# 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

# <u>Automotive Security</u> 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 <a href="http://securitycards.cs.washington.edu/cards.html">http://securitycards.cs.washington.edu/cards.html</a>

### 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 <u>blue suit of cards ("Human Impact"</u>), 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 <u>red "Adversary's Resources" suit</u>
- 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.** <u>Information disclosure</u> Can an attacker gain access to private or potentially injurious data?
- 5. <u>Denial of service</u> 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

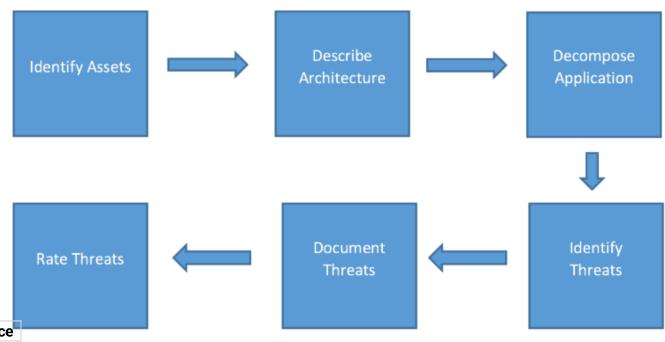
### A security threat brainstorming activity

- 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



Risk Value: 01 to 12 → Risk Level: Notice

•Risk Value: 13 to 18 → Risk Level: **Low** 

•Risk Value: 19 to 36 → Risk Level: **Mediun** 

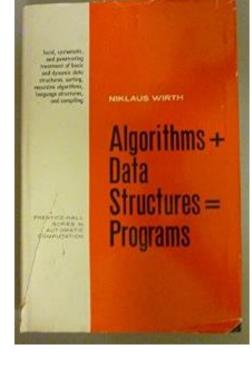
•Risk Value: 37 to 54 → Risk Level: **High** 

# 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



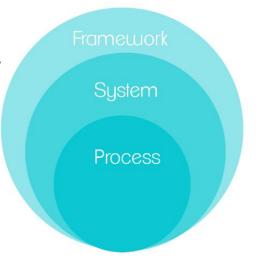
13

- 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?

Conceptual Mode

- 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

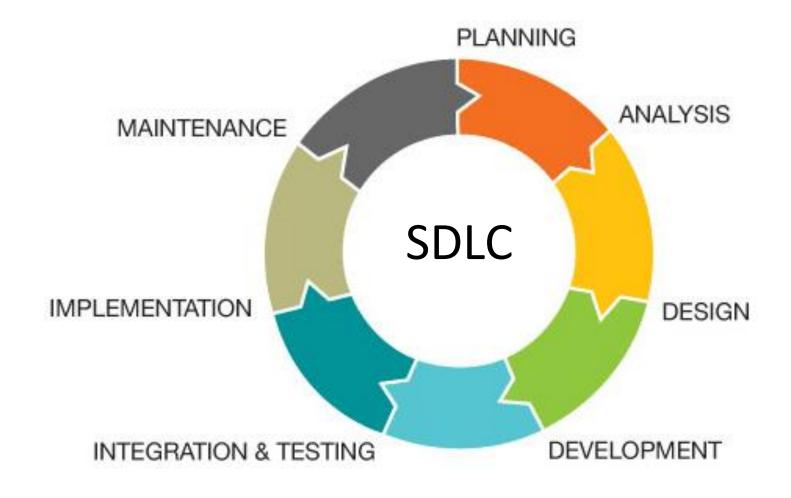
**Model quality** depends on skill of model designers and qualities of the selected model

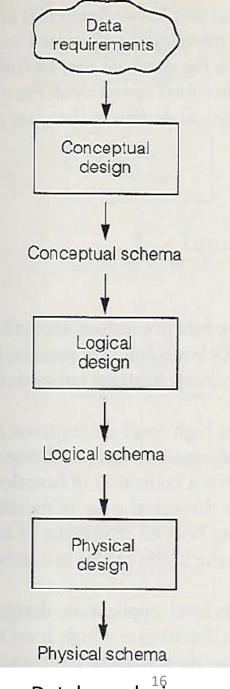
Building blocks of models is a small collection of abstraction mechanisms

- Classification
- Aggregation
- Generalization

Abstractions help the designer understand, classify, and model reality

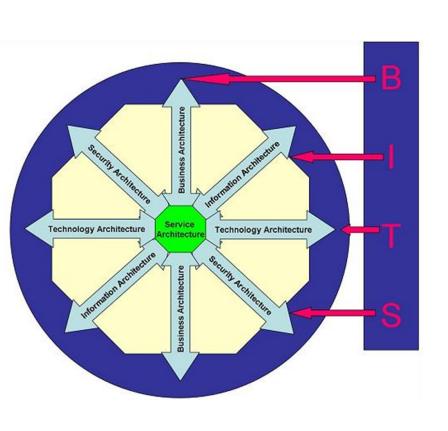
# Conceptual models of information system design and development...





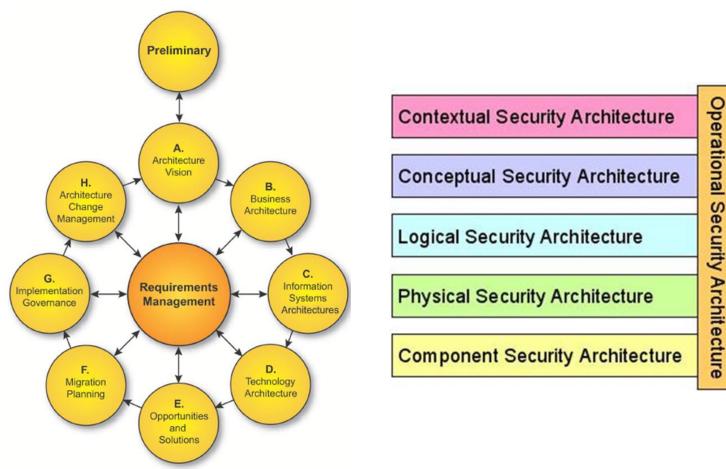
Database design

# Models help us understand enterprise information systems and their security



Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise informatio MIS 5236cSpievriavchreectore



The Open Data Group Architecture Framework (TOGAF) Version 9.2

Sherwood Applied Business Security **Architecture** 

ഗ

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

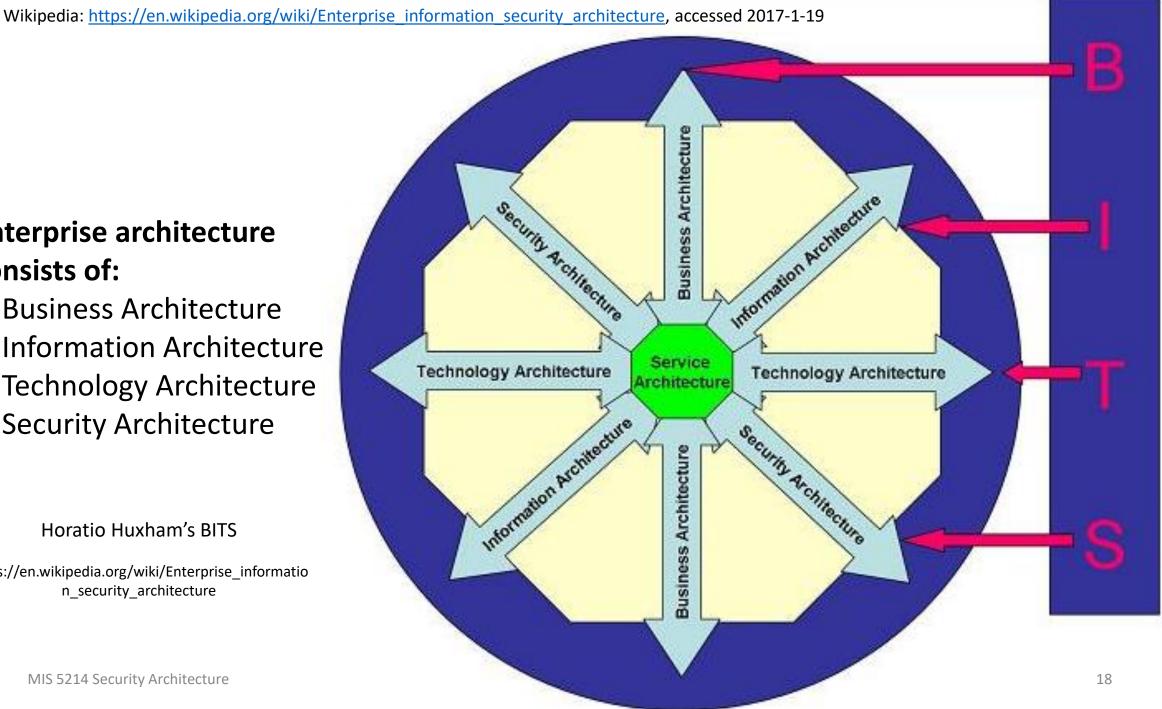
http://www.sabsa.org/white\_paper

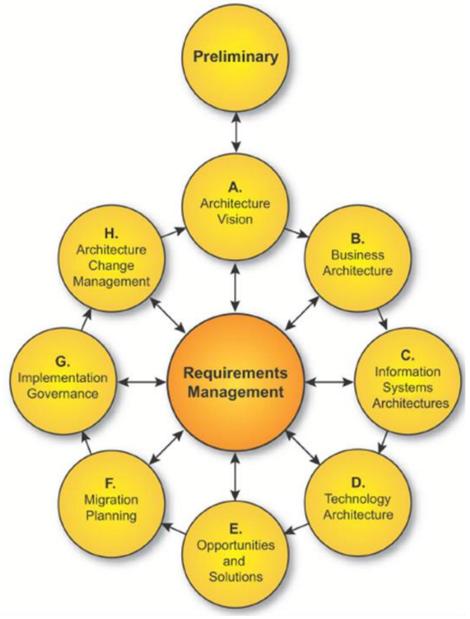
### **Enterprise architecture** consists of:

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

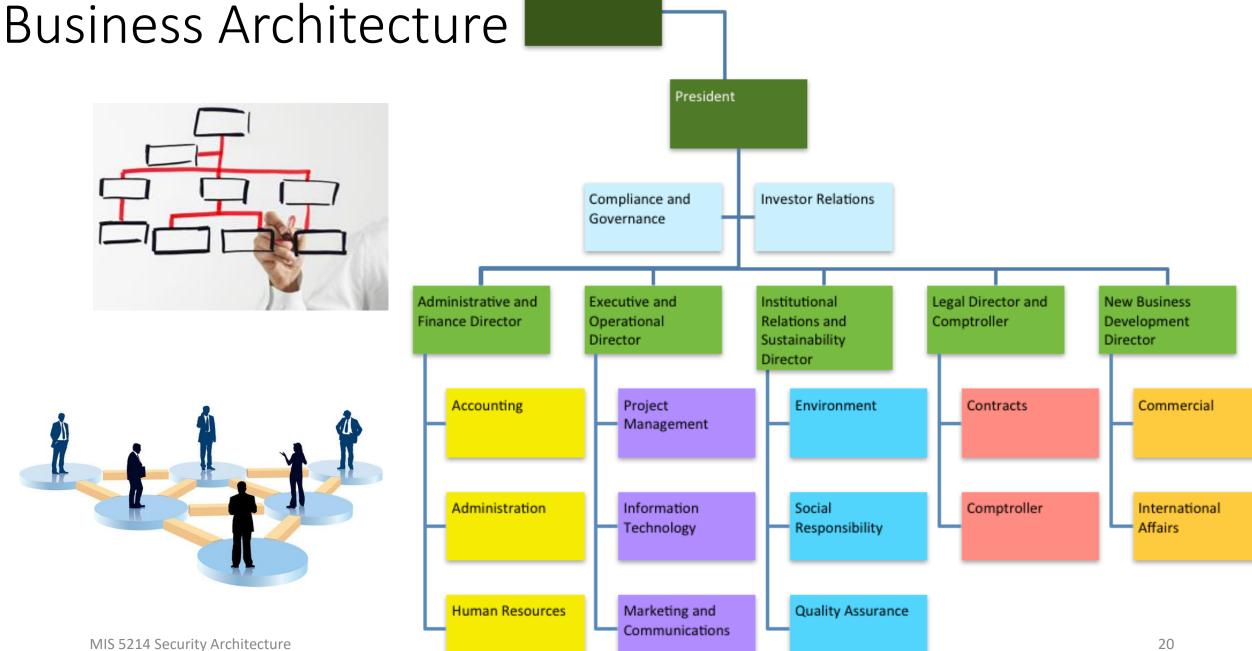
Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise informatio n\_security\_architecture



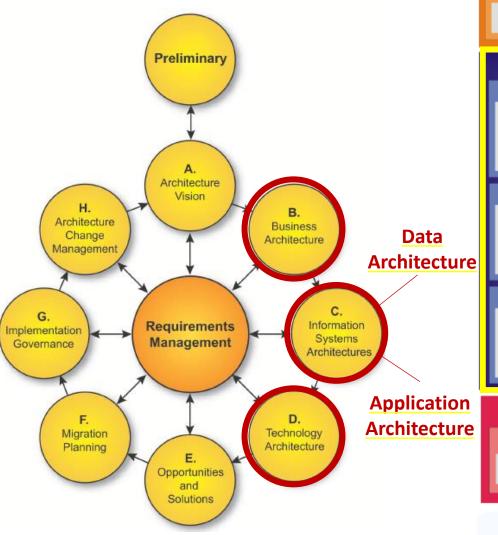


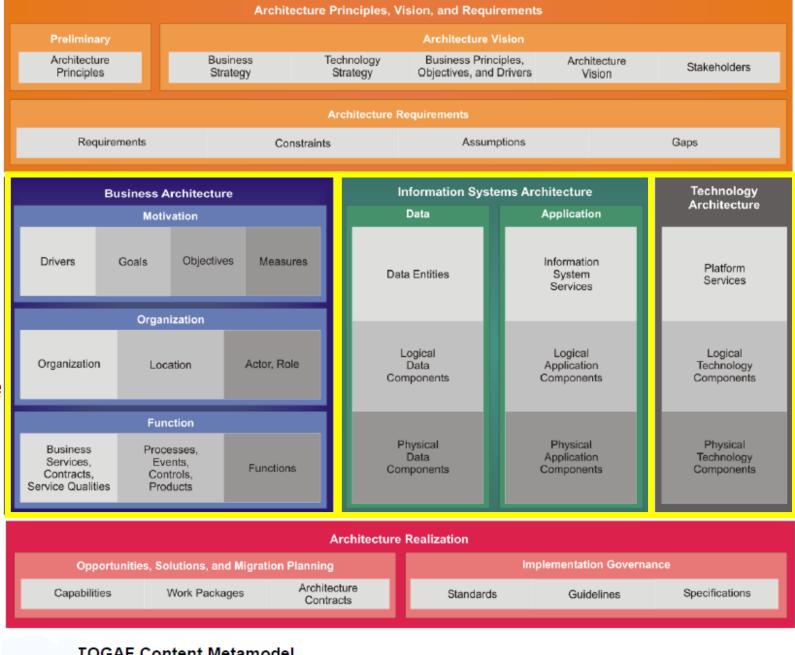
The Open Data Group Architecture Framework (TOGAF) Version 9.1



Board of Directors

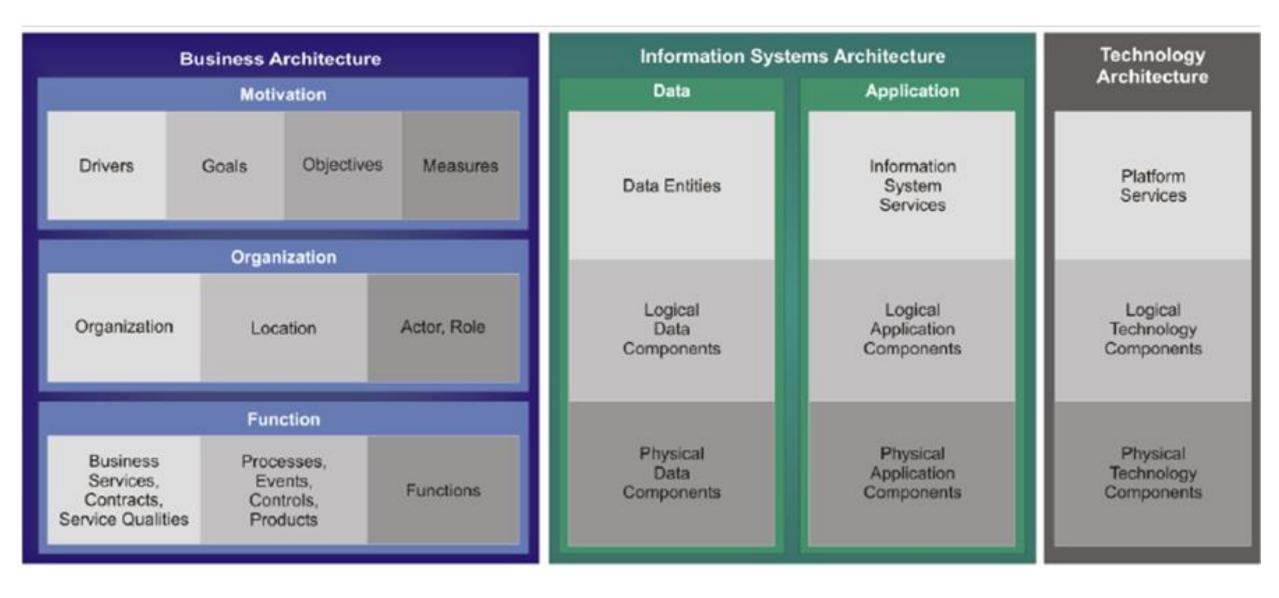
## Information Architecture



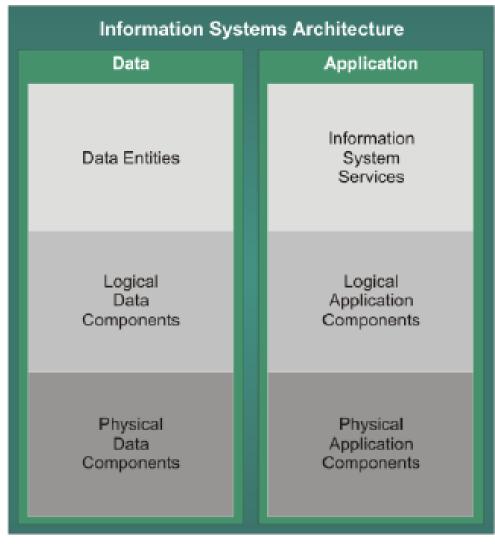


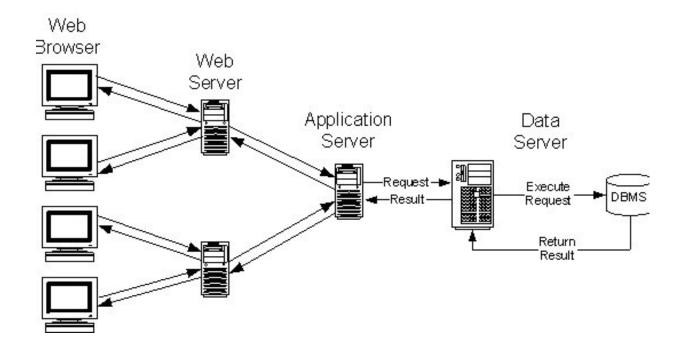
**TOGAF Content Metamodel** 

## Information Architecture



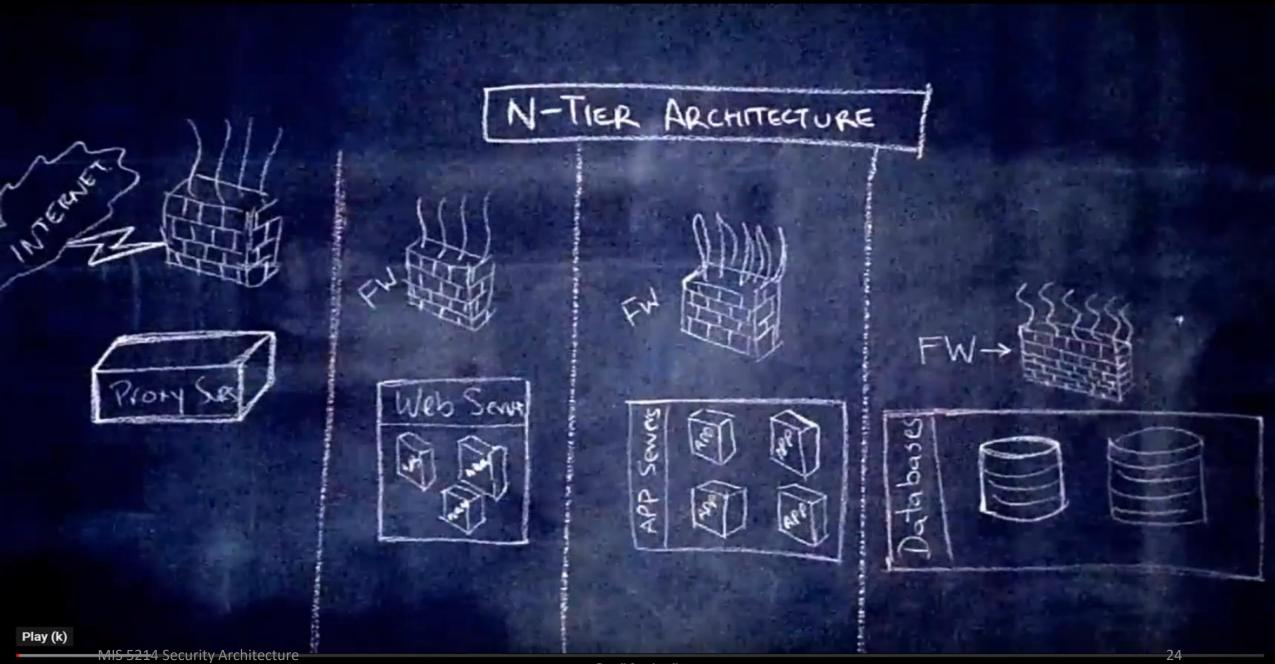
# Conceptual models of Information Systems





Content & Styngeture curity Architecture

Function & Use



ŢĬii.



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

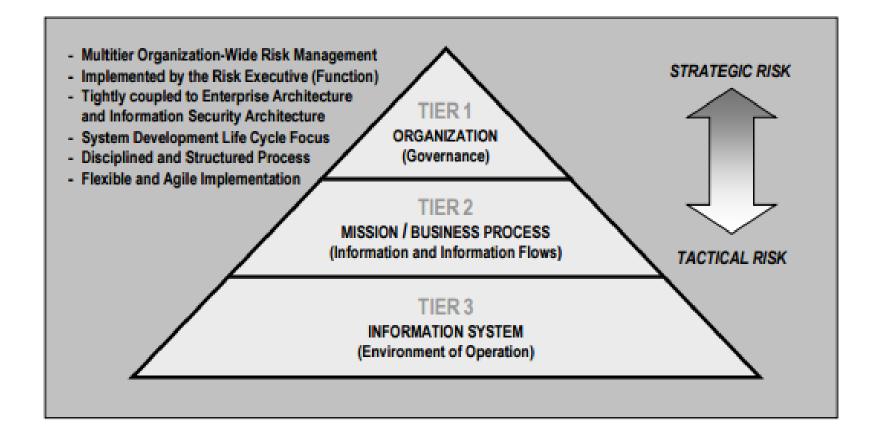
- Consider the purpose and contents of a web-based system for managing the data of public utilities for a small town
- Identify who the users are
- Using what you learned in the video, draw an N-Tier Architecture for the web-based system

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



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

NIST Special Publication 800-37

### Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE TRANSFORMATION INITIATIVE

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

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

February 2010

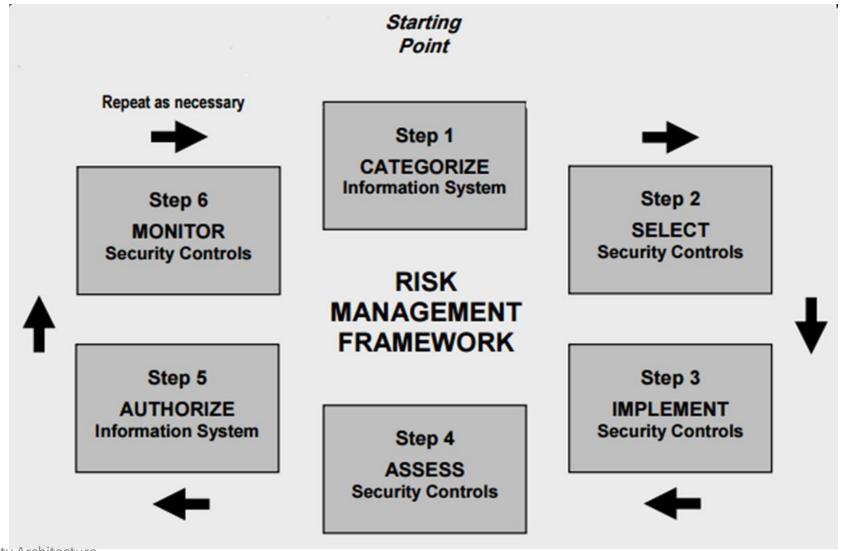
INCLUDES UPDATES AS OF 06-05-2014: PAGE IX



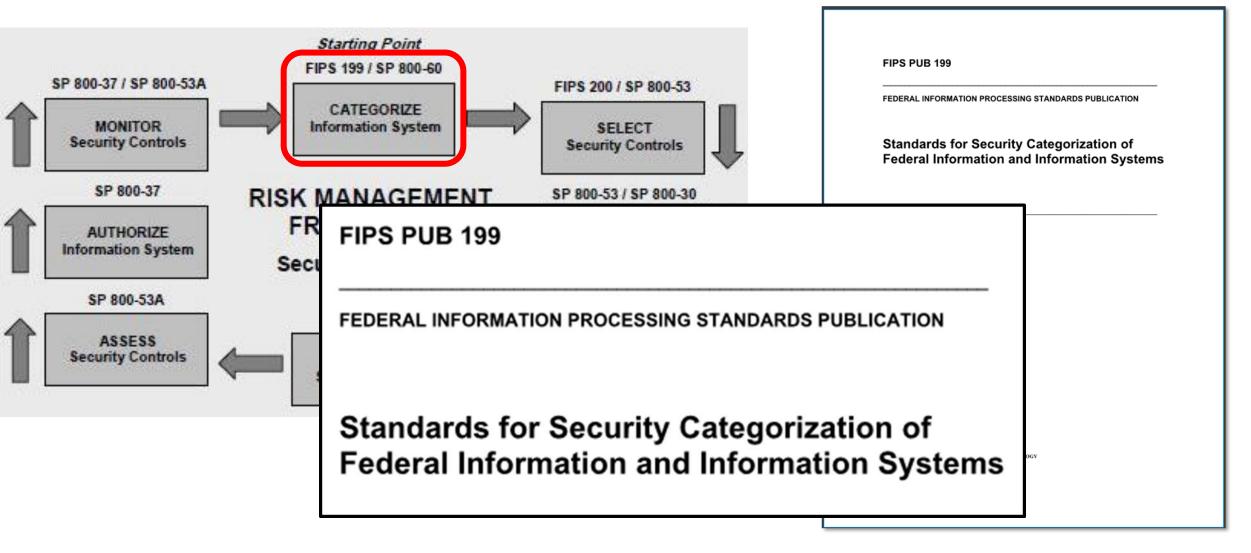
U.S. Department of Commerce Gary Locke, Secretary

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

# NIST Risk Management Framework



# NIST Risk Management Framework



# FIPS 199: Qualitative risk assessment based on security

# objectives

### FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

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

February 2004



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

TECHNOLOGY ADMINISTRATION

Phillip J. Bond, Under Secretary for Technology

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

	POTENTIAL IMPACT				
Security Objective	LOW MODERATE		нідн		
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 <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 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 <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 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



# 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	

# 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

National Institute of Standards and Technology Technology Administration

U.S. Department of Commerce

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

Liteliheed REK Unpact		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								

## Transformation of ordinal qualitative risk categories to interval quantitative risk measures

Likelihood RSK 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

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



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

Risk Scale: High (>50 to 100)

Moderate (>10 to 50)

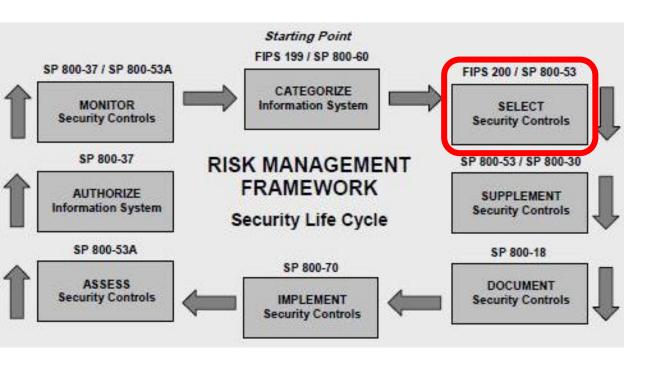
Low (1 to 10)

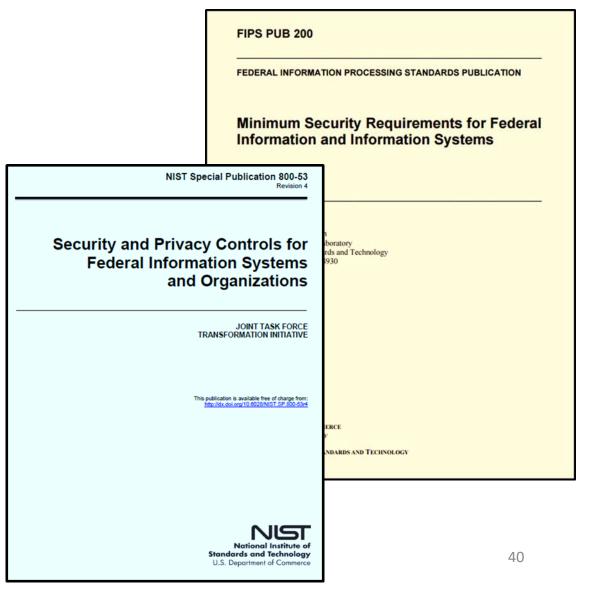


Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Traffic control	10	0.1	1
Comm_Electric Geodatabase	High		
			0
Water Distribution System	50	0.1	5
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1
Water_Sewer Geodatabase	Moderate	0.1	
			0
Parcel Boundary 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	39 <b>1</b>

## 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)

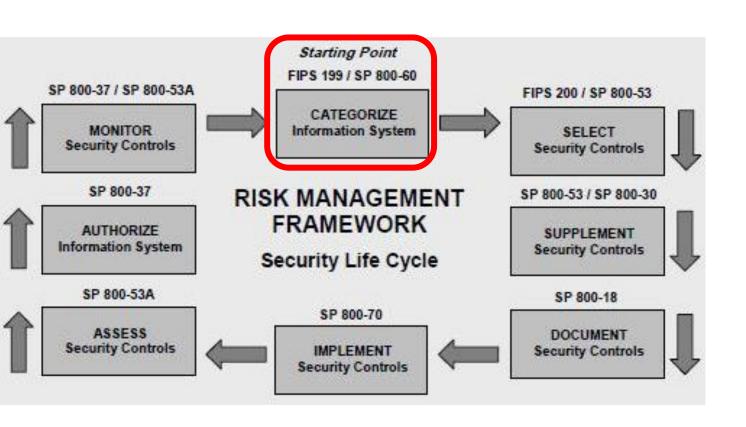


FedRAMP = Federal Risk and Authorization Management Program

<u>Unit 02 – System Security Plan</u> (temple.edu)

42

### Information System Security Plan (SSP)





#### **TABLE OF CONTENTS**

1.	INFORMATI	ON SYSTEM NAME/TITLE1								
2.	INFORMATI	ON SYSTEM CATEGORIZATION1								
	2.1.	Information Types								
	2.2.	Security Objectives Categorization (FIPS 199)								
	2.3.	Digital Identity Determination								
3.	INFORMATI	ON SYSTEM OWNER4								
4.	AUTHORIZING OFFICIALS									
5.	OTHER DES	IGNATED CONTACTS4								
6.	ASSIGNMEN	NT OF SECURITY RESPONSIBILITY5								
7.	INFORMATI	ON SYSTEM OPERATIONAL STATUS								
8.	INFORMATION SYSTEM TYPE7									
	8.1.	Cloud Service Models								
	8.2.	Cloud Deployment Models								
	8.3.	Leveraged Authorizations								
9.	GENERAL SY	YSTEM DESCRIPTION9								
	9.1.	System Function or Purpose								
	9.2.	Information System Components and Boundaries9								
	9.3.	Types of Users								
	9.4.	Network Architecture11								
10.	SYSTEM EN	VIRONMENT AND INVENTORY12								
	10.1.	Data Flow12								
	10.2.	Ports, Protocols and Services14								
11.	SYSTEM INT	TERCONNECTIONS								
12.	LAWS, REGI	ULATIONS, STANDARDS AND GUIDANCE								
	12.1.	Applicable Laws and Regulations17								
	12.2.	Applicable Standards and Guidance17								
13.	MINIMUM	SECURITY CONTROLS								

# FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Cloud Service Provider Name

Information System Name

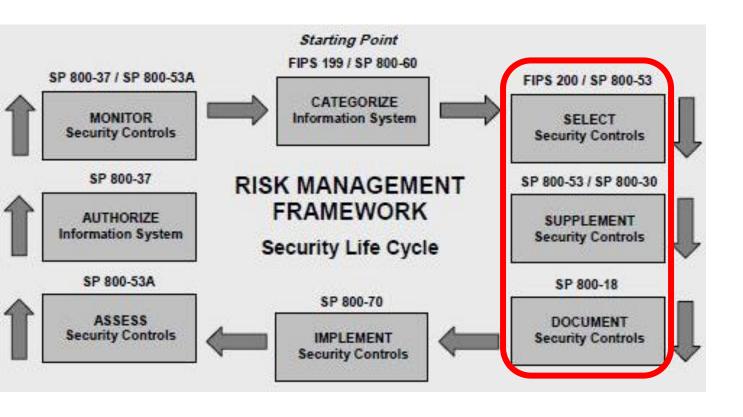
Version #

Version Date



CONTROLLED UNCLASSIFIED INFORMATION

### Information System Security Plan (SSP)





#### **TABLE OF CONTENTS**

1.	INFORMATI	ON SYSTEM NAME/TITLE1
2.	INFORMATI	ON SYSTEM CATEGORIZATION1
	2.1.	Information Types
	2.2.	Security Objectives Categorization (FIPS 199)
	2.3.	Digital Identity Determination
3.	INFORMATI	ON SYSTEM OWNER 4
4.	AUTHORIZI	NG OFFICIALS4
5.	OTHER DES	IGNATED CONTACTS 4
6.	ASSIGNMEN	NT OF SECURITY RESPONSIBILITY5
7.	INFORMATI	ON SYSTEM OPERATIONAL STATUS
8.	INFORMATI	ON SYSTEM TYPE7
	8.1.	Cloud Service Models
	8.2.	Cloud Deployment Models
	8.3.	Leveraged Authorizations
9.	GENERAL SY	YSTEM DESCRIPTION9
	9.1.	System Function or Purpose
	9.2.	Information System Components and Boundaries9
	9.3.	Types of Users
	9.4.	Network Architecture11
10.	SYSTEM EN	VIRONMENT AND INVENTORY12
	10.1.	Data Flow
	10.2.	Ports, Protocols and Services14
11.	SYSTEM INT	TERCONNECTIONS
12.	LAWS, REGI	ULATIONS, STANDARDS AND GUIDANCE17
	12.1.	Applicable Laws and Regulations
	12.2.	Applicable Standards and Guidance17
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

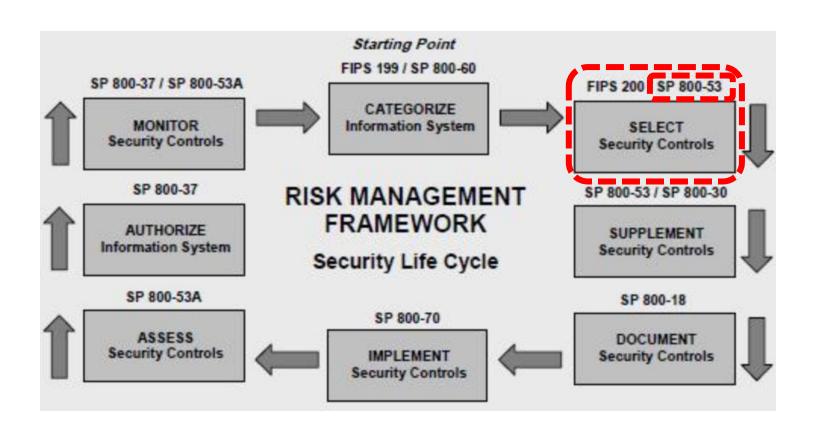
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY William Jeffrey, Director

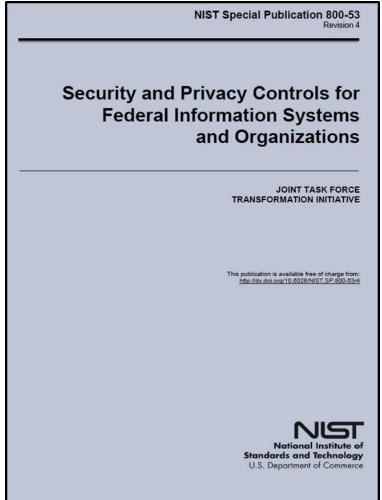
### FIPS 200 Minimum Security Control Requirements

- 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)

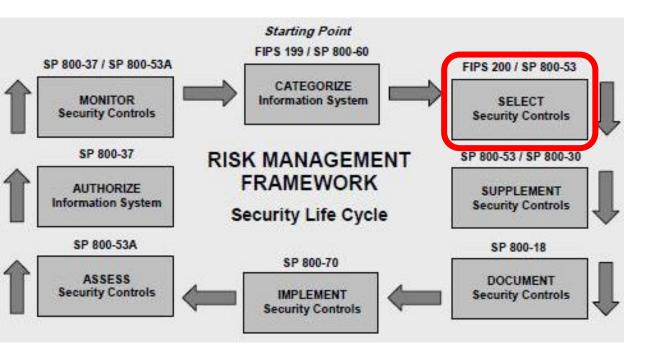
- 10. Media Protection (MP)
- 11. Physical and Environmental Protection \*PE)
- 12. Planning (PL)
- 13. Personal Security (PS)
- 14. Risk Assessment (RA)
- 15. System and Services Acquisition(SA)
- 16. System and Communications Protection (SC)
- 17. System and Information Integrity (SI)

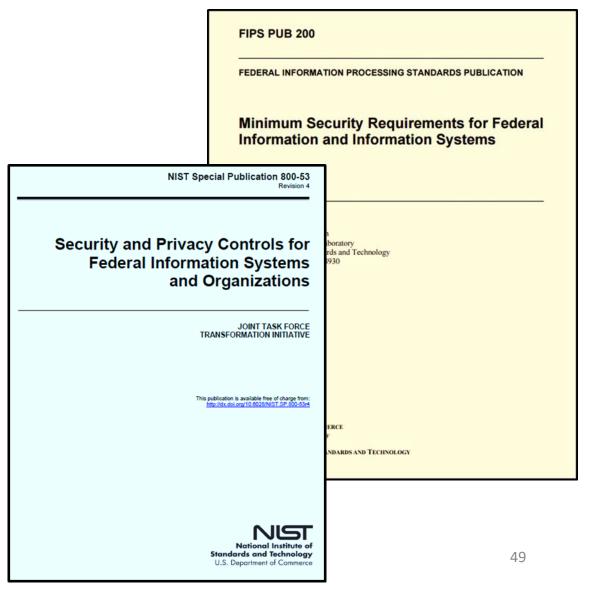
### NIST Risk Management Framework





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





#### NIST Special Publication 800-53 Revision 4

#### Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

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

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

CNTL	CONTROL WAYS	IORITY	INITIA	L CONTROL BASE	ELINES							
NO.	CONTROL NAME	PRIO	LOW	MOD	HIGH							
	Awarenes	s 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 Assessn	nent ar	nd 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							
	Configurati	on Ma	nagement									
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)							

NO										CNT						) L		INITIAL	L CO	NTROL BASE	LINES
SCATE   SCATE   Product of information R Please   Product of information												(	CONT	ROLI	NAME	PRIOF		LOW		MOD	HIGH
Social Control Control Laborate   Facility   Facility																					Not Selected
CNT   Control   Laborate   Fig.   Control   Laborate   Fig.   Control   Control   Laborate   Fig.   Control   Cont																					
Course   C																					
Coll							_			SC-2	8 Pr	otection o	f Inform	ation a	at Rest	P1	No	Selected			
No.   CONTROL NAME   For Several Part Services   For Several Part Severa														<b>E</b>	INITIAL	CONTRO	L BASI	SELINES			
Second Control   Part   Part								NO.		CONTR	OL N	AME		800					=		
Sub-10   S														_	LOW						
Section   Supply Claim Projection   Fig.   As   Section   Supply Claim Projection   Fig.   No.   Section   Fig.   No.   Section   Supply Claim Projection   Fig.   No.   Section   Fig.   No.   Section   Supply Claim Projection   Fig.   No.   Section   Fig.   No.																					
Coll												and Evalua	tion						_	t Selected	Not Selected
Coll   No.     Coll   P.											tion										
CNT   Control Name   First   Absence   First										1.1										t Selected	Not Selected
P.C.17   Account Vision   Telescope   P.C.17   Account Vision   Telescope   P.C.17   Telescope   Tel				0	ONTL	CONT	rpoi	NAME		TBC		INITIAL	CONTR	IOL BA	SELINES			SA-15		t Selected	Not Selected
Part   December   Part   December   Part   December   Part   Part   December   Part   Part   December   Part   Decembe						CON	INOL	THAIR.		8	E LOW			OD	HIGH	-t Cale		CA 10	_		Not Selected
Second Continue		F				Alternate Work Sit	e			P2	Not Se	elected PF-		-17	PE-17				_		
PE 20   Asset Montaning and Trouting   PE 20   Asset Montaning and PE 20   PE 20					PE-18	Location of Inform	ation S	ystem Co	mponents	P3	Not Se								ed		
Parameter   Para																		Not Select	ed		
CONTROL NAME   Part   No.   CONTROL NAME   Part   No.   No				P	E-20	Asset Monitoring	and Tra	cking			Not Se	elected	Not Si	elected Not Selected		ot Sele	cted	Not Select	ed		
CNT   CONTROL NAME														1.	DI 4	ot Sele	cted	Not Selected			
R.S.			CNTL				F	INITIAL		CONTRO	L BASI	ELINES		(3)						1 Delected	not beledied
R.3			NO.	CONT	ROL N	IAME		.,	w	мо	n	uic	u	. (0)	FC-2 (0)	_				SI-1	SI-1
R4   Incident Mandring			ID A	Incident Dans	Tour		-	_						(1)	PL-4 (1)	SC-		SC-1			
Rid		-			resting									-	_	SC-		SC-2			
CONTROL NAME		IR-5 Incident Monitoring IR-6 Incident Reporting												-		ot Sele	cted	SC-3			
CONTROL NAME							P1	IF	1-0	IR-6	(1)	IR-6	(1)	lected .e		SC-					
Control Cont					<b>\</b>	INITIAL	CON	TROL BA	SELINES		)			lected							
Configuration Energy   P   CM					TRIO	INITIAL	CON	NOL DA	DELINES							ot Sele					
Contingency   Pi			OOM TO LINE			LOW	- 1	MOD	н	IGH				-1	PS-1	(7)		(7) (8) (18)	(21)	er (1) (r)	(7) (14)
March   Second   Se											, ieu	Not Se	evieu			SC-8	1)	SC-8 (1)		-8 (1) (2)	SI-8 (1) (2)
Continuo System Normaling													-3				SC-10				
College   Part   Part	CM-8	Information System Component Inventory		P1	CM-8	CM-8	(1) (3) (5	) CM-8 (	1) (2) (3) ) (5)				-5							01 10	
CM-10   Contingency Planning   P1		Configuration Management Plan		ent Plan	P1	Not Selected		CM-9	С	M-9	(2)										
March   Contingency property   Contingency		10 Software Usage Restrictions												-7	PS-7			SC-13			
CB-1	CM-11						(	M-11	CI	W-11	-			-8	PS-8	SC-1	3	SC-13			
Procedures	cn ı	Continuo	Diameter D					CD 4	1 0	0.1		MA	MA-6			SC-1	5	SC-15			
CP-2   Configure Plan   P   CP-2		Procedures	rianning r	olicy and	"									-1					ed		
CP-3    Configurery Training   P2	CP-2	Contingency l	Plan		P1	CP-2	CP-2	CP-2 (1) (3) (8) CP-2 (1)		1) (2) (3)				_							Not Selected
CPA         Contingency Pair Testing         P2         CP4         CP4 (1)         CP4 (1)         CP4 (1)         MPA (1)         (2)         RPA (1)         (2)         RPA (1)         (3)         SC-19         SC-19         SC-19         SC-19         SC-19         SC-19         SC-19         SC-19         SC-19         SC-10         SC-21         SC-21         SC-21         SC-22         SC-23         SC-	CP-3	Contingency	Training		P2	CP-3					1-			Ť	-						
CP-5         Willmaram         P1         Not Selected         CP-6 (1) (2) (3)         0         MP-6 (4)         MP-6 (4)         SC-21         SC-22	CP-4	Contingency i		19										(2) (5							
Section   Sect						-			_		1)			looted							
Part   Telecommunications Services   P1   Not Selected   CP-8 (1) (2)   CP-8 (1)   CP-8 (1) (2)   CP-8 (1) (2											-			lected	Not Selected	SC-2	1	SC-21			
December   Part   December   Part   December   Decemb					1					(4)				-		SC-2	2	SC-22			
CP-0   Information System Baskup	CP-8	Telecommuni	ications Se	rvices	P1	Not Selected	CP.	8 (1) (2)	CP-8 (	1) (2) (3)	ited	rvot Se	ected	-1	SA-1						
CP-10   Information System Recovery and   P1   CP-10   CP-10	CP-9	Information S	vstem Bac	kup	P1	CP-9	С	P-9 (1)	CP-9	1) (2) (3)		PF.	-1	-2	SA-2						
Proceedings					1					(5)	_			-3			C160	30-24		1	
Part	CP-10	Reconstitution	ystem Rec n	overy and	P1	CP-10	CF	-10 (2)	CP-1	0 (2) (4)	-			(2) (9) SA-4 (1) (2) (9)		9)					
Proceedings			nmunicatio	ns Protocols							1-			-5							
Macroscope   Mac			annih Mar	hanisms								PE	-5	1	_						
M-1   M-1	GP-13	Awemative Se	evanty Méd		1		rvot	oelected	rvot S	elected	0	PE-6 (	1) (4)	-							
Productive   Pro	IA-1	Identification :	and Auther					IA-1	1	A-1	1-	DE 1	(4)	(2)							
Compareational Users   P					-	10.0000000		(4) (2)	10.51	12.402.40	-			100/	(e)	_					
IA-3   Device Identification and Authentication   P1   Net Selected   IA-3	1A-2	(Organization	and Auther al Users)	ntication	P	iA-2 (1) (12)	(8)	(1) (2) (3) (11) (12)	(4) (8)	(9) (11)				1							
M-4   Selection Management	18.2	Davisa ldc - 10	fastion :	Authoritation	D.	Not Colonts 1		IA 2	(	12)											
MA-6   Multericator Management   P1   MA-6 (1)(11)   MA-6 (1)(2)(3)   MA-6 (1)(3)(3)   MA				Awatentication										-							
Med.   Authenticator Feedback   P.2   Med.   Med.   Med.				ent	P1	IA-5 (1) (11)	IA-5	(1) (2) (3	IA-5 (	1) (2) (3)	3)	PE-13	(1) (2) )								
1A-7   Coppographic Module Authentication   P1   1A-7	18.0	-			B^	16.0															
1.48   Secretarian and Authentication Pilor—  F1   1.48 (11) (21) (31   1.48 (11) (31) (31   1.48 (11) (31) (31   1.48 (11) (31) (31   1.48 (11) (31) (31) (31   1.48 (11) (31) (31) (31   1.48 (11) (31) (31) (31) (31   1.48 (11) (31) (31) (31) (31) (31) (31) (31)														-							
4  (4) (4)   (4) (4)   (4) (4)   (4) (4)   (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)		Identification and Authentication (Non-				IA-8 (1) (2) (3)		(1) (2) (3	IA-8 (	1) (2) (3)	1	PE-	16								
M-10		Organizational Users)			_	(4)		(4)	(4)		1										
											1										
					PO	Not Selected					1										
		Incid																			
IR-2   Incident Response Training   P2   IR-2   IR-2   IR-2 (1)(2)											1										
	IR-2	Incident Resp	onse Train	ing	P2	IR-2		IK-2	IR-2	(1)(2)	1										

#### TABLE D-2: SECURITY CONTROL BASELINES 32

CNTL		RITY	INITIAL CONTROL BASELINES							
NO.	CONTROL NAME	PRIORITY	LOW	MOD	HIGH					
	Acc	ess Con	trol							
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					

																		<b> </b>		INITIAL	CONTROL	RASE	LINES
												NO.		CON	rrol	N/	AME	PRIORTY		LOW	MOD		HIGH
												SC-25	-	in Nodes				PO		Selected	Not Select		Not Selected
														n Nodes neypots				PO		Selected	Not Select		Not Selected Not Selected
														atform-Independ	ient Ap	pplic	ations	PO		Selected	Not Select		Not Selected
												SC-28		otection of Infor				P1		Selected	SC-28		SC-28
													•				INITIAL			TIMES	t Selec		Not Selected
									•	NO.		CONTR	OL NA	ME	PRIORTY	L	INITIAL	CONTRO	L BASE	LINES	t Selec		Not Selected
										NU.					8		LOW	MOE	)	HIGH	t Select		Not Selected
									5	A-10 D	eveloper	Configurat	ion Ma	nagement	P1		Not Selected	SA-1	0	SA-10	- Selec	ea	Not Selected
														and Evaluation	P1		Not Selected Not Selected	SA-1		SA-11	t Select	ted	Not Selected
										A-12 S A-13 T		ain Protect	ion		P1 P0		Not Selected Not Selected	Not Sele		Not Selecter	t Select	ted	Not Selected
					1									INITIAL CONT	_	•		ot Sele		Not Selected	t Select		Not Selected
						CNTL NO.		CONT	ROL	NAME		PRIORTY		IMITIAL CONT	nor D	not		ot Sele	ected	SA-15	t Select		Not Selected
													LO		MOD		HIGH	ot Seld	ected	SA-16	SC-39	ted	Not Selected SC-39
						PE-17	Alternat	e Work Site	_				Not Se		E-17	_	PE-17	ot Sele		SA-17	Select	ted	Not Selected
					-	PE-18 PE-10	Informa	of Information Leakag	tion S	stem Com	ponents		Not Se		Selecte Selecte		PE-18 Not Selected	ot Sele		Not Selecter Not Selecter		ted	Not Selected
					l l			lonitoring a		cking					Selecte		Not Selected	ot Sele		Not Selected		ted	Not Selected
											Р	fanning .									t Selec		Not Selected
			[	CNTL					È		INITIAL	CONTRO	L BASI	ELINES	(3)	-	PL-1 PL-2 (3)	ot Sele	ected	Not Selected Not Selected		ted	Not Selected
				NO.	CON	ITROL I	IAME		PRIORTY	LOV	,			HIGH	(3)		PL-2 (3)				SI-1		SI-1
			ļ									MOE			(1)		PL-4 (1)	SC-	1	SC-1			
			}	IR-3 IR-4	Incident Respon				P2 P1	Not Sel		IR-3 ( IR-4 (		IR-3 (2) IR-4 (1) (4)	+			SC-		SC-2	SI-2 (2)		SI-2 (1) (2)
			ŀ	IR-5	Incident Monitori	ng			P1	IR-	5	IR-5		IR-5 (1)	ecte	d	Not Selected	ot Sele	cted	SC-3	-3 (1) (		SI-3 (1) (2) SI-4 (2) (4) (5)
			[	IR-6	Incident Reportin	9			P1	IR-	8	IR-6 (	1)	IR-8 (1)	8		PL-8	SC-		SC-4 SC-5	SI-5	(5)	SI-5 (1)
		CNTL				E		INITIAL	CONT	ROL BAS	ELINES		)	IR-7 (1) IR-8	ecte	d	Not Selected	ot Sele		Not Selecter		ted	SI-6
		NO.	C	ONTRO	NAME	PRIORTY	Η.	ow		MOD	Т	IGH	ted	Not Selected	+	_		-7 (3)		SC-7 (3) (4) (	5) -7 (1) (	7)	SI-7 (1) (2) (5)
		CM-6	Configuration	0.4		P1		M-6		CM-6		(1) (2)	ted	Not Selected	1-1-	-	PS-1 PS-2	(7) SC-8	(1)	(7) (8) (18) (2 SC-8 (1)	1) -8 (1) (	2)	(7) (14) SI-8 (1) (2)
			Least Function			P1				(1) (2) (4)		1) (2) (5)			-3		PS-3		.,,		-0(1)(	2)	31-0 (1) (2)
		CM-8	Information S	ystem Cor	nponent Inventory	P1	C	M-8	CM-8	(1) (3) (5)	CM-8 (	1) (2) (3)		MA-1	-4		PS-4 (2)	SC-1		SC-10	SI-10		SI-10
		_					_			4-9		) (5) M-9		MA-2 (2)	-5-	-	PS-5 PS-6	ot Sele		Not Selecter SC-12 (1)	SI-11		SI-11
CNTL NO.	CON	TROL N	AME	PRIORTY	INITIA	CONTR	OL BASE	LINES		1-10	CN	A-10	(2)	MA-3 (1) (2) (3 MA-4 (2) (3)	1-7		PS-7	1			SI-12	_	SI-12
NO.	CON	I KOL N	-UNI C	PRIC	LOW	м	OD	HIGH	н	5-11	CN	A-11	-	MA-5 (1)	-8		PS-8	SC-1	3	SC-13	t Select		Not Selected Not Selected
			Awarer	ness and	Training					2-1	C	P-1		MA-8	Ī.	_	RA-1	SC-1	5	SC-15	t Selec		Not Selected
AT-1	Security Awarene Procedures	ess and Tra	ining Policy and	d P1	AT-1	AT	-1	AT-1	1					MP-1	-1-	-	RA-1	ot Sele	ected	Not Selected	SI-16		SI-16
AT-2	Security Awarene	ss Trainin	,	P1	AT-2	AT-	2 (2)	AT-2	(2)	1) (3) (8)	CP-2 (	1) (2) (3) (5) (8)	_	MP-1	-3		RA-3	SC-1		SC-17 SC-18	t Selec	ted	Not Selected
AT-3	Role-Based Secu		9	P1	AT-3	AT	-3	AT-S	3	2.3		-3 (1)		MP-3	┇═			90.1		SC-18 SC-19			
AT-4 AT-5	Security Training Withdrawn	Records		P3	AT-4	A1	-4	AT-4		4 (1)	CP-4	(1) (2)	_	MP-4	(2)	(5)	RA-5 (1) (2) (4) (5)	SC-2		SC-20			
AIT	TTILITATION		Audit a	nd Accou	ntability					(1) (3)	CP-6 (	1) (2) (3)	*)	MP-5 (4) MP-6 (1) (2) (3	ecte	d	Not Selected	SC-2	1	SC-21			
AU-1	Audit and Accoun	ntability Pol	icy and	P1	AU-1	AL	-1	AU-	1	1) (2) (3)	CP-7 (	1) (2) (3)	1)	MP-7 (1)				SC-2	_	SC-22			
AU-2	Procedures Audit Events			P1	AU-2	AU-	2 (3)	AU-2	(3)	(1) (2)	CP-8 (	1) (2) (3)	ted	Not Selected	-1		SA-1						
AU-3	Content of Audit 8			P1	AU-3	AU-		AU-3 (1		9 (1)		(4) 1) (2) (3)	_	PF-1 -2			SA-2	SC-23		SC-23			
AU-4 AU-5	Audit Storage Ca Response to Aud			P1	AU-4 AU-5	AL AL		AU-5 (1			(	(5)			-3	3 SA-3		ot Sele	ected	SC-24			
AU-6	Audit Review, An			P1	AU-6	AU-6		AU-6 (1)		10 (2)	CP-10	0 (2) (4)	_	PE-2 PE-3 (1)	(2)	(2) (9) SA-4 (1) (2) (9) (10)							
AU-7	Audit Reduction a			P2	Not Selected	AU-		(6) AU-7		elected		elected		PE-4	-5		SA-5						
	Time Stamps	апо кероп	Generation	P1	AU-8	AU-		AU-8		elected		elected elected		PE-5	1-	_		-					
AU-9	Protection of Aud	it Informati	on	P1	AU-9	AU-	(4)	AU-9 (2)	(3) (4)	1			)	PE-8 (1) (4)	-8		SA-8	1					
	Non-repudiation			P2	Not Selected AU-11	Not Se		AU-1		1-1	U	A-1	_	PE-8 (1)	(2)		SA-9 (2)						
	Audit Record Ret Audit Generation			P1	AU-11 AU-12	AU		AU-12 (1		) (2) (3)	IA-2 (1	1) (2) (3)		PE-9	1								
AU-13	Monitoring for Info	omation D	isolosure	P0	Not Selected	Not Se		Not Sele		1) (12)	(4) (8)	(9) (11) (9) (11) 12)	_	PE-10	-								
AU-14 AU-15	Session Audit Alternate Audit C			P0	Not Selected	Not Se		Not Sele		i-3	U	4-3		PE-11 (1) PE-12	+								
	Cross-Organizati		00	PO	Not Selected Not Selected	Not Se		Not Sele		) (2) (3)		4-4 1) (2) (3)	3)	PE-13 (1) (2)									
			Security Asses		d Authorization					1)	(1	11)		(3) PE-14	+								
CA-1	Security Assessm Policies and Proc	nent and A	uthorization	P1	CA-1	CA	-1	CA-	1	i-8 i-7		4-6 4-7		PE-15 (1)									
CA-2	Security Assessm			P2	CA-2	CA-	2 (1)	CA-2 (1	) (2)	) (2) (3)	IA-8 (1	1) (2) (3)		PE-18									
	System Interconn	nections		P1	CA-3	CA-	3 (5)	CA-3	(5)	4) elected	(	(4) elected											
	Withdrawn Plan of Action an	d Mineton		P3	CA-5	C.F		CA-		elected		elected											
	Security Authoriz		-	P2	CA-6	CA		CA-		elected		elected											
CA-7	Continuous Monit	toring		P2	CA-7	CA-		CA-7	(1)														
	Penetration Testi			P2	Not Selected CA-9	Not Se		CA-		I-1 I-2		R-1 (1)(2)											
CA-9	Internal System C	onnection	S Configur		nagement	C.F	-8	CA-		-	110-2	(-/(4)											
CM-1	Configuration Ma	nagement		P1	CM-1	CN	1-1	CM-	1	1													
CM-2	Procedures Baseline Configu	ration		P1	CM-2	CM-2 (1	(3) (7)	CM-2 (1) (7)	(2) (3)	1													
										-													
	Configuration Cho Security Impact A		OI	P1 P2	Not Selected CM-4	CM-		CM-3 (1 CM-4		1													
	Access Restrictio		nge	P1	Not Selected	CN		CM-5 (1)		1													

### NIST 800-53 Controls are presented alphabetically

- 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

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

### 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:

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

#### RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

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

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

of the risk assessment policy and associated

nization-defined frequency]; and organization-defined frequency].

tablishment of policy and procedures for the Is and control enhancements in the RA family. s, Executive Orders, directives, regulations, policies and procedures at the organization s and procedures unnecessary. The policy can ity policy for organizations or conversely, can mplex nature of certain organizations. The am in general and for particular information nent 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 55

#### SSP – Control Inventory Example

#### RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

- Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
  - A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  - 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:	Responsible Role:		
Parameter RA-1(a)			
Parameter RA-1(b)	(1):		
Parameter RA-1(b)	(2):		
Implementation St	atus (check all that apply):		
☐ Implemented			
☐ Partially implen	nented		
☐ Planned	☐ Planned		
☐ Alternative imp	☐ 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-I What is the solution and how is it implemented?		
Part a		
Part b		

### **RA** -2

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

#### 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.

ntative reviews

for effective
e impacts to
information and
vailability.
activity with
information
nizations also
ith the USA
national-level

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:

- 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
- 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 St	atus (check all that apply):			
☐ Implemented				
☐ Partially implen	nented			
☐ Planned				
☐ Alternative imp	lementation			
☐ Not applicable				
Control Origination	Control Origination (check all that apply):			
☐ Service Provide	☐ 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	☐ 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

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]];

#### 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;
- Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];
- 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 Ennancements. INOIR.

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

r there ig the

ive

unt

on

rcing ition of c or

access

on

ilso be ecurity

of must

t role

ice.

#### 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]];
- c. Reviews risk assessment results [Assignment: organization-defined frequency];
- 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 F	esponsible Role:		
arameter RA-3(b):			
arameter RA-3(c):			
Parameter RA	A-3(d):		
Parameter RA	A-3(e):		
mplementation Status (check all that apply):			
□ Implemented □ Partially implemented			
□ Planned			
	e implementation		
□ Not applic			
Control Origin	nation (check all that apply):		
☐ Service Pr	ovider Corporate		
☐ Service Pr	ovider 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???