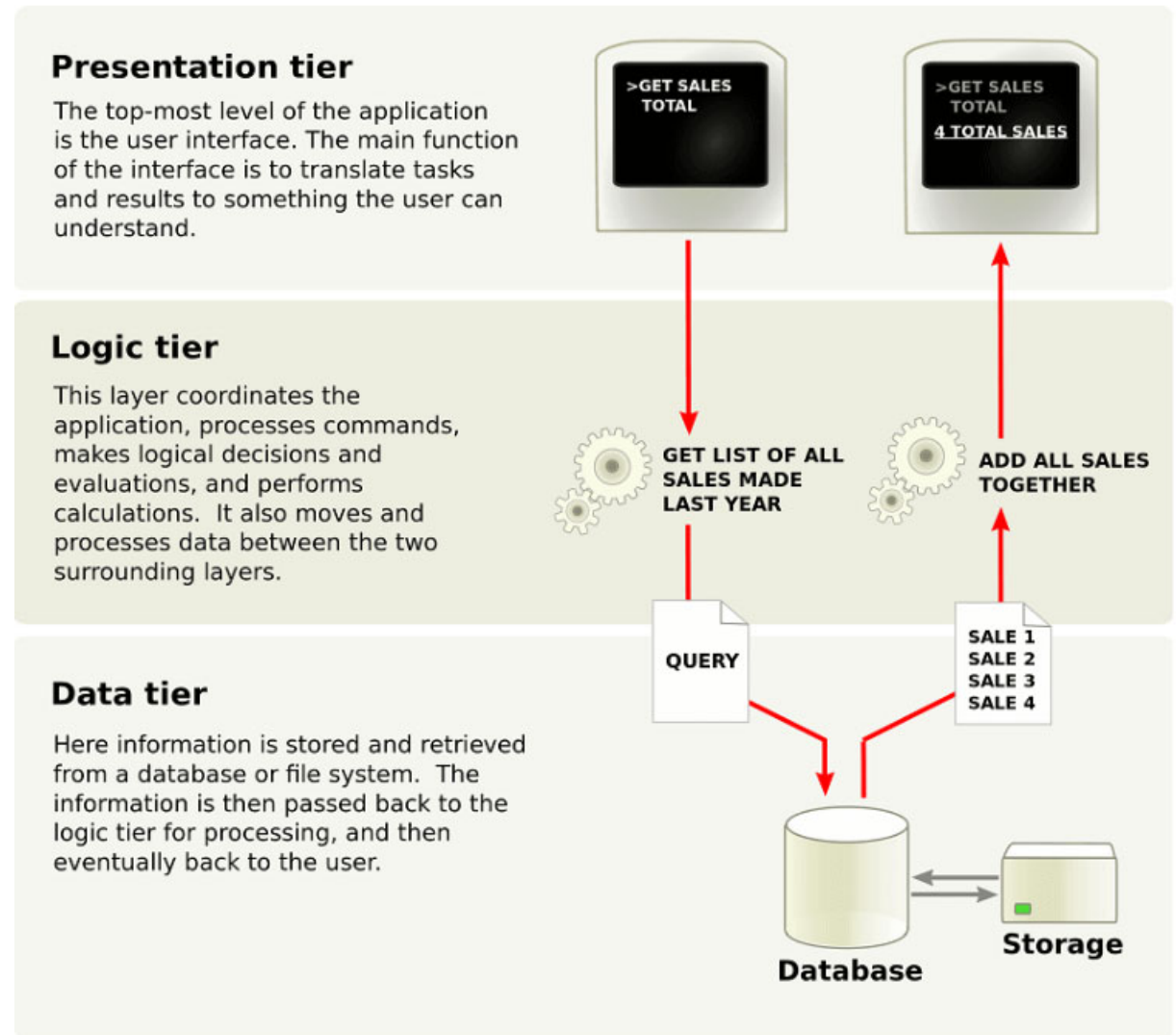
## For practice: Draw a conceptual mode of an N-Tier Architecture for a Web-Based System

- 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/>

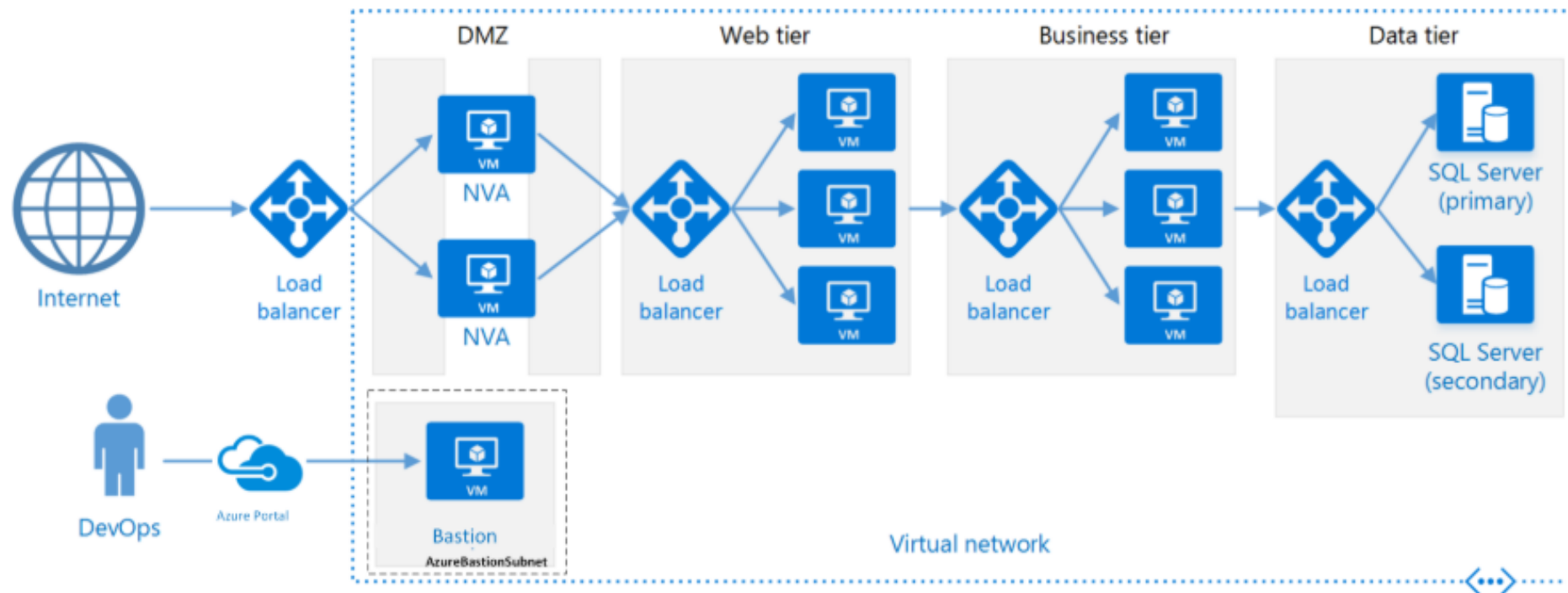
- Identify in your diagram:
  1. Where the users are ?
  2. How their data flows through the system as they access and view their billing records ?

N-tier architecture is also called multi-tier architecture because the software is engineered to have the processing, data management, and presentation functions physically and logically separated.



# N-tier architecture on virtual machines

This section describes a recommended N-tier architecture running on VMs.

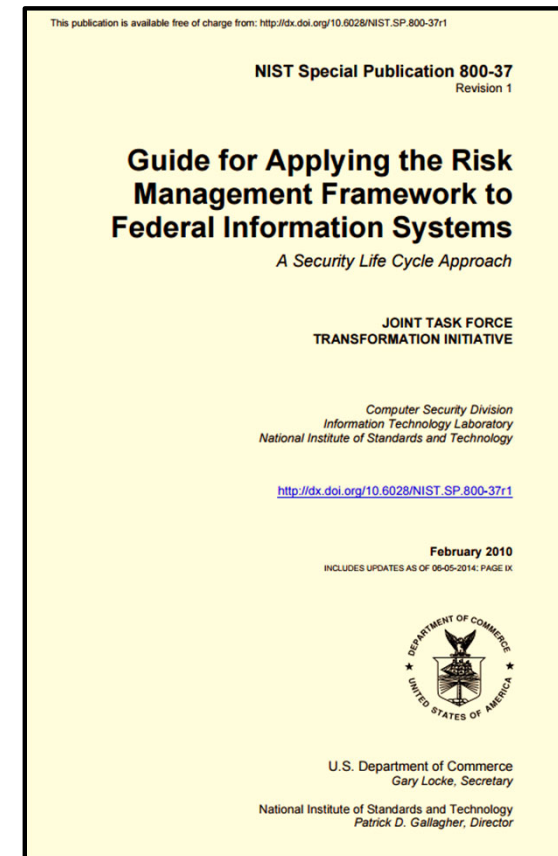
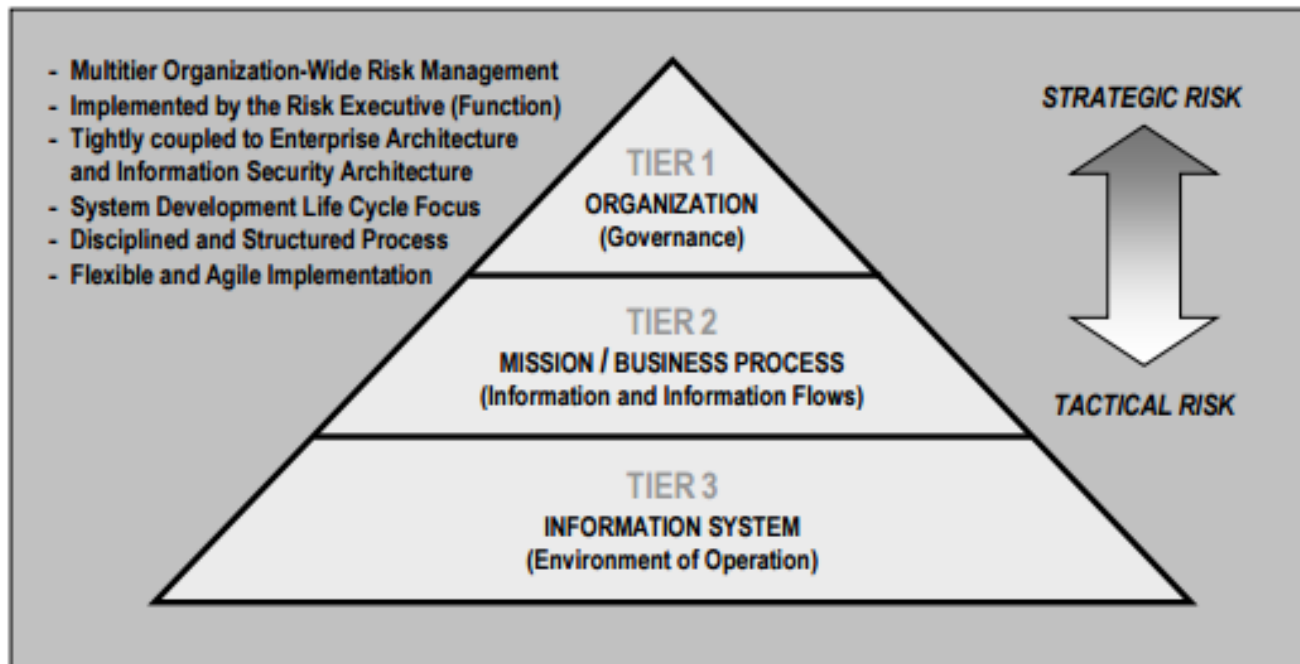


# Agenda

- ✓ 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



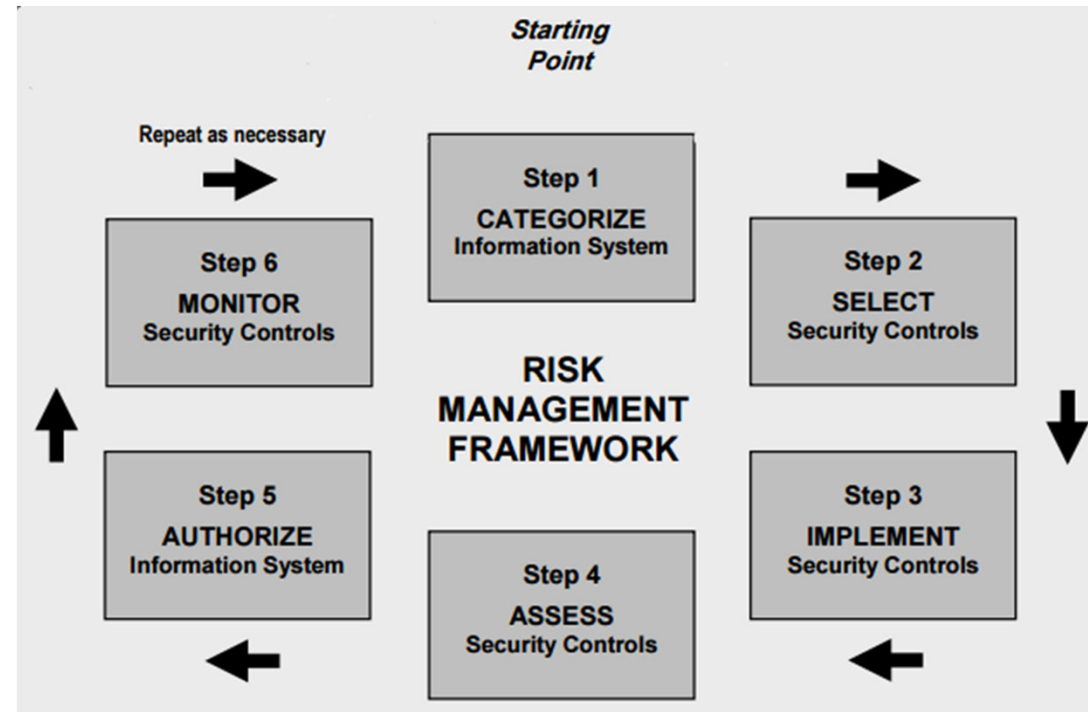
# NIST Risk Management Framework



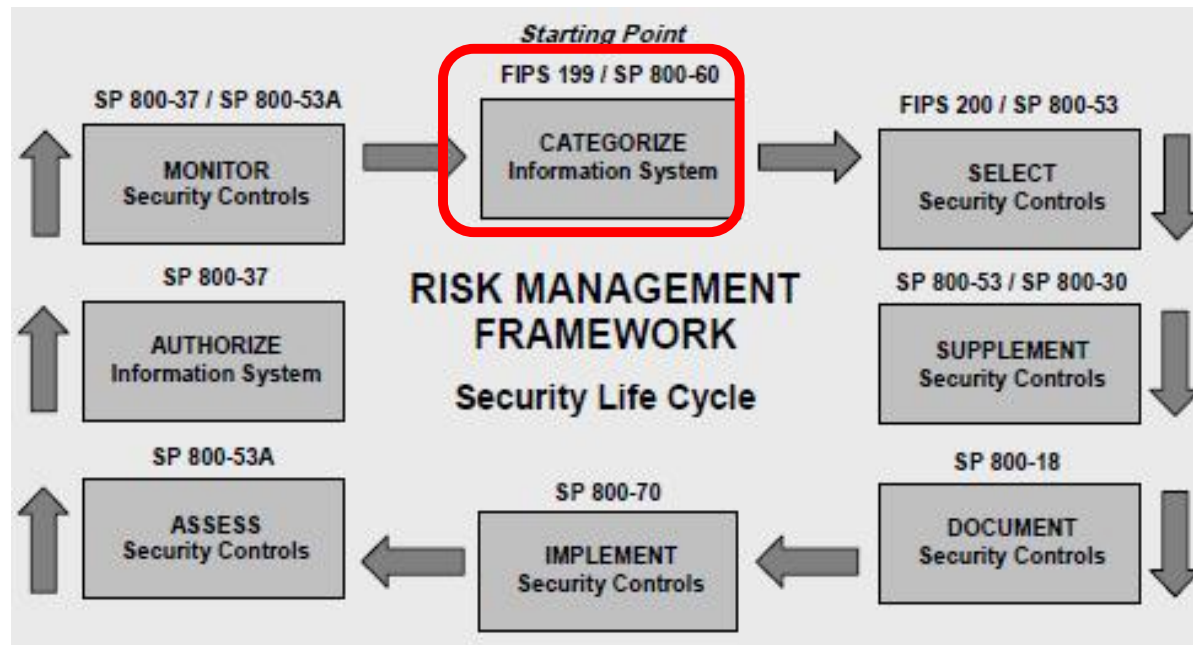
# Risk Management Framework

The **Risk Management Framework (RMF)**, defined in **SP 800-37**, provides a **security life cycle** approach:

- 1. Categorize** – Identify system impact using FIPS 199 / SP 800-60.
- 2. Select** – Choose security controls using FIPS 200 / SP 800-53.
- 3. Implement** – Apply security controls (SP 800-70).
- 4. Assess** – Evaluate control effectiveness (SP 800-53A).
- 5. Authorize** – Accept system risk (SP 800-37).
- 6. Monitor** – Continuously track security controls (SP 800-37 / SP 800-53A).



# NIST Risk Management Framework



Before implementing security controls, organizations must first **understand the information system, its business context, and risk environment**. This step aligns with NIST CSF **Identify** and **Risk Assessment** functions.

# Qualitative risk assessment based on security objectives

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<b><i>Confidentiality</i></b> 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 <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Integrity</i></b> 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 <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
<b><i>Availability</i></b> 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 <b>limited</b> 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 <b>serious</b> 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 <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.

A **dataset** refers to any collection of structured or unstructured data that is used, processed, stored, or transmitted within an organization's information systems. This dataset can include information related to cybersecurity risks, incidents, assets, threat intelligence, logs, configurations, and any other data relevant to an organization's cybersecurity posture.

# 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:

$$\text{SC information system} = \{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\},$$
  
where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:

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

and

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

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

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

*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
<b>Comm_Electric Geodatabase</b>	<b>High</b>	<b>Moderate</b>	<b>Moderate</b>	<b>High</b>
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
<b>Water_Sewer Geodatabase</b>	<b>Moderate</b>	<b>Moderate</b>	<b>Low</b>	<b>Moderate</b>
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
				<b>High</b>

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
<b>Comm_Electric Geodatabase</b>	<b>High</b>	<b>Moderate</b>	<b>Moderate</b>	<b>High</b>
Water Distribution System	Moderate	Moderate	Low	Moderate
Sanitary Collection System	Low	Low	Low	Low
Storm Collection System	Low	Low	Low	Low
<b>Water_Sewer Geodatabase</b>	<b>Moderate</b>	<b>Moderate</b>	<b>Low</b>	<b>Moderate</b>
Parcel Boundary Shapefile	Low	Low	Low	Low
				<b>High</b>

To **transform qualitative risk assessment into quantitative risk assessment**, follow these key steps:

- 1. Define qualitative risk categories** (likelihood and impact).
- 2. Assign numerical values** (probability for likelihood, dollar values for impact).
- 3. Calculate SLE, ARO, and ALE** to quantify risk.
- 4. Use data-driven insights** to prioritize mitigation efforts and justify security investments.

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

## 1. Define the Risk Matrix (Qualitative Input)

A typical **qualitative risk matrix** categorizes risks based on **Likelihood (L)** and **Impact (I)** using subjective ratings such as Low, Medium, High.

### Example Qualitative Risk Matrix

Likelihood \ Impact	Low Impact	Medium Impact	High Impact
Low Likelihood	Low Risk	Low Risk	Medium Risk
Medium Likelihood	Low Risk	Medium Risk	High Risk
High Likelihood	Medium Risk	High Risk	Critical Risk

## 2. Assign Numerical Values to Likelihood and Impact

To **quantify** qualitative ratings, assign **probability values** to likelihood and **monetary values** to impact.

### Example of Mapping Likelihood to Probability (%)

Qualitative Likelihood	Probability (%)	Annualized Rate of Occurrence (ARO)
Rare (Low)	1-10% (0.01 - 0.1)	0.1
Unlikely (Medium-Low)	11-30% (0.11 - 0.3)	0.2
Possible (Medium)	31-50% (0.31 - 0.5)	0.5
Likely (Medium-High)	51-80% (0.51 - 0.8)	0.7
Almost Certain (High)	81-100% (0.81 - 1)	0.9

### Example of Mapping Impact to Monetary Value

Qualitative Impact	Financial Impact (\$)
Low	\$10,000 - \$50,000
Medium	\$50,000 - \$500,000
High	\$500,000 - \$5,000,000
Critical	\$5,000,000+

### Scenario:

A company has an **important server** valued at **\$800,000**. A ransomware attack is expected to cause **30% damage** to the asset each time it happens. The company estimates that the attack could occur **70% of the time annually** ( $ARO = 0.7$ ).

### Step 1: Calculate Single Loss Expectancy (SLE)

$$SLE = AssetValue \times ExposureFactor$$

$$SLE = 800,000 \times 0.3 = 240,000$$

This means that each ransomware attack is expected to cause a **\$240,000 loss**.


### Step 2: Calculate Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

$$ALE = 240,000 \times 0.7 = 168,000$$

Thus, the company expects an **annual financial loss of \$168,000** due to ransomware.

# 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). 'Threat' is at the top, with 'Likelihood' to its left and 'Impact' to its right. 'Risk' is below 'Threat', with 'Vulnerability' below it. Arrows point from 'Threat' to 'Risk' and from 'Impact' to 'Risk'.

Threat Likelihood	Impact		
	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 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)

= ?

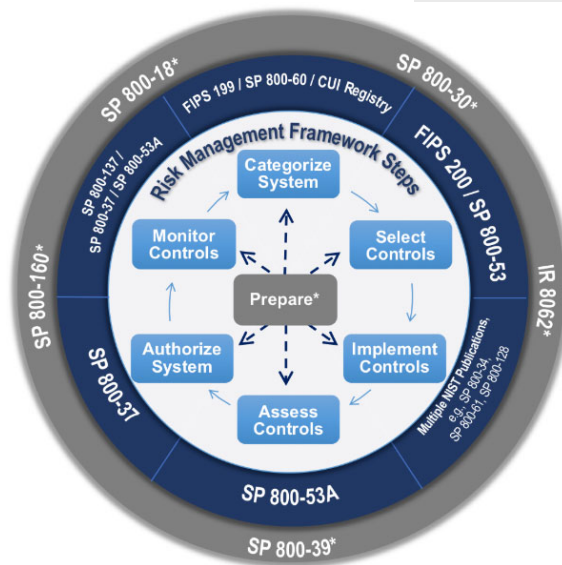
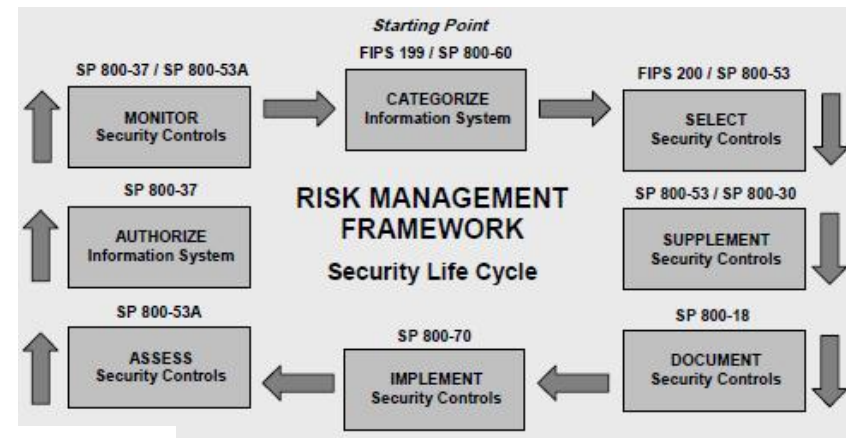
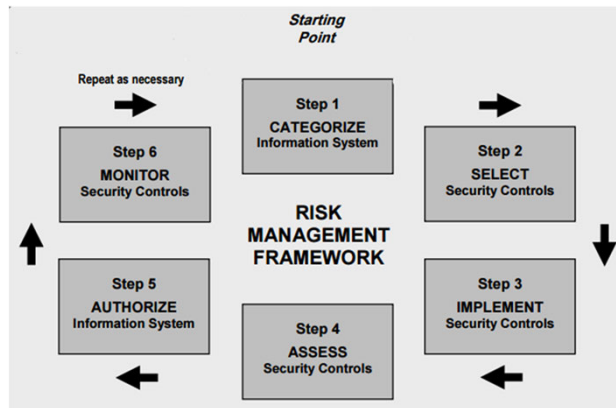
Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Traffic control	10	0.1	1
<b>Comm_Electric Geodatabase</b>	<b>High</b>		
			0
Water Distribution System	50	0.1	5
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1
<b>Water_Sewer Geodatabase</b>	<b>Moderate</b>	0.1	
			0
<b>Parcel Boundary Shapefile</b>	<b>10</b>	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
- ✓ Risk Management Framework
- ✓ Security Categorization
- ✓ Transforming qualitative risk assessment into quantitative risk assessment
- **System Security Plan – overview**
  - Security controls
  - Role of Security Categorization in selecting a security control baseline
  - A classification system for security control families

# Conceptual Views of NIST Risk Management Framework



# System Security Plan (SSP)



## SELECT Security Controls

Relevant Publications: FIPS 200 / SP 800-53

### •FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems)

- Defines **baseline security controls** based on the categorization of information systems.

### •SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)

- Provides a **catalog of security controls** for confidentiality, integrity, and availability (CIA Triad).
- Enables organizations to **select appropriate controls** based on system categorization.

## NIST CSF Alignment:

- ◆ **Protect Function** – Defines security controls to mitigate identified risks.

## The Federal Risk and Authorization Management Program (FedRAMP)

ensures that cloud service providers (CSPs) meet stringent cybersecurity requirements before being used by federal agencies.

A **System Security Plan (SSP)** documents the security controls and processes implemented by a cloud service provider (CSP) to protect federal data. FedRAMP SSPs are categorized based on the impact level of the system, which determines the security controls required.

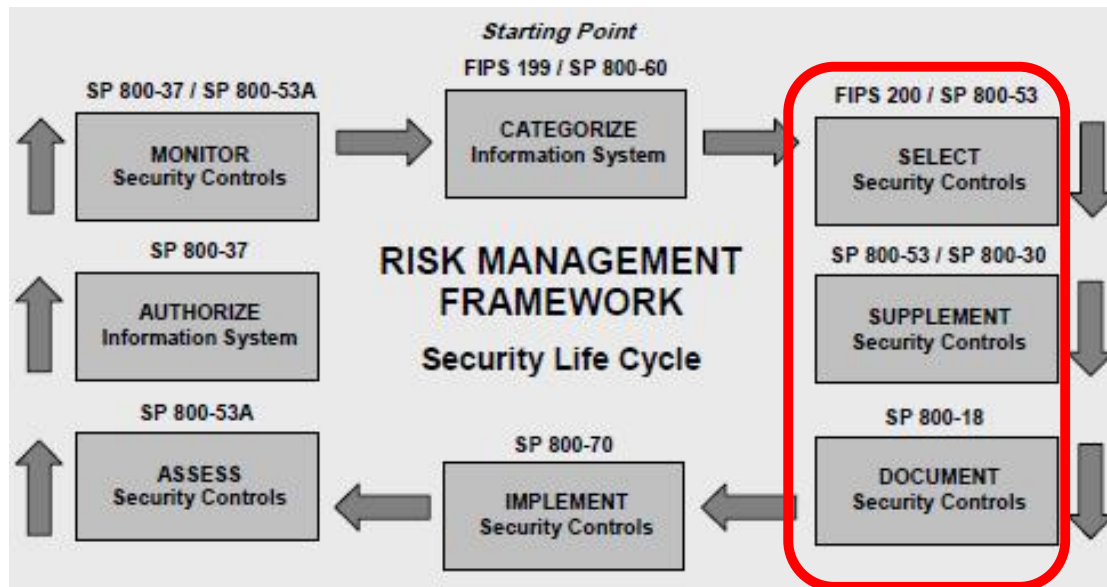
**TABLE OF CONTENTS**

1.	INFORMATION SYSTEM NAME/TITLE.....	1
2.	INFORMATION SYSTEM CATEGORIZATION .....	1
2.1.	Information Types .....	1
2.2.	Security Objectives Categorization (FIPS 199) .....	3
2.3.	Digital Identity Determination.....	3
3.	INFORMATION SYSTEM OWNER.....	4
4.	AUTHORIZING OFFICIALS .....	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.....	10
9.4.	Network Architecture.....	11
10.	SYSTEM ENVIRONMENT AND INVENTORY .....	12
10.1.	Data Flow.....	12
10.2.	Ports, Protocols and Services.....	14
11.	SYSTEM INTERCONNECTIONS .....	15
12.	LAWS, REGULATIONS, STANDARDS AND GUIDANCE.....	17
12.1.	Applicable Laws and Regulations.....	17
12.2.	Applicable Standards and Guidance .....	17
13.	MINIMUM SECURITY CONTROLS .....	18

Where to document information system categorization within a System Security Plan



# Information System Security Plan (SSP)



## 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
2.3.	Digital Identity Determination.....	3
3.	INFORMATION SYSTEM OWNER.....	4
4.	AUTHORIZING OFFICIALS .....	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.....	10
9.4.	Network Architecture.....	11
10.	SYSTEM ENVIRONMENT AND INVENTORY .....	12
10.1.	Data Flow.....	12
10.2.	Ports, Protocols and Services.....	14
11.	SYSTEM INTERCONNECTIONS .....	15
12.	LAWS, REGULATIONS, STANDARDS AND GUIDANCE.....	17
12.1.	Applicable Laws and Regulations.....	17
12.2.	Applicable Standards and Guidance .....	17
13.	MINIMUM SECURITY CONTROLS .....	18

## 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*

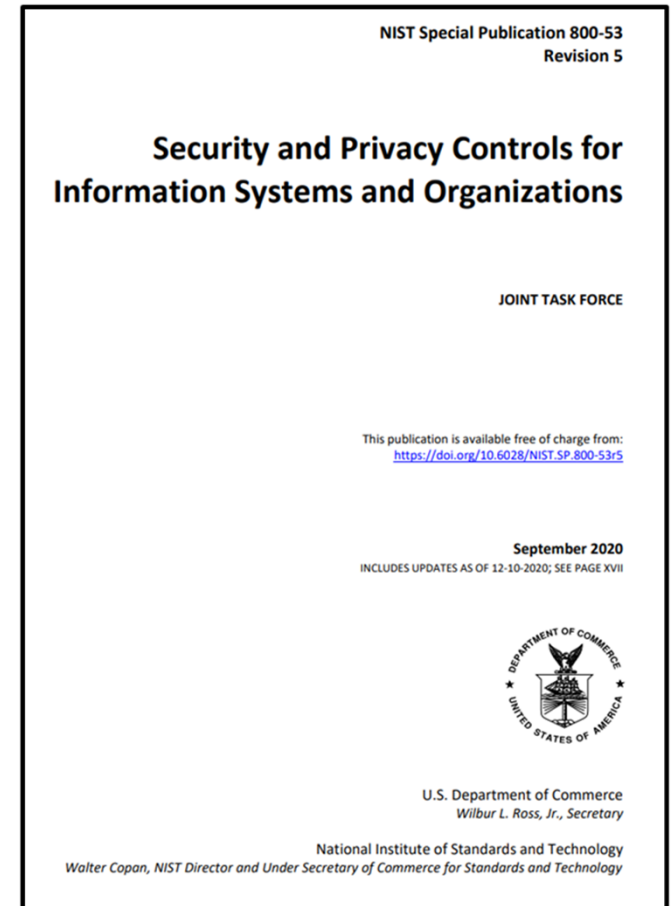
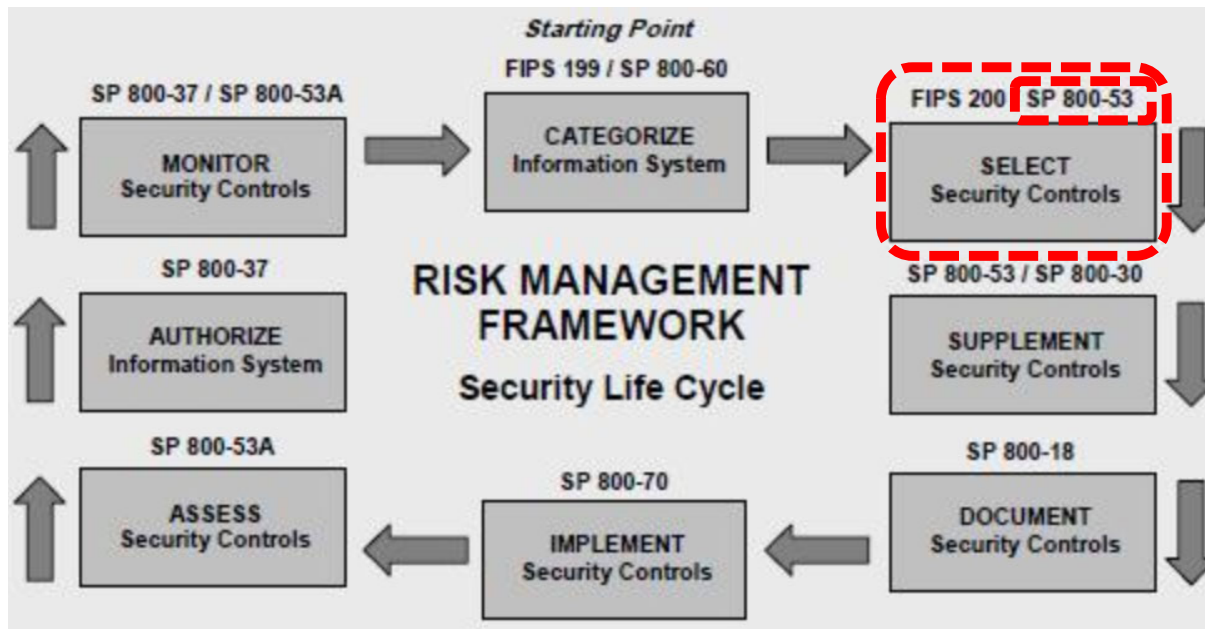
- |   |  |
|---|--|
| 1. Access Control (AC)  | 10. Media Protection (MP)                      |
| 2. Awareness and Training (AT)                                | 11. Physical and Environmental Protection *PE) |
| 3. Audit and Accountability (AU)                              | 12. Planning (PL)     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

FIPS 200 specifies **17 minimum security control families**, which are also referenced in **NIST SP 800-53**:

These controls must be implemented in alignment with **NIST Special Publication 800-53** and the **Risk Management Framework (RMF)**.



# NIST RMF



# Minimum Security Controls continue to evolve...

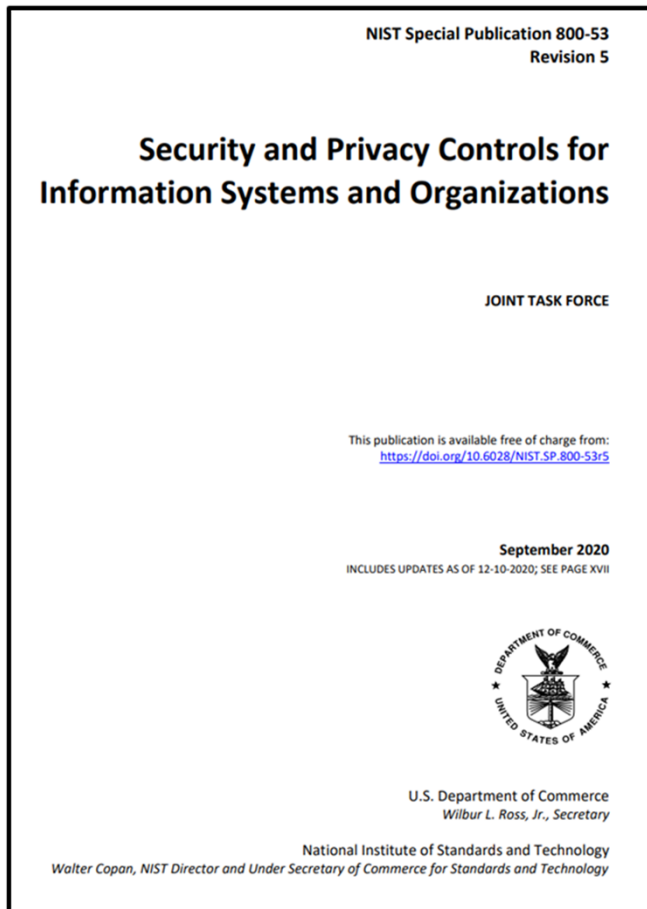


TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

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

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

*NIST 800-53 risk controls are typically presented alphabetically*

**TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES**

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

# NIST 800-53 Controls can be grouped by “Class”

NIST Special Publication 800-18  
Revision 1

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


Guide for Developing Security  
Plans for Federal Information  
Systems

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

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)

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

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeyports	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	Not Selected	Not Selected
Planning					
PL-1	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-2	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-3	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-4	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-5	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-6	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-7	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-8	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-9	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-10	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-11	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-12	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-13	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-14	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-15	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-16	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-17	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-18	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-19	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-20	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-21	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-22	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-23	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-24	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-25	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-26	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-27	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-28	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-29	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-30	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-31	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-32	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-33	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-34	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-35	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-36	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-37	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-38	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-39	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-40	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-41	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-42	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-43	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-44	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-45	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-46	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-47	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-48	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-49	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-50	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-51	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-52	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-53	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-54	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-55	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-56	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-57	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-58	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-59	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-60	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-61	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-62	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-63	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-64	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-65	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-66	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-67	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-68	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-69	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-70	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-71	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-72	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-73	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-74	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-75	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-76	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-77	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-78	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-79	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-80	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-81	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-82	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-83	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-84	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-85	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-86	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-87	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-88	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-89	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-90	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-91	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-92	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-93	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-94	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-95	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-96	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-97	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-98	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-99	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected
PL-100	Threat Intelligence	P0	Not Selected	Not Selected	Not Selected






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				

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 ?

# Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

*Provides a crosswalk among IS  
risk control frameworks*

Table 1: Function and Category Unique Identifiers

Function	Category Unique Identifier	Category
Identify	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
Protect	PR.AC	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
Detect	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
Respond	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
Recover	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications



Category	Subcategory	Informative References
<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	<b>ID.RA-1:</b> Asset vulnerabilities are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	<b>ID.RA-2:</b> Cyber threat intelligence is received from information sharing forums and sources	CIS CSC 4 COBIT 5 BAI08.01 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.6.1.4 NIST SP 800-53 Rev. 4 SI-5, PM-15, PM-16
	<b>ID.RA-3:</b> Threats, both internal and external, are identified and documented	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
	<b>ID.RA-4:</b> Potential business impacts and likelihoods are identified	CIS CSC 4 COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 ISO/IEC 27001:2013 A.16.1.6, Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-14, PM-9, PM-11
	<b>ID.RA-5:</b> Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CIS CSC 4 COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
	<b>ID.RA-6:</b> Risk responses are identified and prioritized	CIS CSC 4 COBIT 5 APO12.05, APO13.02 ISO/IEC 27001:2013 Clause 6.1.3 NIST SP 800-53 Rev. 4 PM-4, PM-9

CIS CSC – Center for Internet Security (CIS) Critical Security Controls (CSC)  
 COBIT 5 – ISACA’s Control Objectives for Information and Related Technologies  
 ISA – International Society of Automation  
 ISO/IEC – International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)  
 NIST – National Institute of Standards and Technology

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].

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA 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, 800-30, 800-100.

Priority and Baseline Allocation:

P1	LOW RA-1	MOD RA-1	HIGH RA-1	76
----	----------	----------	-----------	----

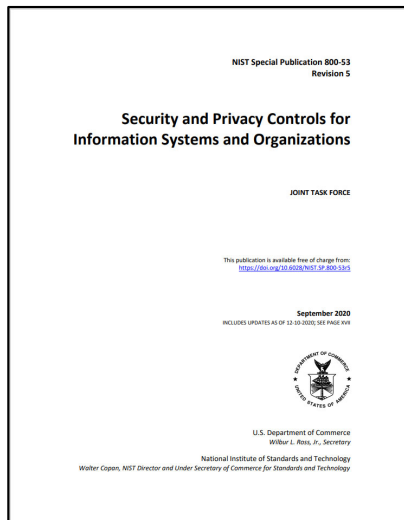


# SSP – Control Inventory Example

## RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

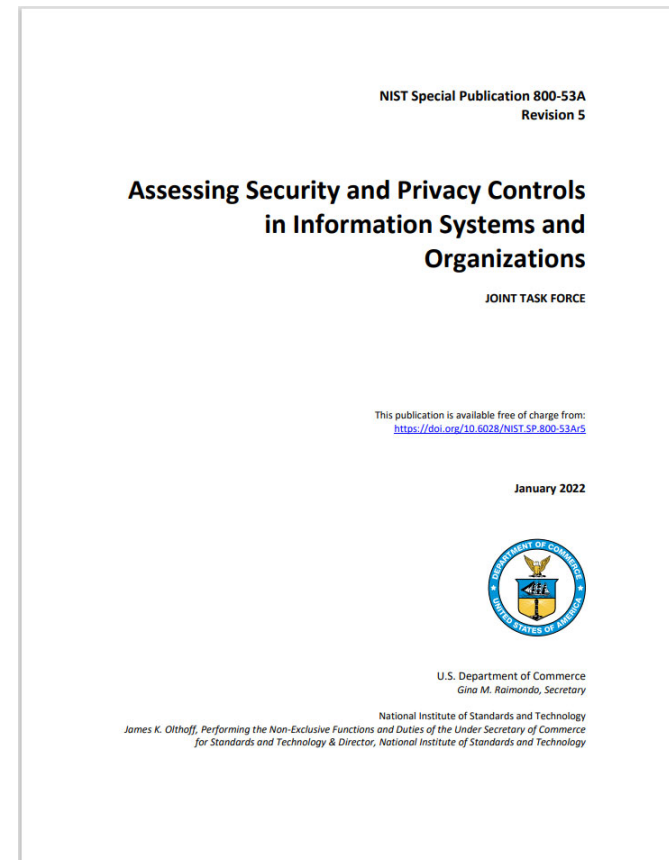
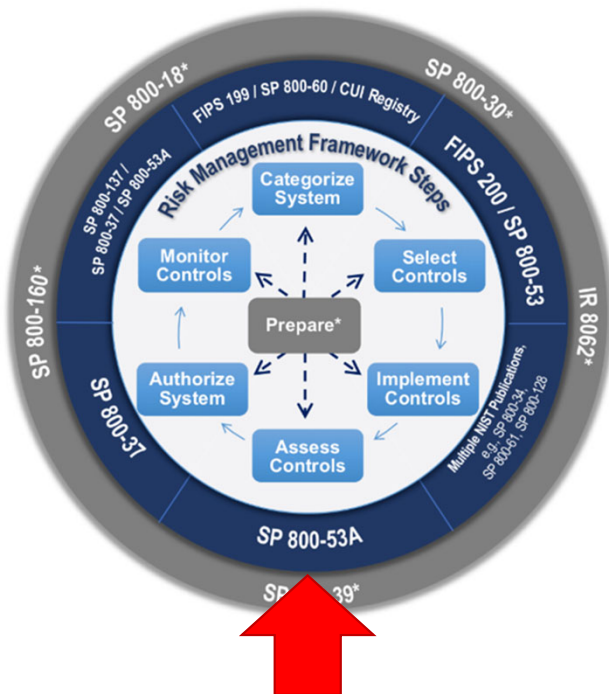
- a. Develops, documents, and disseminates to *[Assignment: organization-defined personnel or roles]*:
  1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  2. Procedures to facilitate 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]*.



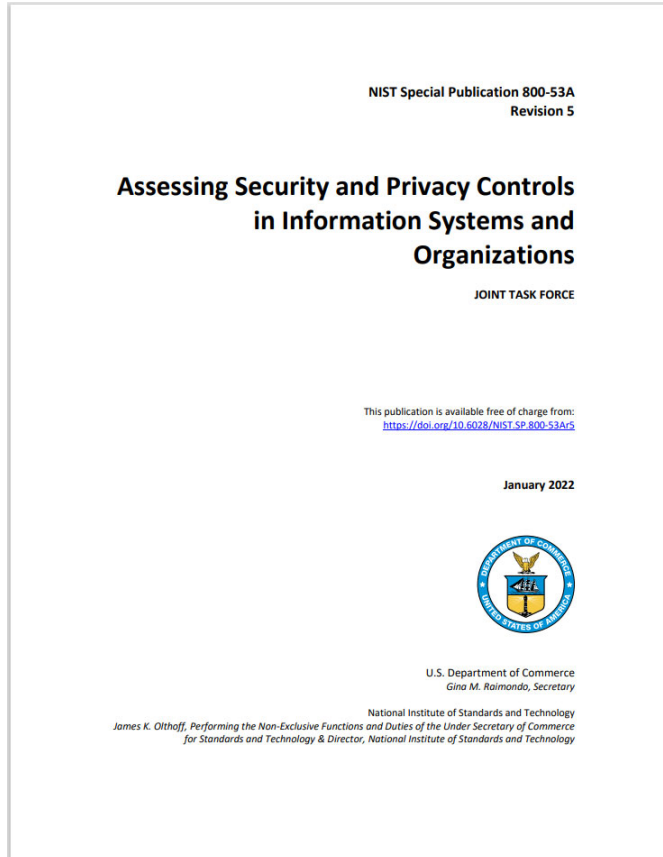
RA-I	Control Summary Information
	Responsible Role:
	Parameter RA-1(a):
	Parameter RA-1(b)(1):
	Parameter RA-1(b)(2):
	Implementation Status (check all that apply): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable
	Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific)

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

# How to assess an InfoSec Control ?



# Assessing InfoSec control



## FAMILY: RISK ASSESSMENT

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

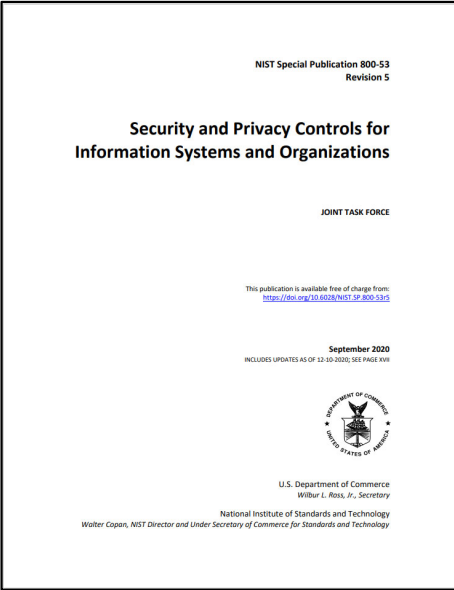
Supplemental Guidance: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are comprised through a loss of confidentiality, integrity, or availability. Organizations conduct the security categorization process as an organization-wide activity with the involvement of chief information officers, senior information security officers, information system owners, mission/business owners, and information owners/stewards. Organizations also consider the potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential 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	80
----	----------	----------	-----------	----



# SSP – Control Inventory Example (RA-2)

## RA-2 SECURITY CATEGORIZATION

Control: The organization:

- Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
- 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):	
<input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply):	
<input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization	

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

# NIST SP 800-53A provides guidance for assessing InfoSec controls...

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

- 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;
- Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- Reviews risk assessment results [Assignment: organization-defined frequency];
- Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
- 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): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable
	Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing FedRAMP Authorization for <a href="#">Click here to enter text.</a> , Date of Authorization
	<b>RA-3 What is the solution and how is it implemented?</b>
Part a	
Part b	
Part c	
Part d	
Part e	



# Assessing InfoSec control

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

## TABLE OF CONTENTS

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

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.	Digital Identity Determination.....	3
3.	INFORMATION SYSTEM OWNER.....	4
4.	AUTHORIZING OFFICIALS .....	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.....	10
9.4.	Network Architecture.....	11
10.	SYSTEM ENVIRONMENT AND INVENTORY .....	12
10.1.	Data Flow .....	12
10.2.	Ports, Protocols and Services.....	14
11.	SYSTEM INTERCONNECTIONS .....	15
12.	LAWS, REGULATIONS, STANDARDS AND GUIDANCE .....	17
12.1.	Applicable Laws and Regulations.....	17
12.2.	Applicable Standards and Guidance .....	17
13.	MINIMUM SECURITY CONTROLS .....	18

14.	ACRONYMS .....	392
15.	ATTACHMENTS.....	393
Attachment 1	Information Security Policies and Procedures.....	395
Attachment 2	User Guide .....	396
Attachment 3	Digital Identity Worksheet .....	397
	Introduction and Purpose .....	397
	Information System Name/Title .....	397
	Digital Identity Level Definitions .....	397
	Review Maximum Potential Impact Levels.....	398
	Digital Identity Level Selection .....	399
Attachment 4	PTA/PIA .....	400
	Privacy Overview and Point of Contact (POC) .....	400
	Applicable Laws and Regulations.....	400
	Applicable Standards and Guidance.....	401
	Personally Identifiable Information (PII).....	401
	Privacy Threshold Analysis .....	402
	Qualifying Questions .....	402
	Designation.....	402
Attachment 5	Rules of Behavior .....	403
Attachment 6	Information System Contingency Plan .....	404
Attachment 7	Configuration Management Plan .....	405
Attachment 8	Incident Response Plan .....	406
Attachment 9	CIS Workbook.....	407
Attachment 10	FIPS 199.....	408
	Introduction and Purpose .....	408
	Scope .....	408
	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 Contains & Documents the status of a system's Control Inventory

Control Summary Information
Responsible Role:
Implementation Status (check all that apply):
<input type="checkbox"/> Implemented
<input checked="" type="checkbox"/> Partially implemented
<input type="checkbox"/> Planned
<input type="checkbox"/> Alternative implementation
<input type="checkbox"/> 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