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:
http://securitycards.cs.washington.edu/cards.html

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

Team 1	Team 2	Team 3	Team 4
Dan Xu	Bernard Antwi	Victoria Zak	Vraj Patel
Zijian Ou	Kofi Bonsu	Madalyn Stiverson	Lauren Deinhardt
Kyuande Johnson	Patrick Jurgelewicz	Andrew Nguyen	Kelly Sharadin
John Lucas	Dhaval Patel	Antonio Cozza	Mike Jordan

University of Washington Security Cards

A security threat brainstorming activity

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

University of Washington Security Cards

A security threat brainstorming activity

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

STRIDE

Threat 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


```
Identify Assets  →  Describe Architecture  →  Decompose Application
                                                       ↓
Rate Threats  ←  Document Threats  ←  Identify Threats
```
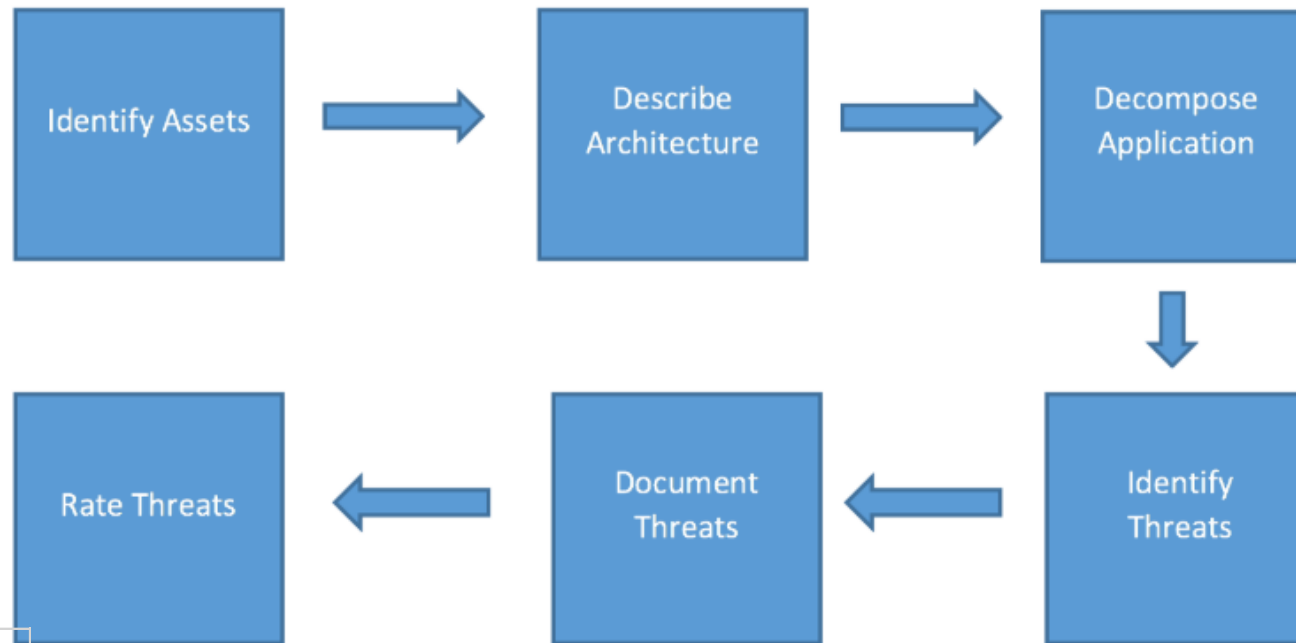
•Risk Value: 01 to 12 → Risk Level: **Notice**
•Risk Value: 13 to 18 → Risk Level: **Low**
•Risk Value: 19 to 36 → Risk Level: **Medium**
•Risk Value: 37 to 54 → Risk Level: **High**

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
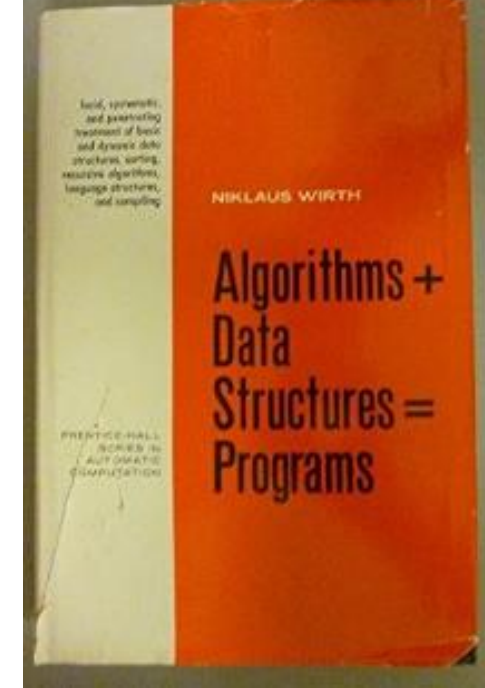
Information System Architecture

- 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*
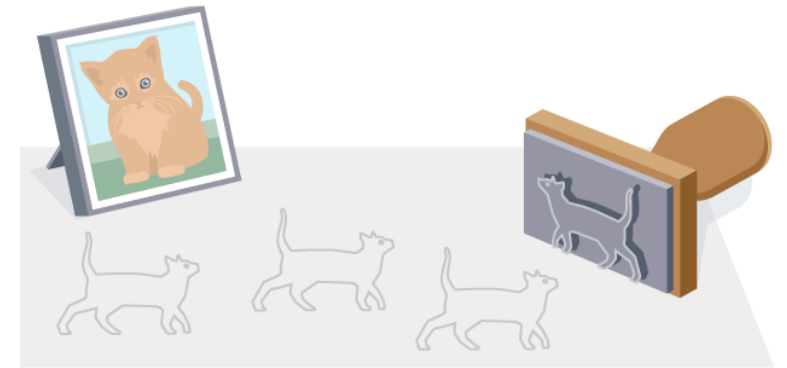
What is a conceptual model ?

- 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
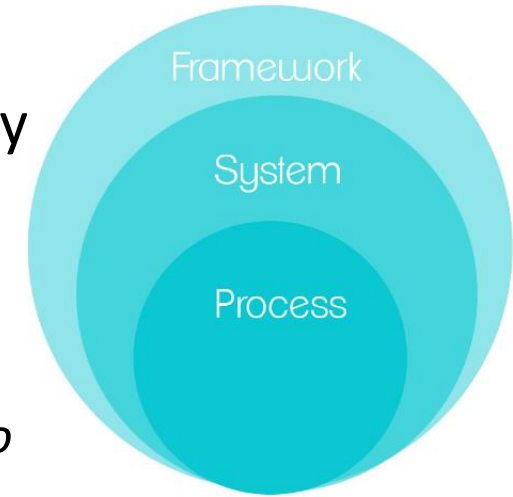
Models help us understand Information Systems… and how to defend them…

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
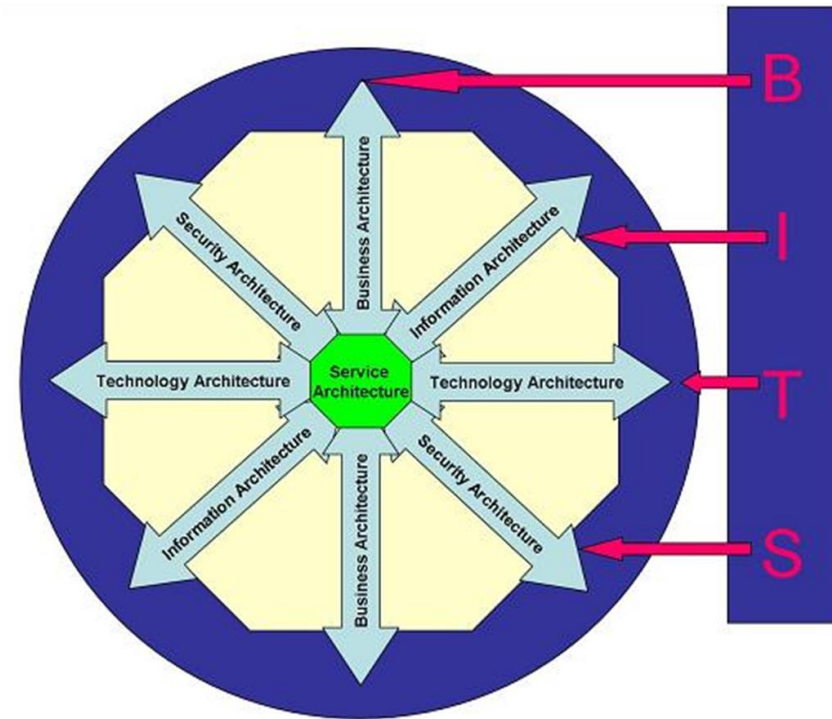- Aggregation
- Generalization

Abstractions help the designer understand, classify, and model reality

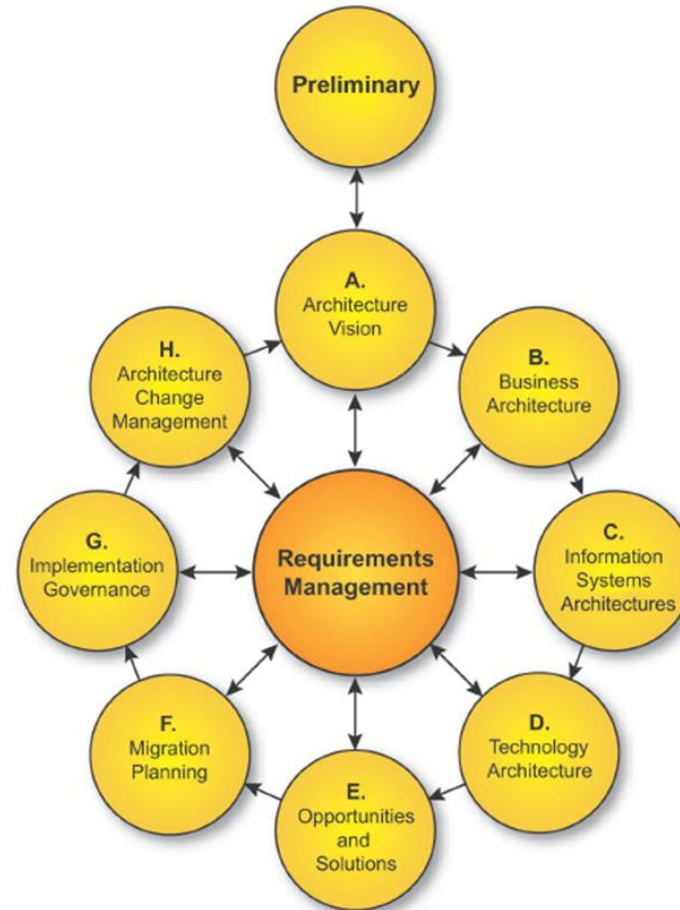# Conceptual models of information system design and development…

SDLC cycle:
- PLANNING
- ANALYSIS
- DESIGN
- DEVELOPMENT
- INTEGRATION & TESTING
- IMPLEMENTATION
- MAINTENANCE

Data requirements → Conceptual design → Conceptual schema → Logical design → Logical schema → Physical design → Physical schema

Database design
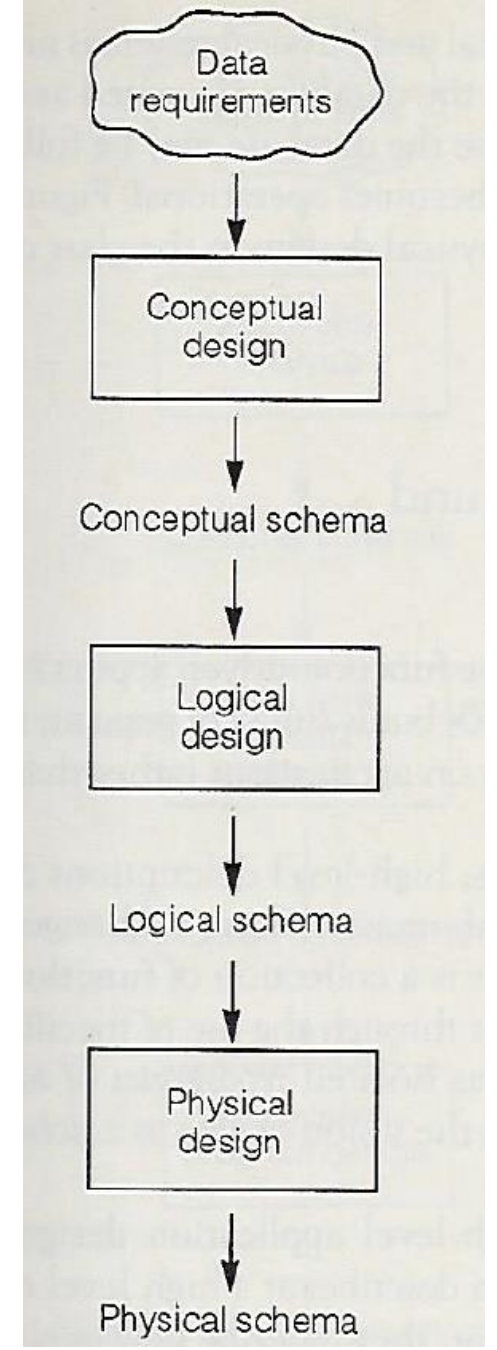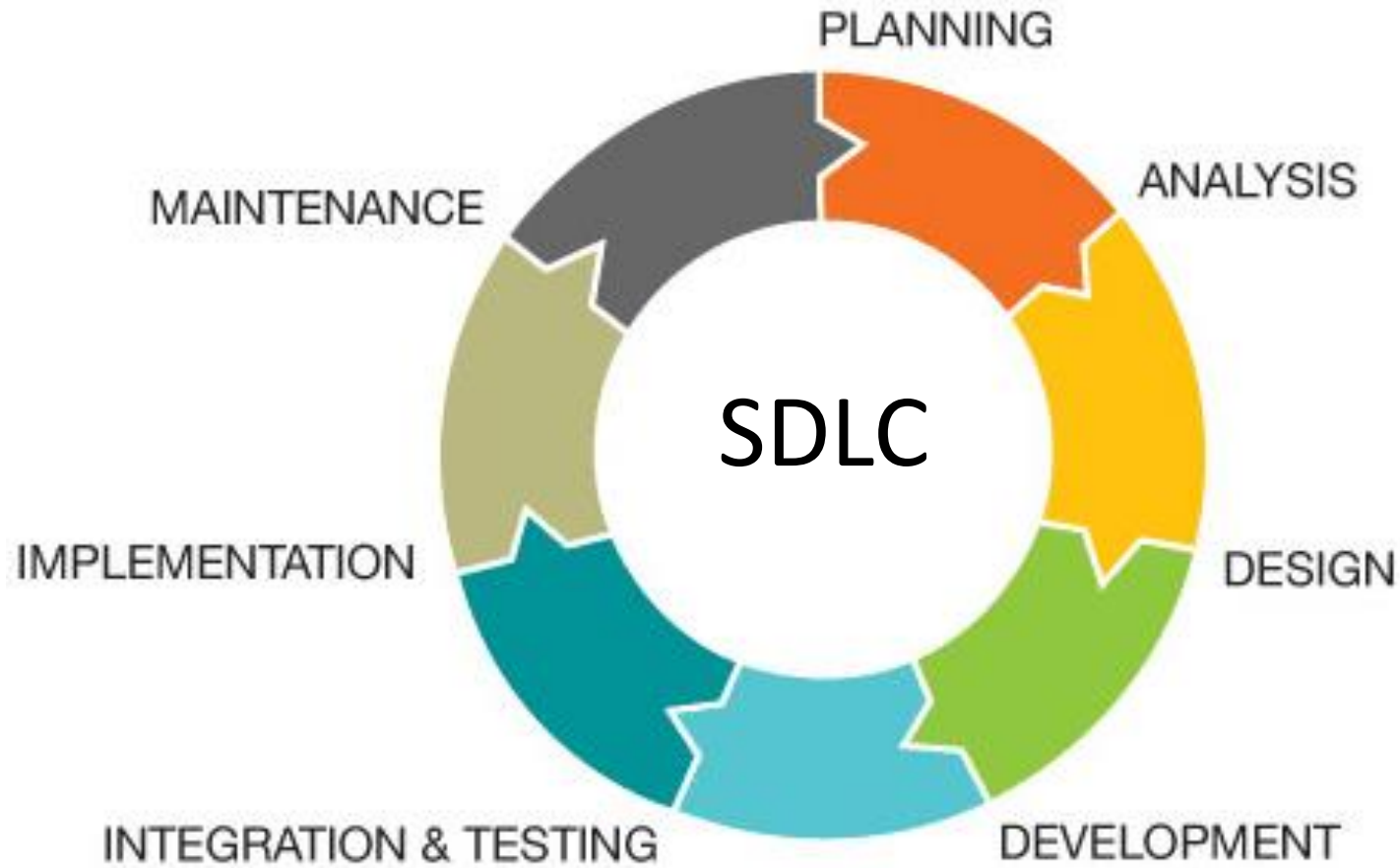
Models help us understand enterprise information systems and their security

Horatio Huxham's BITS

The Open Data Group Architecture Framework (TOGAF) Version 9.2

Sherwood Applied Business Security Architecture

Enterprise architecture consists of:

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

Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise_informatio
n_security_architecture
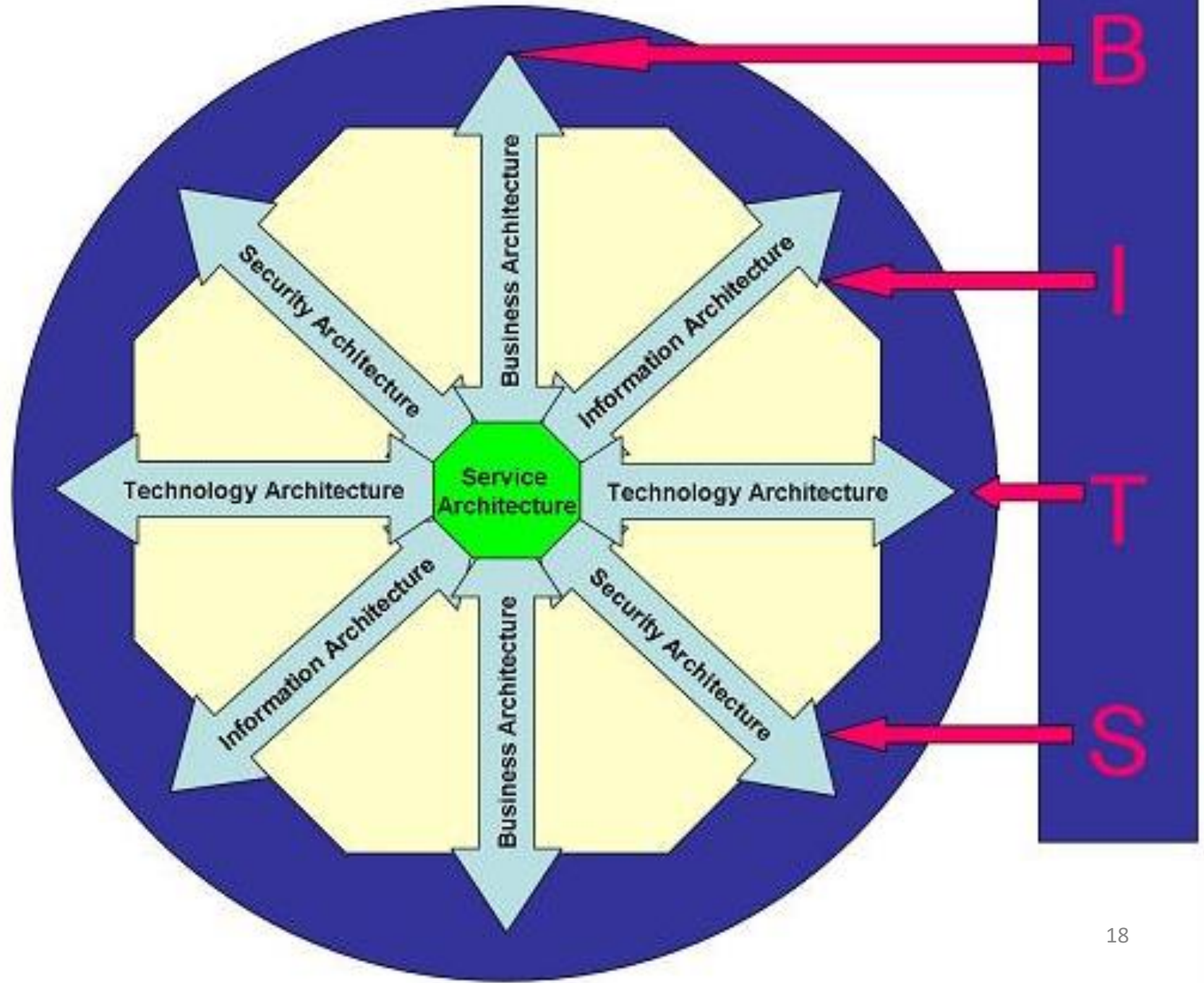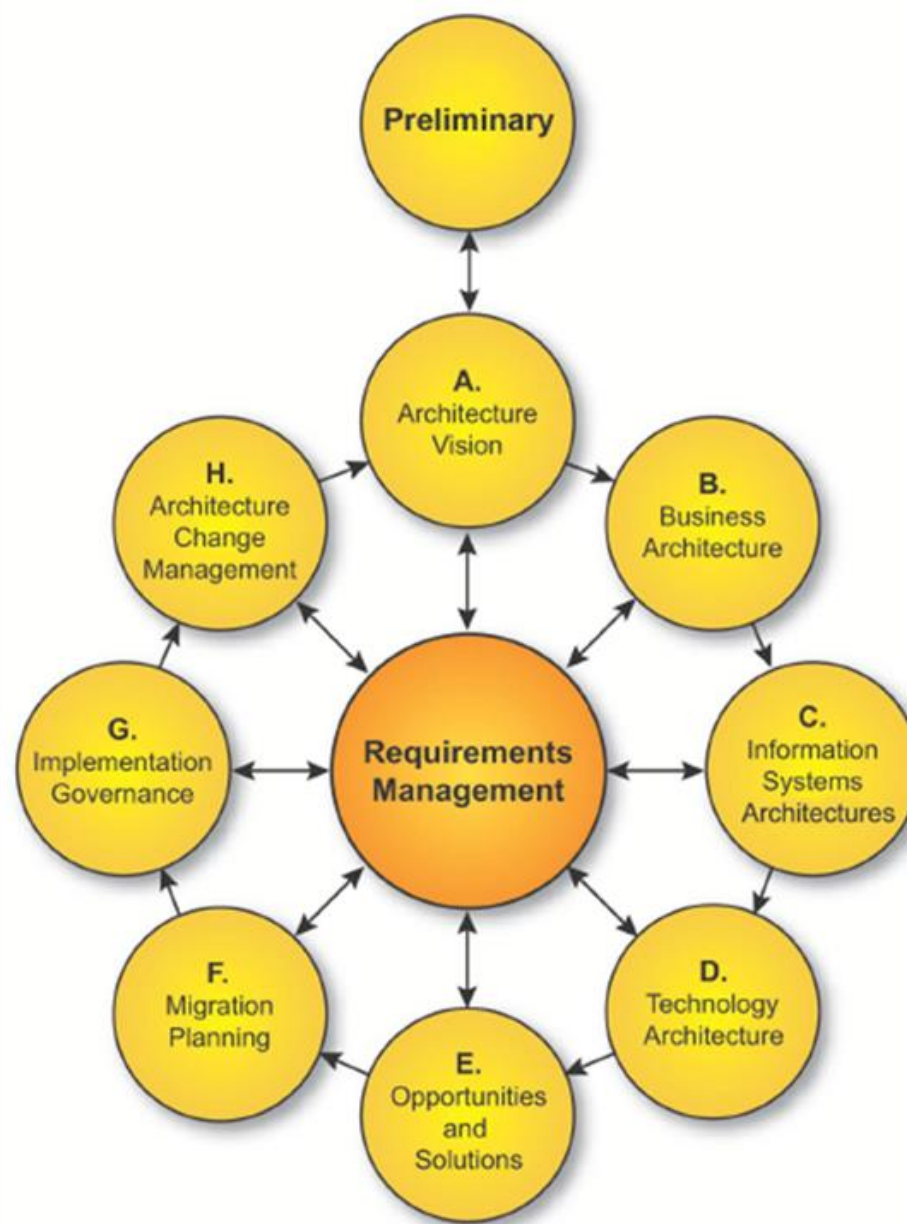
The Open Data Group Architecture Framework
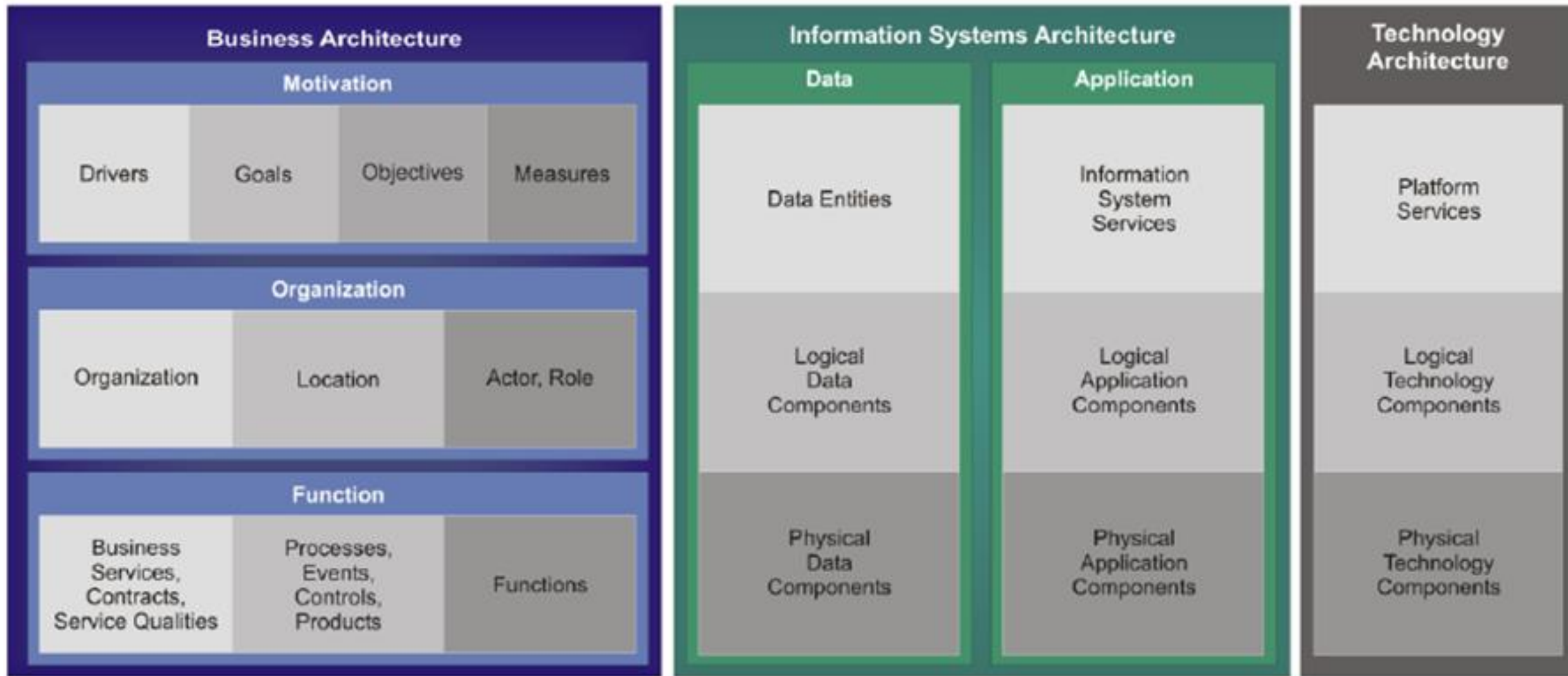(TOGAF) Version 9.1

Business Architecture

Board of Directors

President

Compliance and Governance | Investor Relations

Administrative and Finance Director	Executive and Operational Director	Institutional Relations and Sustainability Director	Legal Director and Comptroller	New Business Development Director
Accounting	Project Management	Environment	Contracts	Commercial
Administration	Information Technology	Social Responsibility	Comptroller	International Affairs
Human Resources	Marketing and Communications	Quality Assurance		

Information Architecture

Data Architecture

Application Architecture

TOGAF Content Metamodel

Architecture Principles, Vision, and Requirements				
Preliminary	**Architecture Vision**			
Architecture Principles	Business Strategy	Technology Strategy	Business Principles, Objectives, and Drivers	Architecture Vision	Stakeholders

Architecture Requirements			
Requirements	Constraints	Assumptions	Gaps

Business Architecture			Information Systems Architecture		Technology Architecture
Motivation			**Data**	**Application**	
Drivers	Goals	Objectives / Measures	Data Entities	Information System Services	Platform Services
Organization			Logical Data Components	Logical Application Components	Logical Technology Components
Organization	Location	Actor, Role			
Function			Physical Data Components	Physical Application Components	Physical Technology Components
Business Services, Contracts, Service Qualities	Processes, Events, Controls, Products	Functions			

Architecture Realization	
Opportunities, Solutions, and Migration Planning	**Implementation Governance**
Capabilities / Work Packages / Architecture Contracts	Standards / Guidelines / Specifications

Information Architecture

Conceptual models of Information Systems
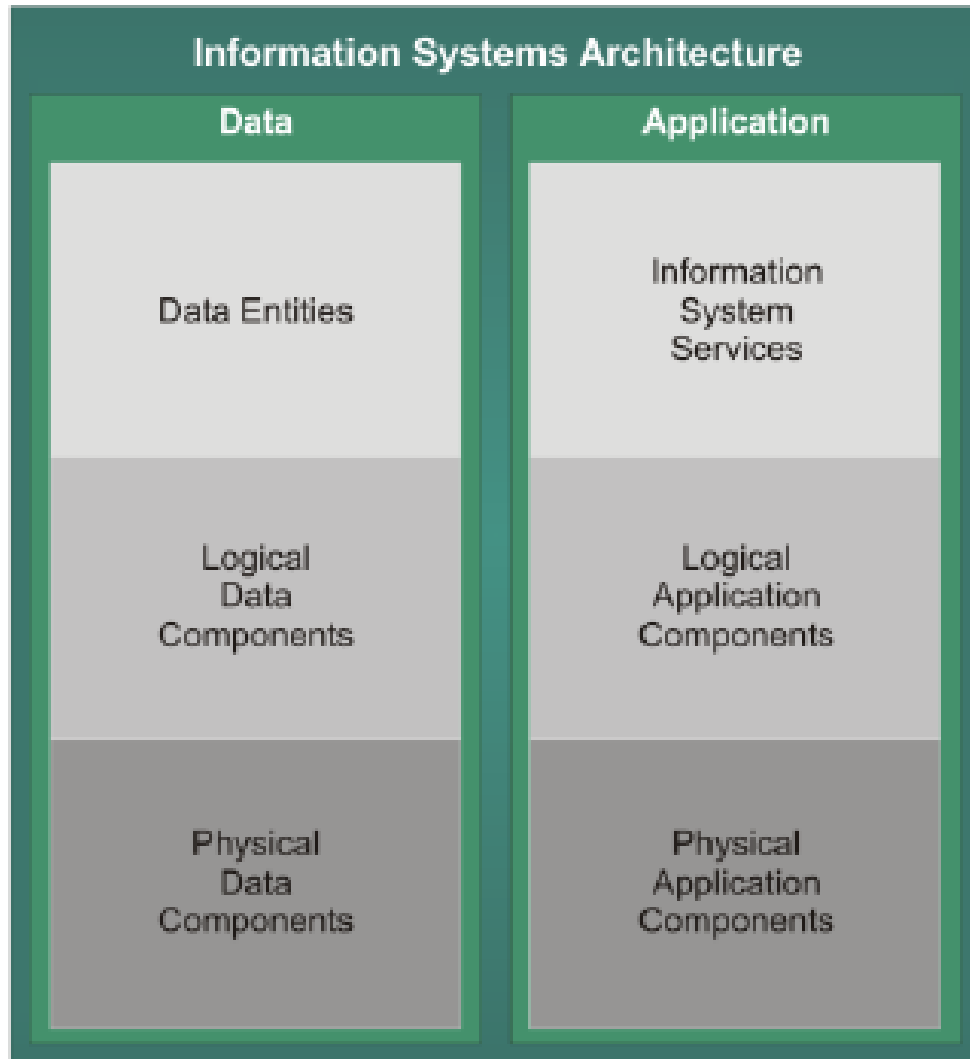
Content &
Structure

Function &
Use
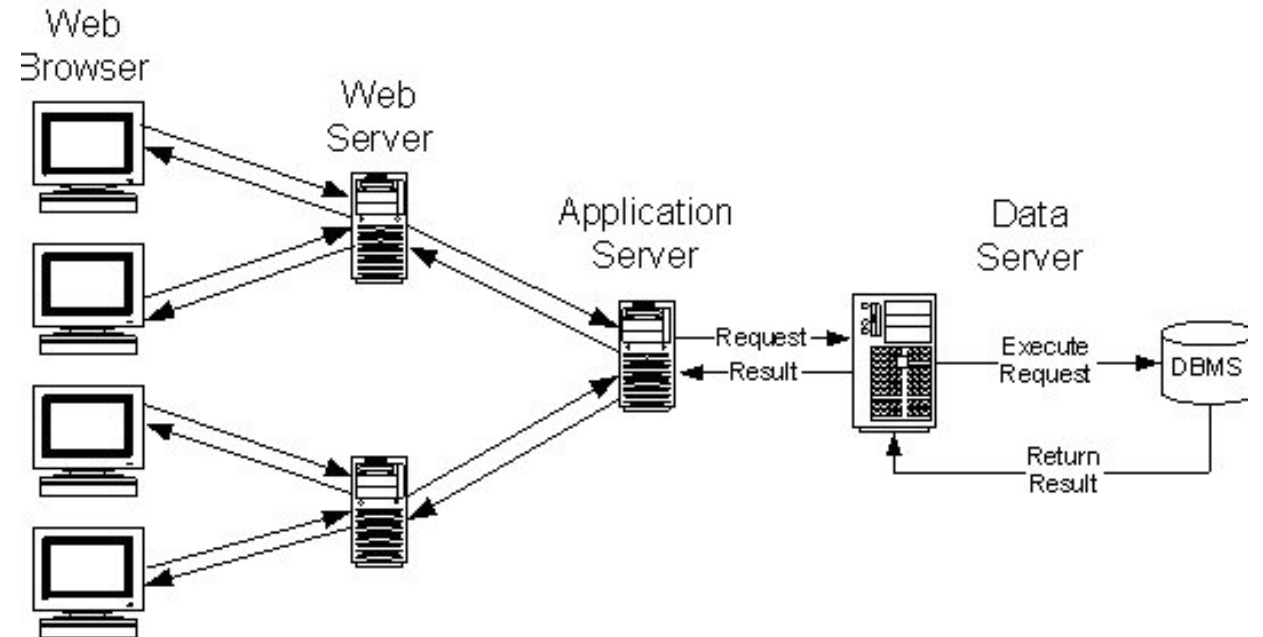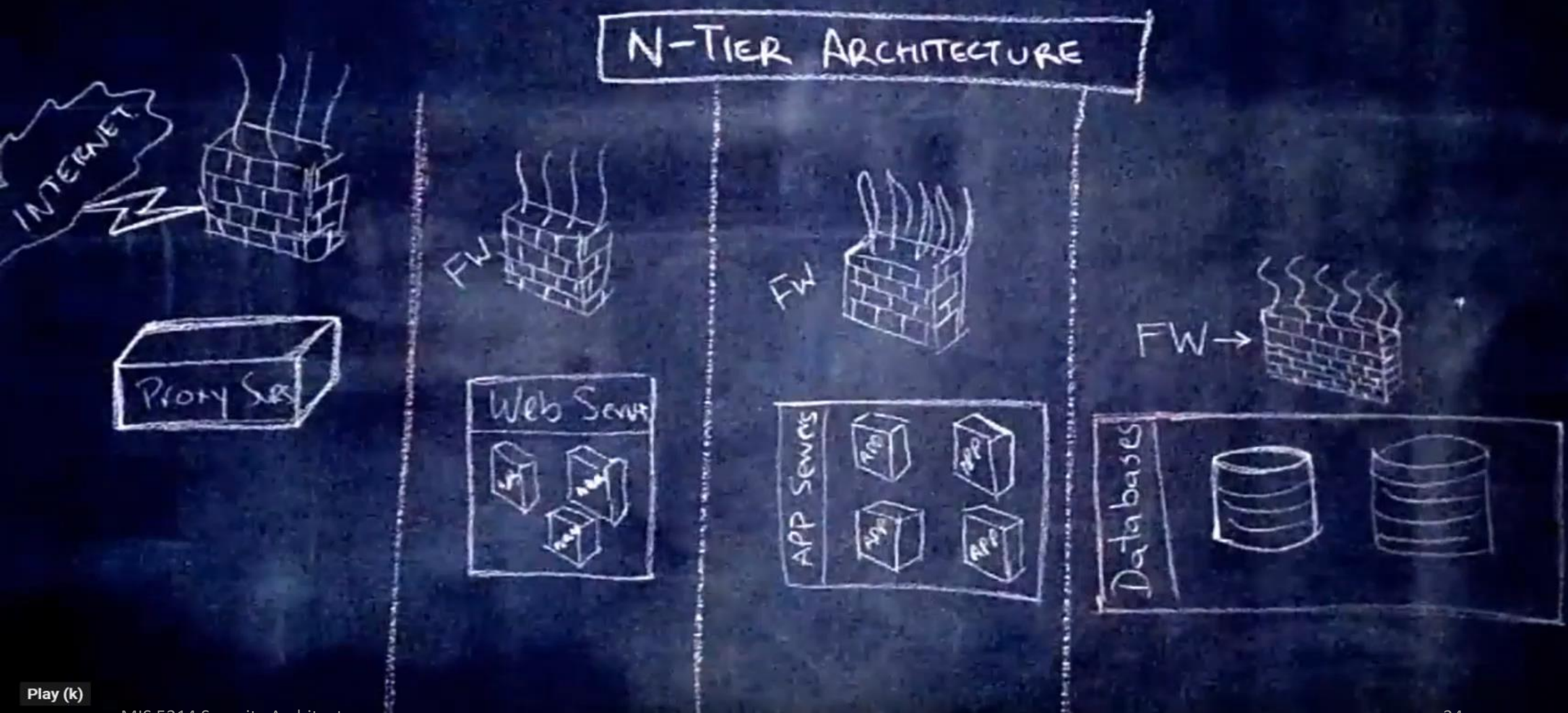
In-Class Exercise: Draw an N-Tier Architecture for a Web-Based System

- Consider the purpose and contents of a web-based system for managing the data of public utilities for a small town

- Identify who the users are

- Using what you learned in the video, draw an N-Tier Architecture for the web-based system
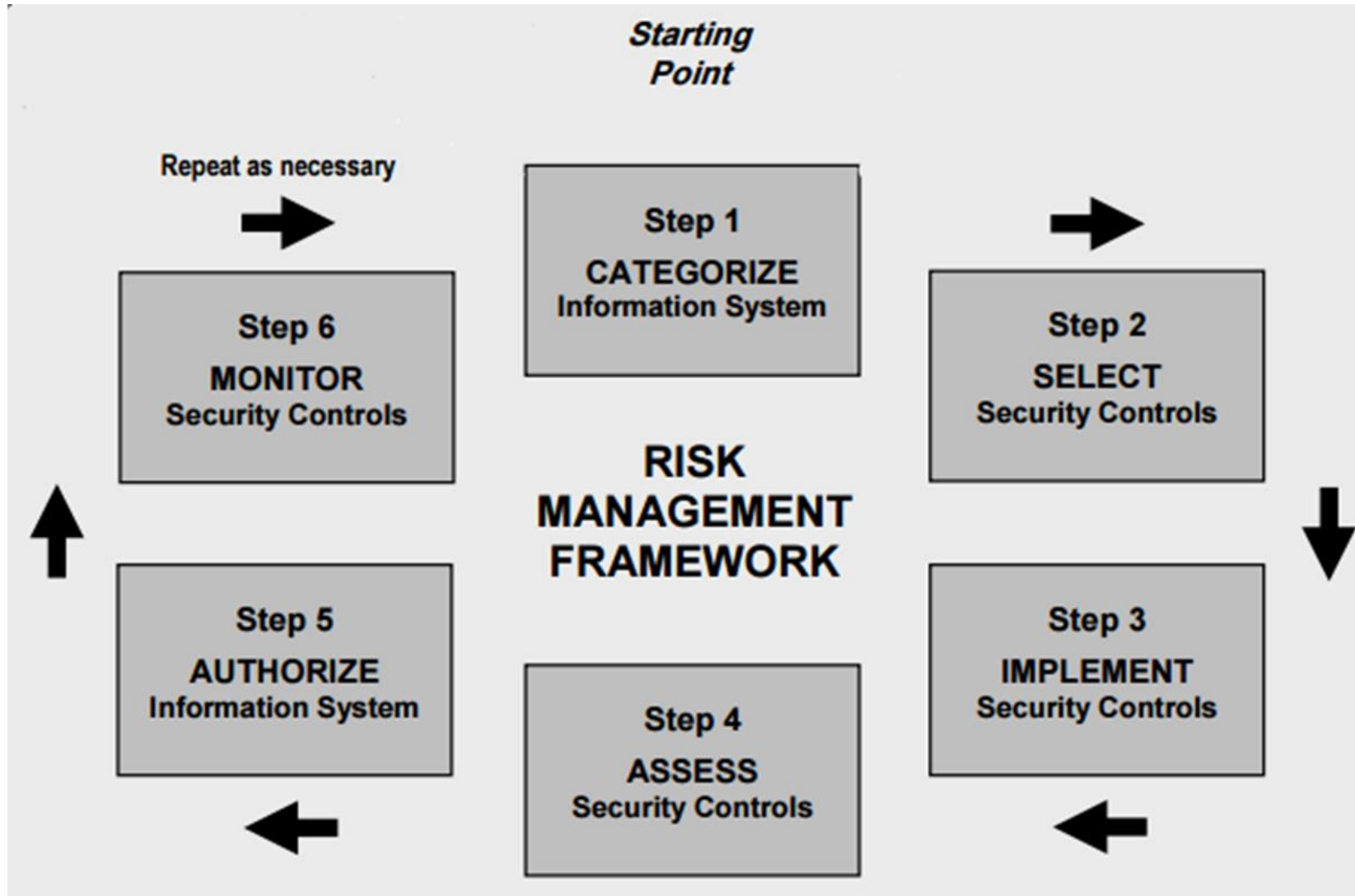
    https://app.diagrams.net/

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

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

TIER 1
ORGANIZATION
(Governance)

TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)

TIER 3
INFORMATION SYSTEM
(Environment of Operation)

STRATEGIC RISK

TACTICAL RISK

NIST Risk Management Framework

NIST Risk Management Framework
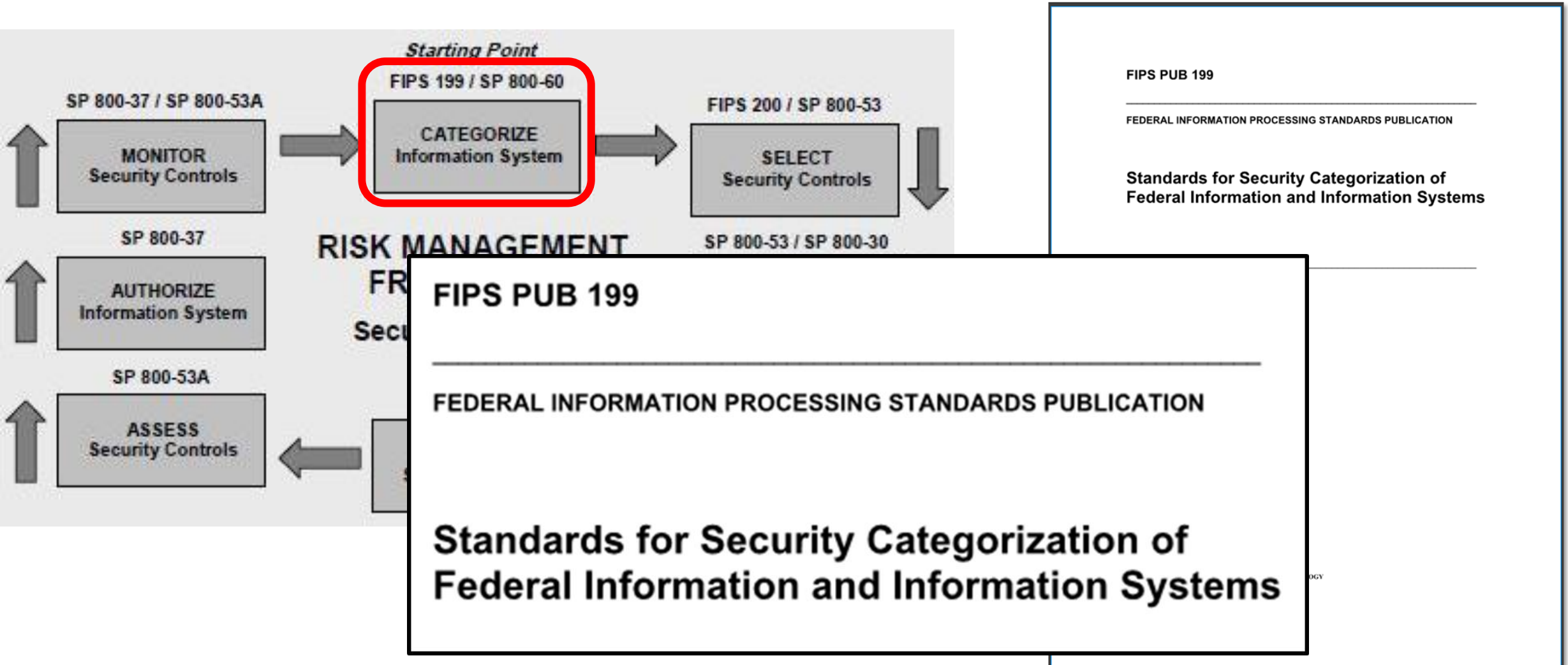
FIPS 199: <u>Qualitative risk assessment</u> based on security objectives

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

Security Objective	POTENTIAL IMPACT		
	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.

What are the security categorizations of these datasets?

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

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect
Medium: Serious adverse effect
High: Severe or catastrophic adverse effect

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

SC information system = {(**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 is the overall impact ratings of the datasets?

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

What is the overall Information System impact rating?

System - Critical Infrastructure Information

Dataset	Confidentiality	Integrity	Availability	Impact Rating
Communication	High	Moderate	Moderate	High
Electric	Moderate	Moderate	Moderate	Moderate
Traffic control	Low	Low	Low	Low
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?

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:
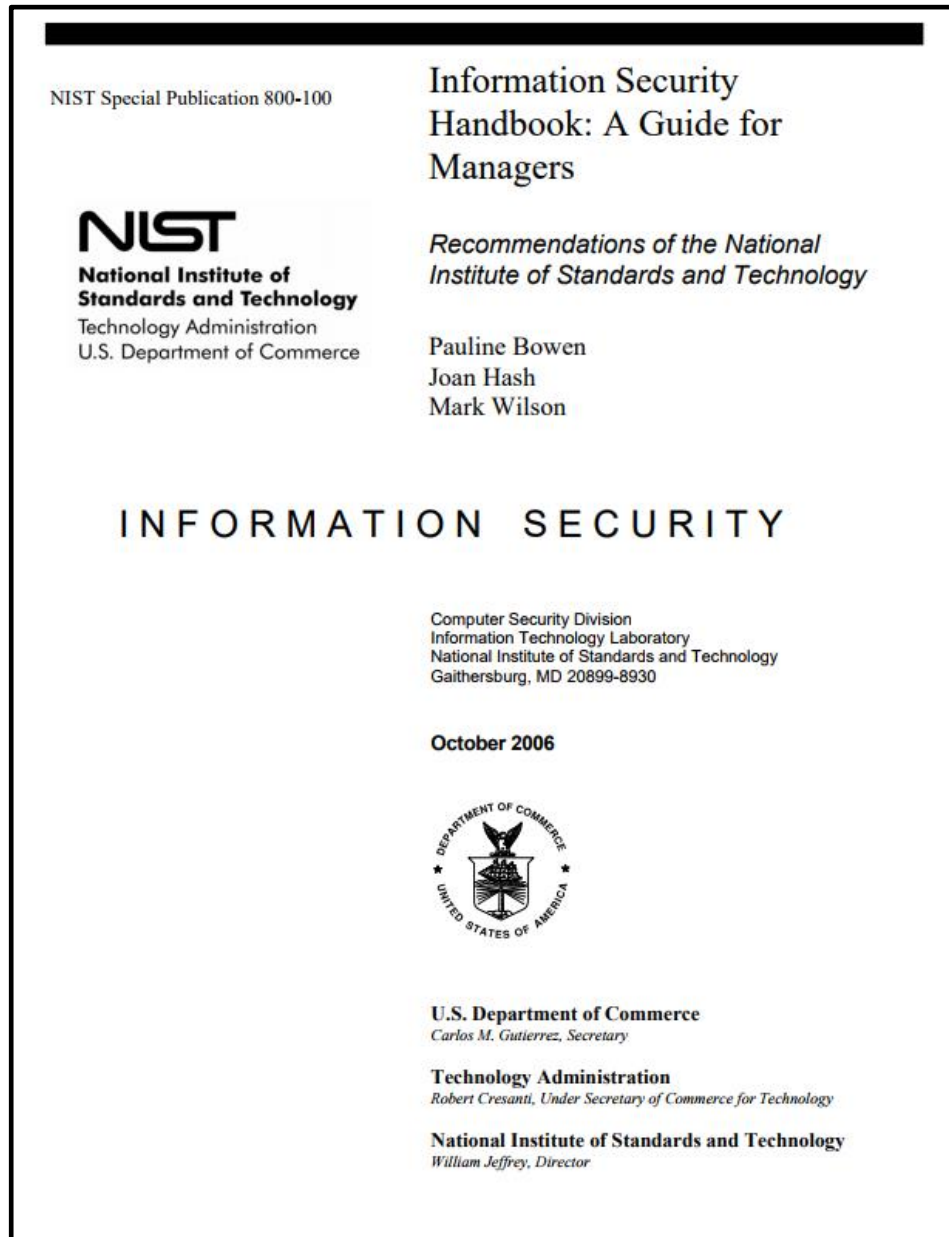
NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

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

	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

Transformation of ordinal qualitative risk categories to interval quantitative risk measures

Threat Likelihood	Impact		
	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

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

NIST SP 800-100 "Information Security Handbook: A Guide for Managers", page 99

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

+

Threat Likelihood	Impact		
	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

How do we use security categorization to select security controls?
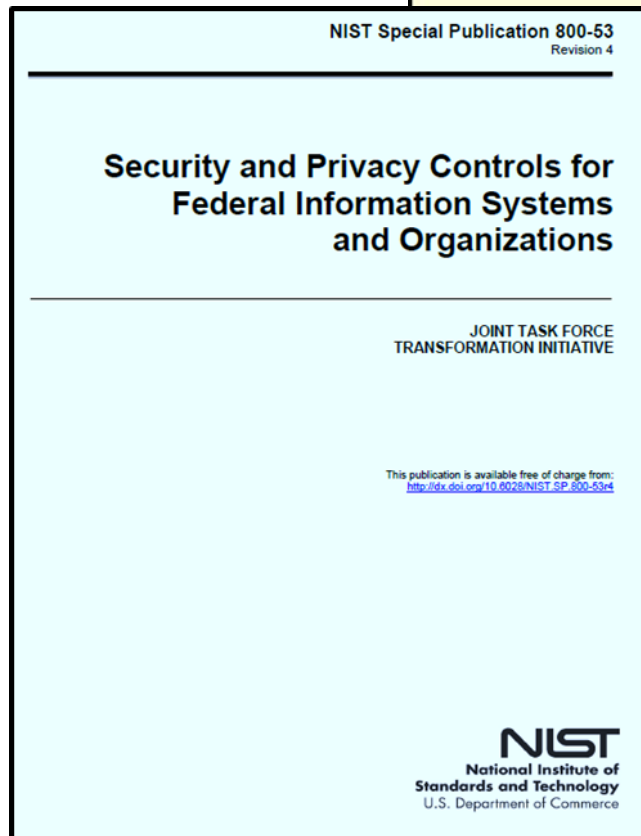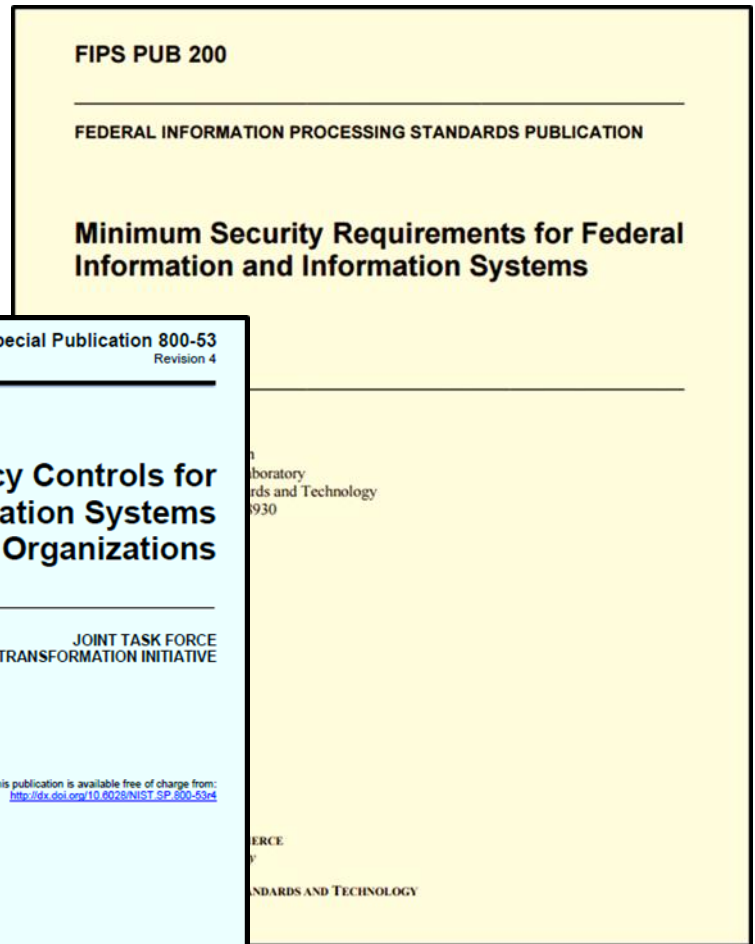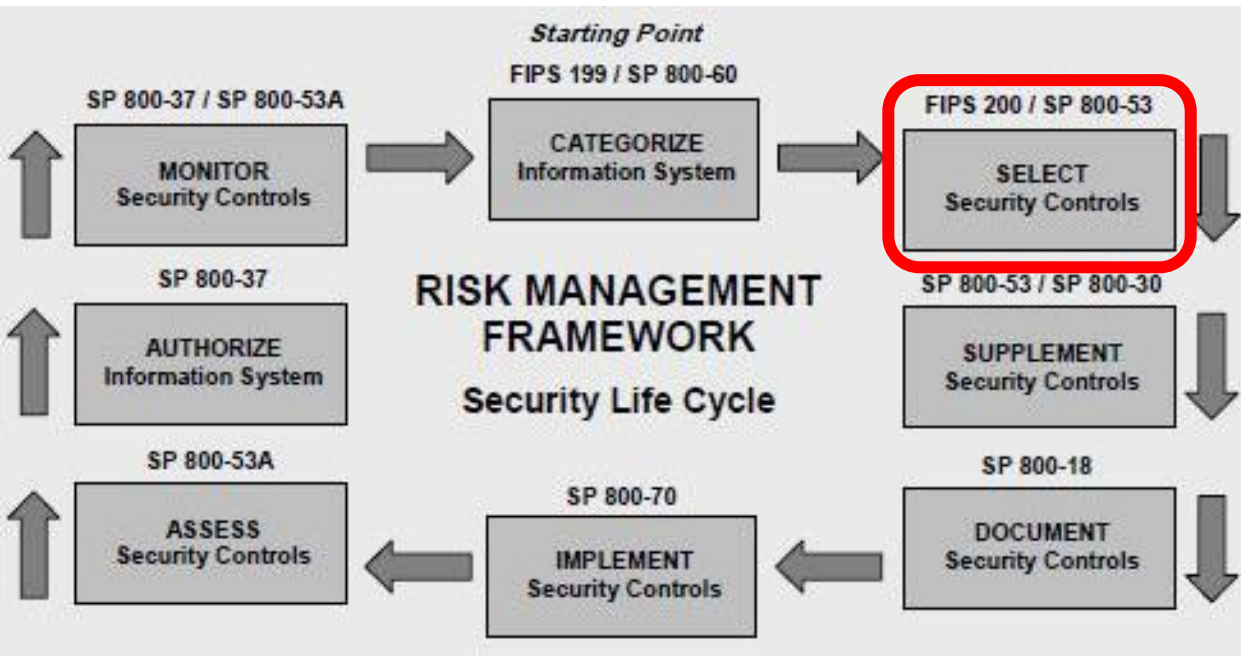
Agenda

✓Information Systems – some definitions

✓Conceptual models of information systems

✓NIST Risk Management Framework

✓FIPS 199 Security Categorization

✓Transforming qualitative risk assessment into quantitative risk assessment

- FedRAMP System Security Plan – overview
  - NIST 800-53 Security controls
  - Role of FIPS 199 in selecting a security control baseline
  - NIST 800-18 classification system for security control families

System Security Plan (SSP)

FedRAMP = Federal Risk and Authorization Management Program

FEDRAMP SECURITY LOW TEMPLATE

Cloud Se...
Inform...

FEDRAMP SECURITY PLAN MODERATE TEMPLATE

Cloud Service Pro...
Information Syst...
Version...
Version D...

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Cloud Service Provider Name
Information System Name
Version #
Version Date

FedRAMP

FedRAMP

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

[Unit 02 – System Security Plan (temple.edu)](temple.edu)

Information System Security Plan (SSP)

TABLE OF CONTENTS

FEDRAMP SYSTEM
SECURITY PLAN (SSP)
HIGH BASELINE
TEMPLATE

Cloud Service Provider Name

Information System Name

Version #

Version Date

FR

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

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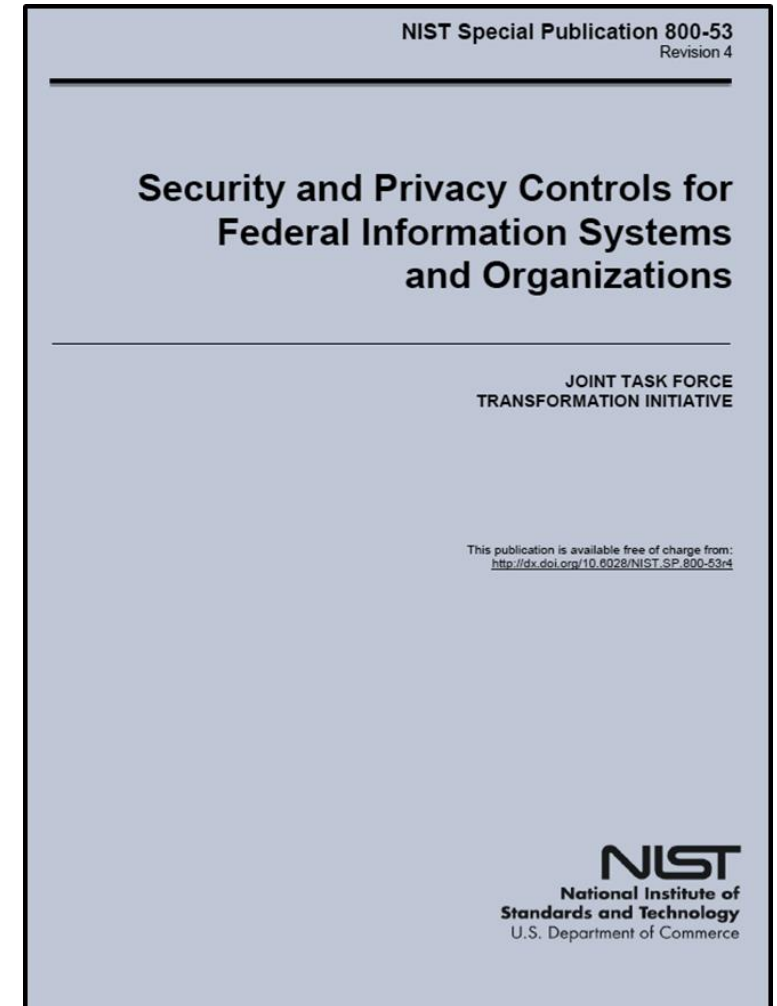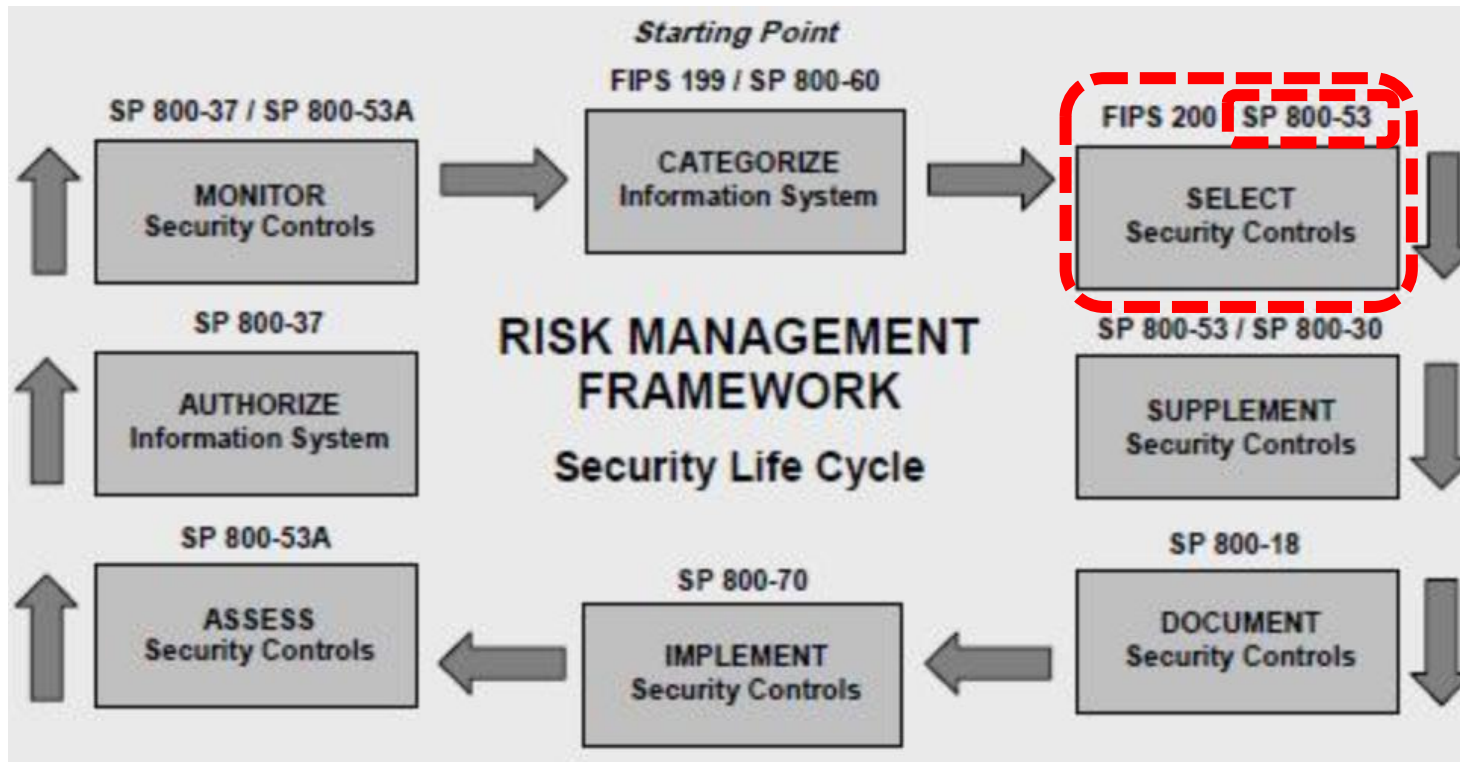
How do we use FIPS 199 security categorization to select security controls?

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)

50

TABLE D-2: SECURITY CONTROL BASELINES[92]

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

51

NIST 800-53 Controls are presented alphabetically

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessment (CA)
5. Configuration Management (CM)
6. Contingency Planning
7. Identification and Authentication
8. Incident Response (IR)
9. Maintenance (MA)

10. Media Protection (MP)
11. Physical and Environmental Protection *PE)
12. Planning (PL)
13. Personal Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition(SA)
16. System and Communications Protection (SC)
17. System and Information Integrity (SI)

NIST 800-53 Controls are grouped by "Class"

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

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

Marianne Swanson
Joan Hash
Pauline Bowen

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

53

Risk Assessment (RA) Controls

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

RA-1

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*].

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	

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.

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 | 57 |

SSP – Control Inventory Example

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	

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*]];

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	

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

•QUESTIONS???