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 <u>here</u>: <u>http://securitycards.cs.washington.edu/cards.html</u>

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	Team 5
Chen, Cami	Marin, Vanessa	Amiani, Humbert B.	Johnson, Kyuande	Ranu, Priyanka
Conger, Kelly J.	Mecca, Austin C.	Castelli, Jonathan R.	Li, Zhen	Wang, Mei X.
Damany, Krish	Messina, Anthony R.	Yang, Zibai	Lin, Haozhe	Wong, Anthony
Ergler, Heather	Zheng, Xinyi	Huang, Ting-Yen	Patel, Prince	Murray, Robert
				Ma, Wenyao

University of Washington Security Cards

A security threat brainstorming activity

- Next move onto the <u>orange "Adversary Motivation" suit</u>
- 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.** <u>Spoofing</u> Can an attacker gain access using a false identity?
- 2. <u>Tampering</u> Can an attacker modify data as it follows through the application?
- **3.** <u>**Repudiation**</u> 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. <u>Elevation of privilege</u> Can an attacker assume the identify of a privileged user?

STRIDE Threat Modeling

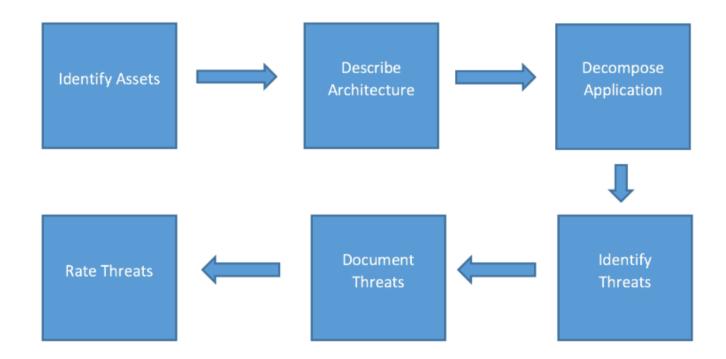
A security threat brainstorming activity

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

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

Threat Modeling

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



Agenda

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

Information Systems – some definitions

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



NIKLAUS WIRTH

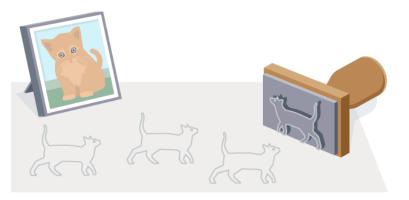
ACRIES .

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 MIS 5214 Security Architecture



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

Conceptual Model



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

Models are ways to describe reality

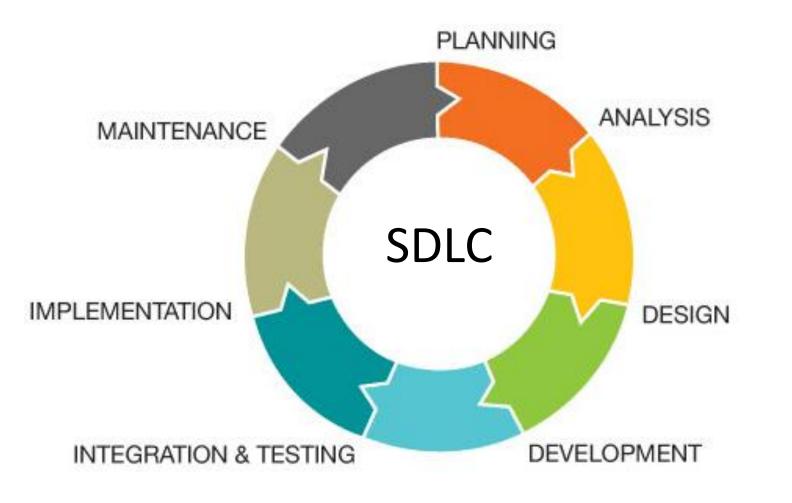
Model quality depends on skill of model designers and qualities of the selected model

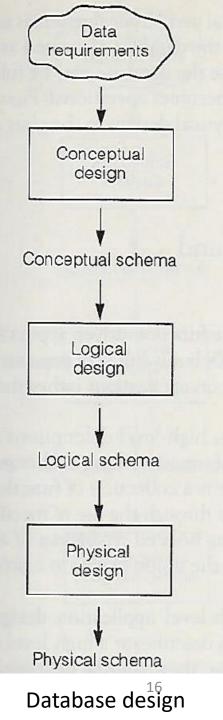
Building blocks of models is a small collection of abstraction mechanisms

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

Abstractions help the designer understand, classify, and model reality

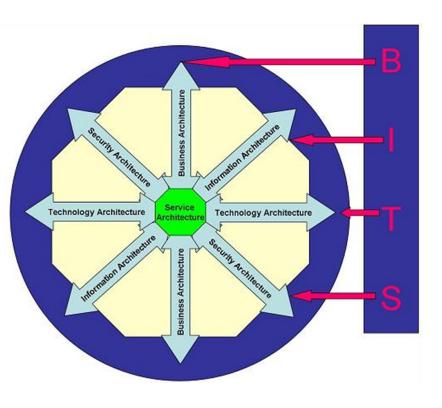
Conceptual models of information system design and development...





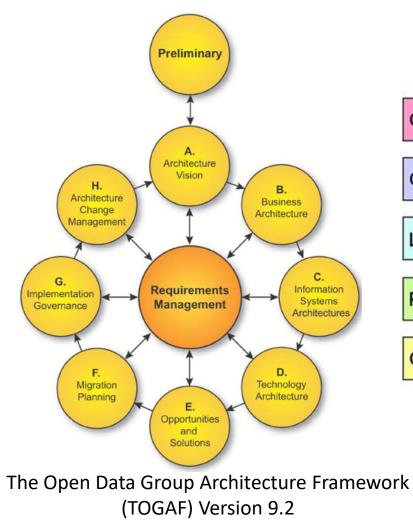
MIS 5214 Security Architecture

Models help us understand enterprise information systems and their security



Horatio Huxham's BITS

https://en.wikipedia.org/wiki/Enterprise_informatio MIS គ2secជពម្ភារដែរក្នុងអ្នកដែរត្រង់អាវុណា



Contextual Security Architecture	Opera	
Conceptual Security Architecture	Operational	
Logical Security Architecture	Security	
Physical Security Architecture	P	
Component Security Architecture	vrchitecture	

Sherwood Applied Business Security Architecture

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

http://www.sabsa.org/white_paper

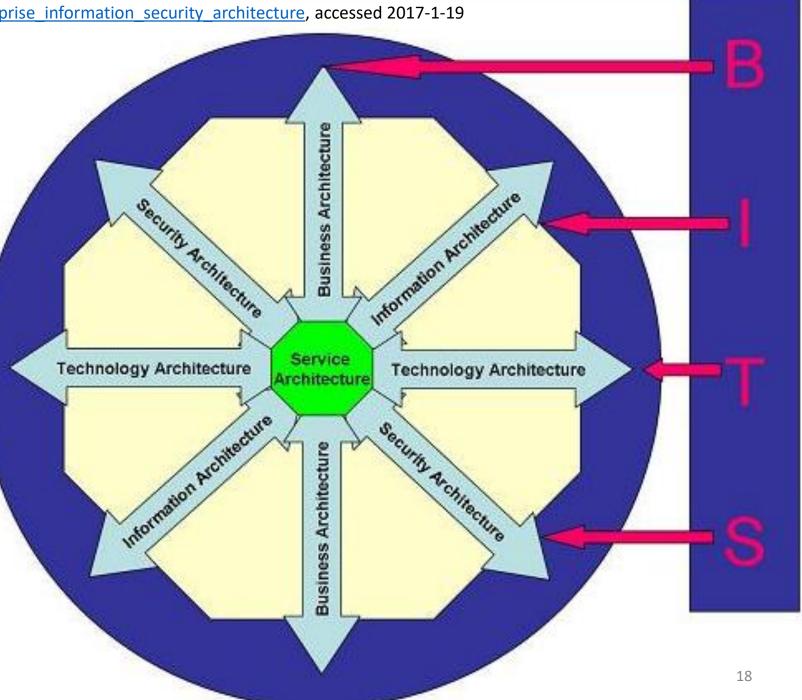
Wikipedia: <u>https://en.wikipedia.org/wiki/Enterprise_information_security_architecture</u>, accessed 2017-1-19

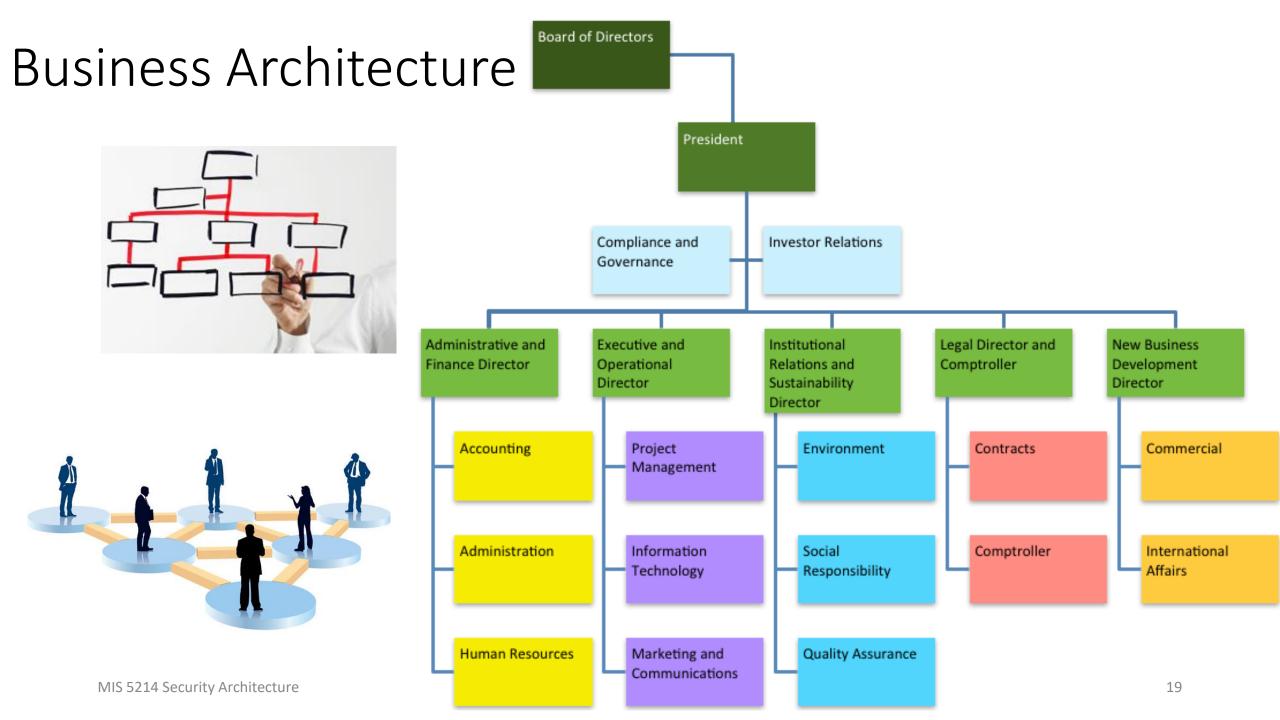
Enterprise architecture consists of:

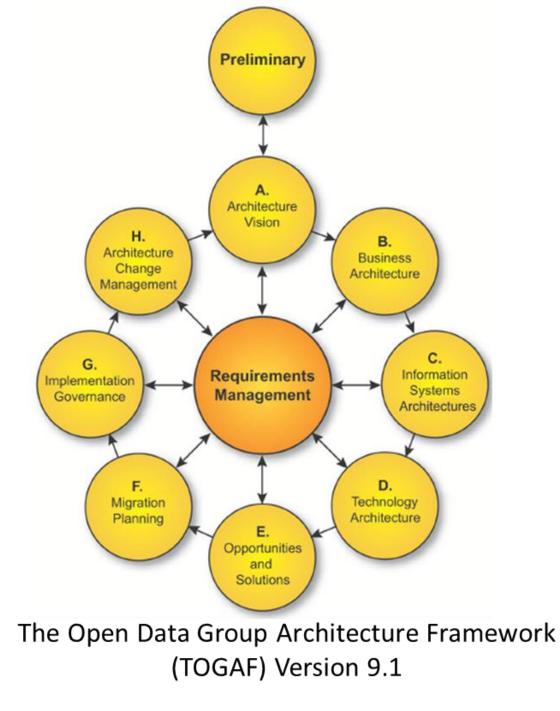
- **Business Architecture** lacksquare
- Information Architecture •
- Technology Architecture •
- Security Architecture •

Horatio Huxham's BITS

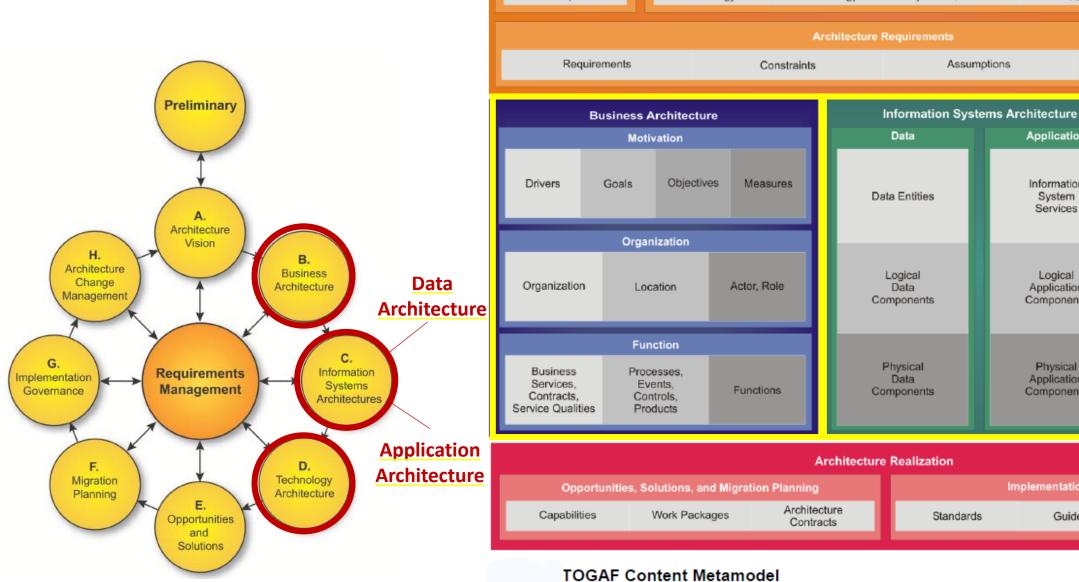
https://en.wikipedia.org/wiki/Enterprise informatio n_security_architecture







Information Architecture



Architecture

Principles

Business

Strategy

Architecture Principles, Vision, and Requirements

Technology

Strategy

Architecture Vision

Business Principles,

Objectives, and Drivers

Architecture

Vision

Application

Information

System

Services

Logical

Application

Components

Physical

Application

Components

Implementation Governance

Guidelines

Stakeholders

Technology

Architecture

Platform

Services

Logical

Technology

Components

Physical

Technology

Components

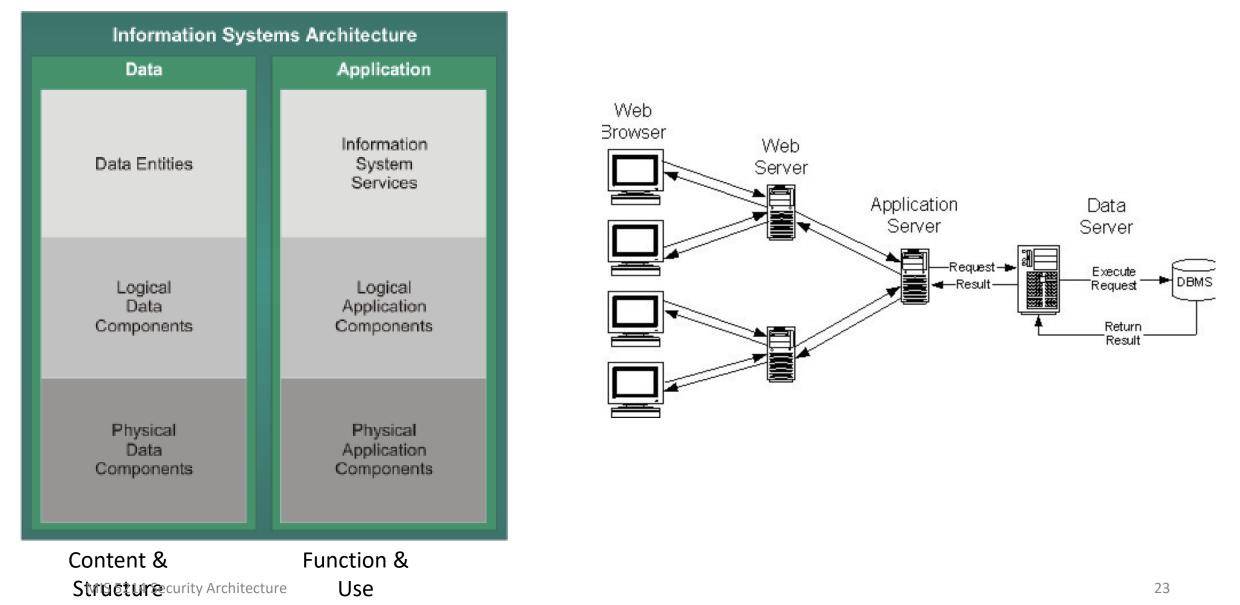
Specifications

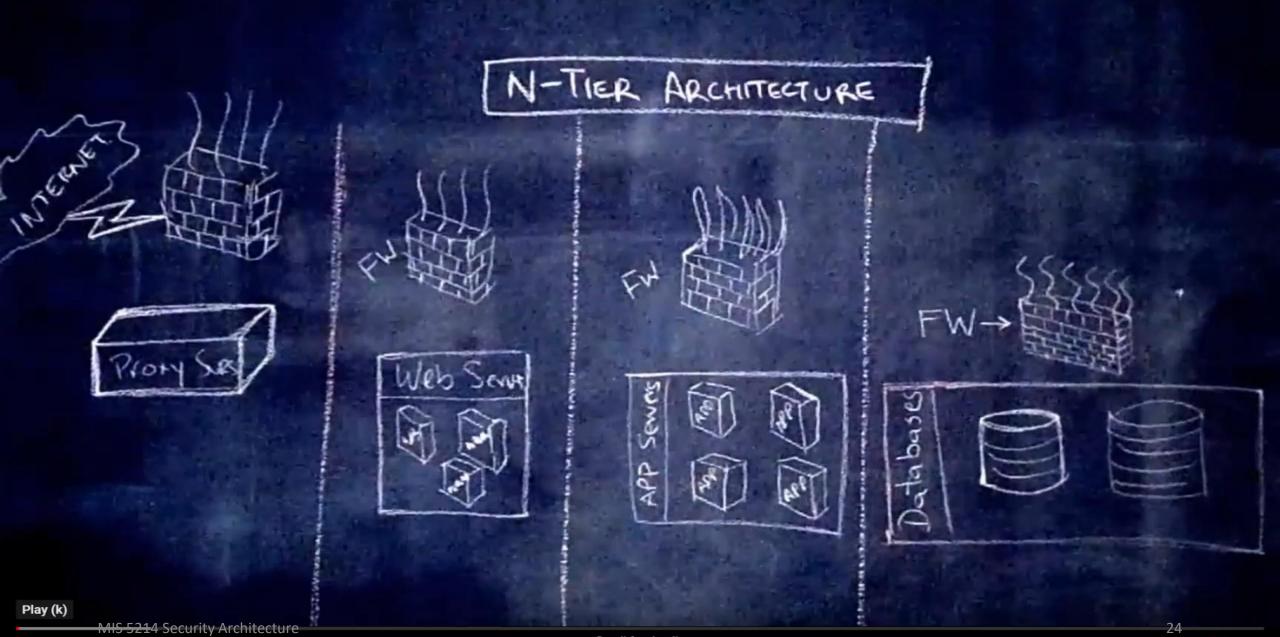
Gaps

Information Architecture

B	usiness Archited	ture	Information Syst	tems Architecture	Technology
Motivation		Data	Application	Architecture	
Drivers	Goals Objec	ctives Measures	Data Entities	Information System Services	Platform Services
Organization	Organization Location	Actor, Role	Logical Data Components	Logical Application Components	Logical Technology Components
Business Services, Contracts,	Function Processes, Events, Controls,	Functions	Physical Data Components	Physical Application Components	Physical Technology Components

Conceptual models of Information Systems





V

lin

 \rightarrow

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

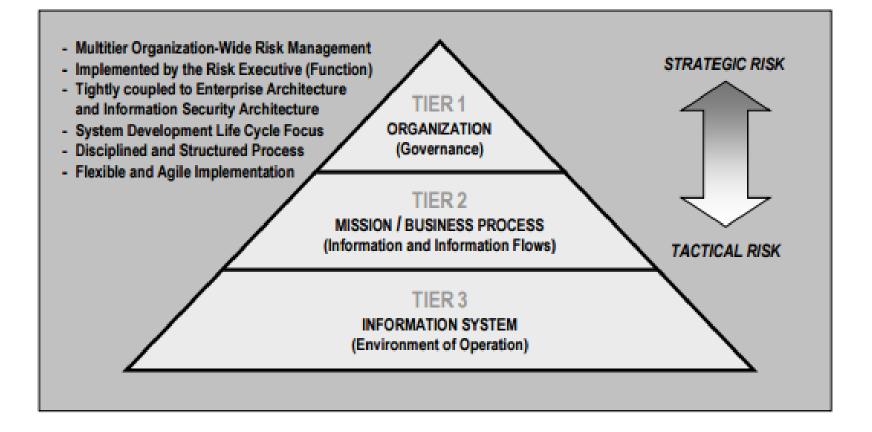
- Consider the purpose and contents of a web-based system for managing the data of public utilities for a small town
- Identify who the users are
- Using what you learned in the video, draw an N-Tier Architecture for the web-based system

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 Revision 1

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE TRANSFORMATION INITIATIVE

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

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

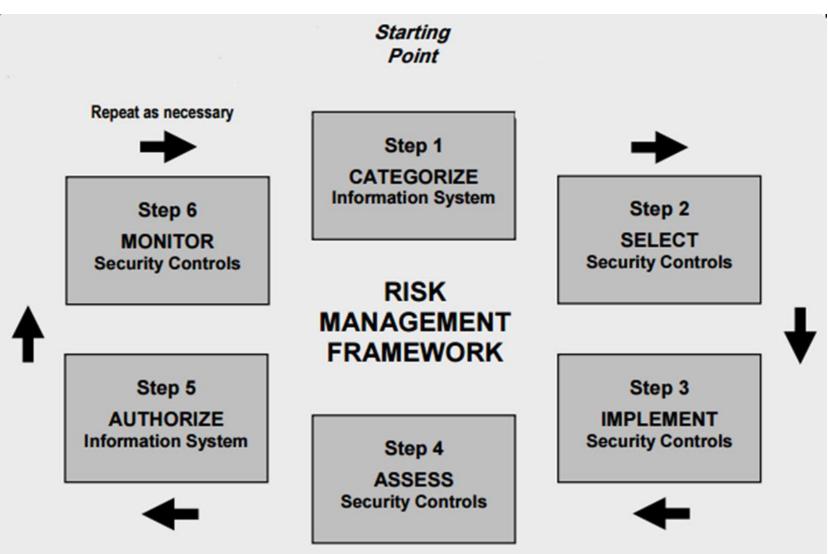
February 2010 INCLUDES UPDATES AS OF 06-05-2014: PAGE IX



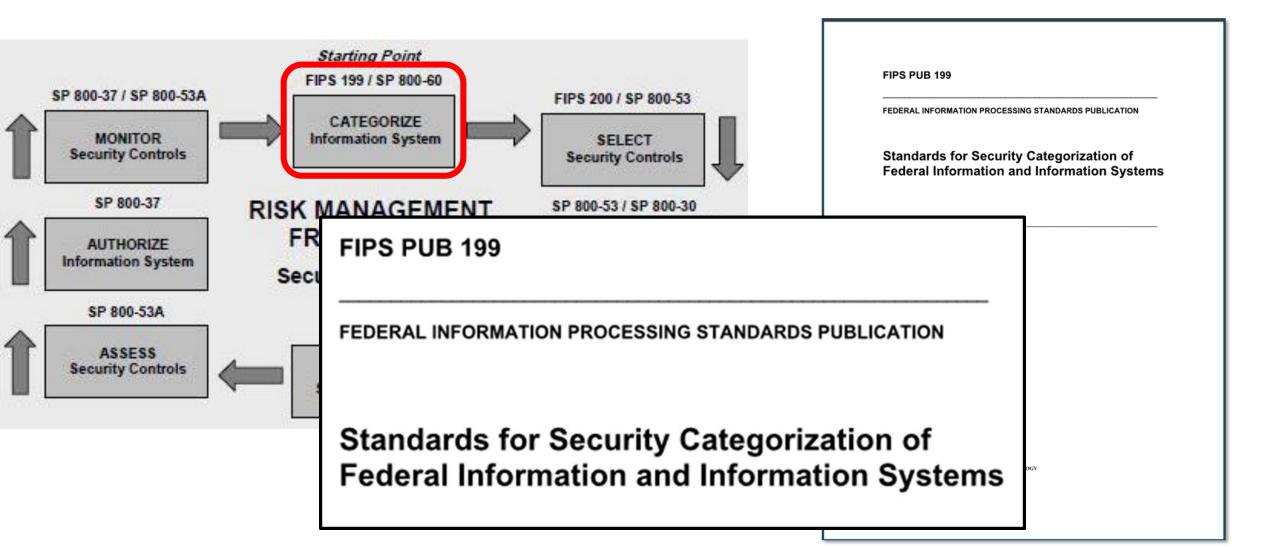
U.S. Department of Commerce Gary Locke, Secretary

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

NIST Risk Management Framework



NIST Risk Management Framework



FIPS 199: Qualitative risk assessment based on security

objectives

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

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

February 2004



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

TECHNOLOGY ADMINISTRATION Phillip J. Bond, Under Secretary for Technology

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

	POTENTIAL IMPACT			
Security Objective	LOW	MODERATE	HIGH	
<i>Confidentiality</i> 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.	
<i>Integrity</i> 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.	
<i>Availability</i> 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 effectMedium: Serious adverse effectHigh: 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:

and

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

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?

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		

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

Likeliheed REK impact		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)	01

Transformation of ordinal qualitative risk categories to interval quantitative risk measures

Likelihood RSK Impact	2	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)	

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

Lindhest - REK - Impart	2	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	o 50) Low (1 to 10)	

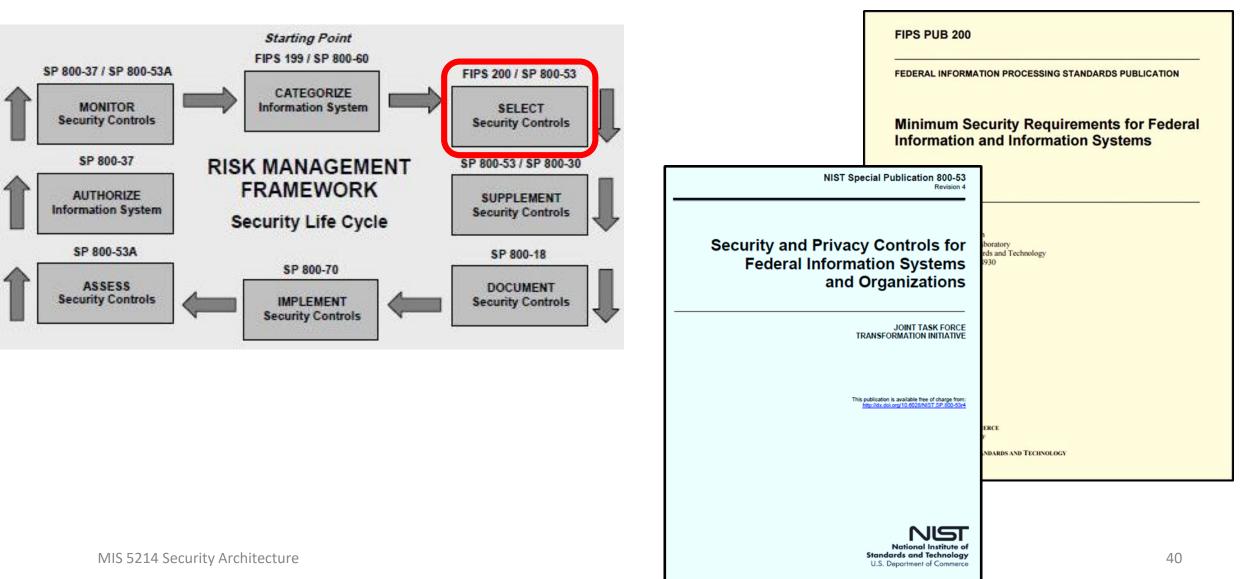
+

= ?

MIS 5214 Security A	Architecture
---------------------	--------------

Impact Rating	Likelihood	Risk
100	1	100
50	0.1	5
10	0.1	1
High		
		0
50	0.1	5
10	0.1	1
10	0.1	1
Moderate	0.1	
		0
10	0.5	5
Impact Rating	Likelihood	Risk
100	1	100
50	0.1	5
50	0.1	5
10	0.5	5
10	0.1	1
10	0.1	1
10	0.1	39 1
	100 50 10 <i>High</i> 50 10 10 10 Moderate 10 10 10 50 50 50 50 10 10	100 1 50 0.1 10 0.1 High

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

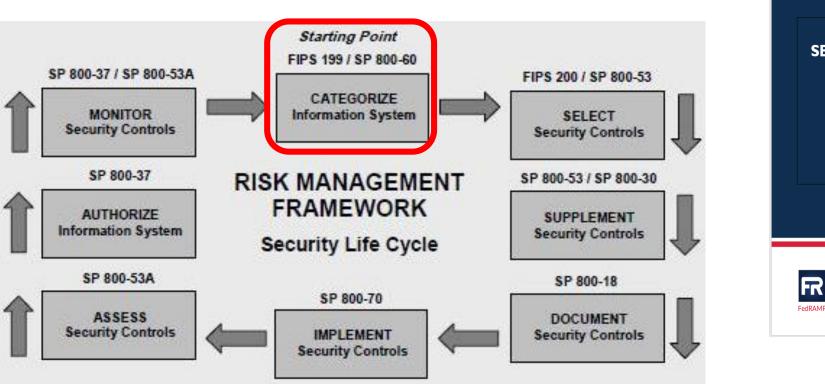
System Security Plan (SSP)

FedRAMP = Federal Risk and Authorization Management Program



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

Information System Security Plan (SSP)





CSP Name | Information System Name

Version #.#, Date

TABLE OF CONTENTS

1.	INFORMAT	ION SYSTEM NAME/TITLE
2.	INFORMAT	ION SYSTEM CATEGORIZATION
	2.1.	Information Types
	2.2.	Security Objectives Categorization (FIPS 199) Digital Identity Determination
	2.3.	Digital Identity Determination
3.	INFORMAT	ION SYSTEM OWNER
4.	AUTHORIZI	NG OFFICIALS
5.	OTHER DES	IGNATED CONTACTS
6.	ASSIGNME	NT OF SECURITY RESPONSIBILITY
7.	INFORMAT	ION SYSTEM OPERATIONAL STATUS
8.	INFORMAT	ION SYSTEM TYPE
	8.1.	Cloud Service Models
	8.2.	Cloud Deployment Models
	8.3.	Leveraged Authorizations
9.	GENERAL S	YSTEM DESCRIPTION
	9.1.	System Function or Purpose
	9.2.	Information System Components and Boundaries
	9.3.	Types of Users10
	9.4.	Network Architecture1
10.	SYSTEM EN	VIRONMENT AND INVENTORY 12
	10.1.	Data Flow12
	10.2.	Ports, Protocols and Services14
11.	SYSTEM IN	TERCONNECTIONS 15
12.	LAWS, REG	ULATIONS, STANDARDS AND GUIDANCE
	12.1.	Applicable Laws and Regulations1
	12.2.	Applicable Standards and Guidance1
13.	MINIMUM	SECURITY CONTROLS 18

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Cloud Service Provider Name

Information System Name

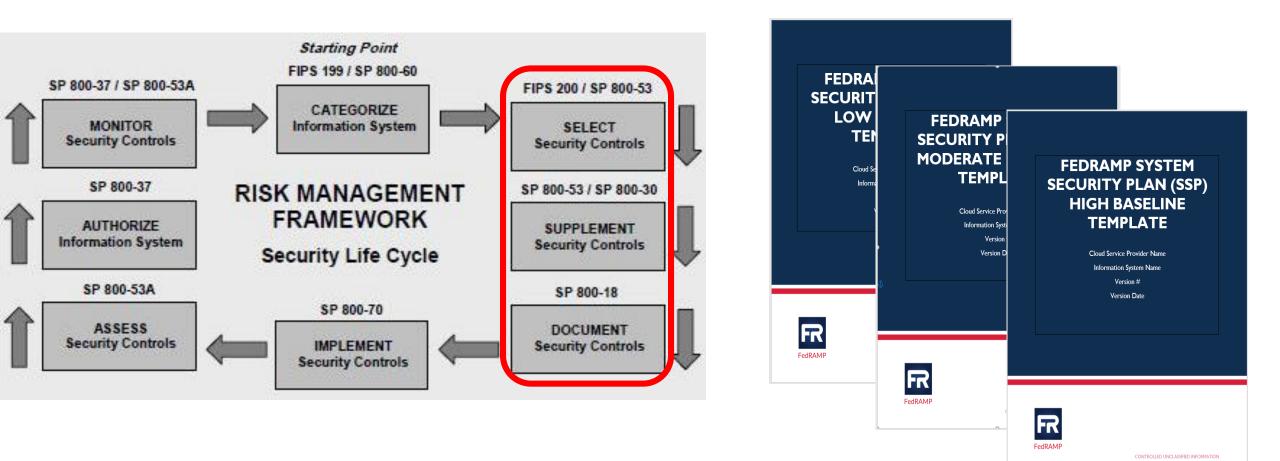
Version #

Version Date



CONTROLLED UNCLASSIFIED INFORMATION

Information System Security Plan (SSP)

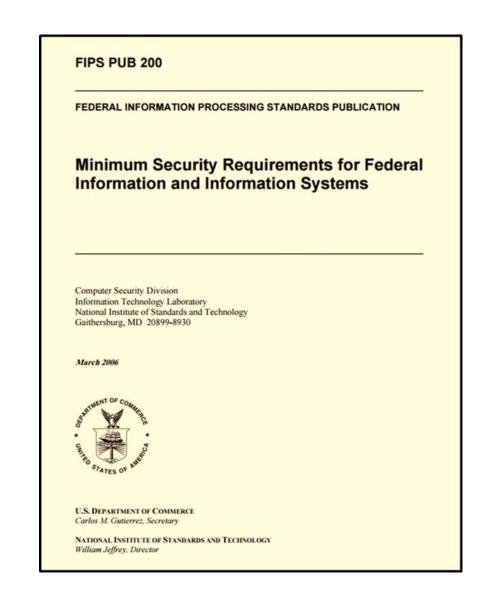


CSP Name | Information System Name

Version #.#, Date

TABLE OF CONTENTS

1.	INFORMAT	ION SYSTEM NAME/TITLE 1
2.	INFORMAT	ION SYSTEM CATEGORIZATION1
	2.1.	Information Types1
	2.2.	Security Objectives Categorization (FIPS 199) 3
	2.3.	Digital Identity Determination
3.	INFORMAT	ION SYSTEM OWNER 4
4.	AUTHORIZI	NG OFFICIALS
5.	OTHER DES	IGNATED CONTACTS 4
6.	ASSIGNME	NT OF SECURITY RESPONSIBILITY
7.	INFORMAT	ION SYSTEM OPERATIONAL STATUS 6
8.	INFORMAT	ION SYSTEM TYPE7
	8.1.	Cloud Service Models 7
	8.2.	Cloud Deployment Models
	8.3.	Leveraged Authorizations
9.	GENERAL S	YSTEM DESCRIPTION9
	9.1.	System Function or Purpose 9
	9.2.	Information System Components and Boundaries
	9.3.	Types of Users
	9.4.	Network Architecture11
10.	SYSTEM EN	IVIRONMENT AND INVENTORY 12
	10.1.	Data Flow12
	10.2.	Ports, Protocols and Services14
11.	SYSTEM IN	TERCONNECTIONS 15
12.	LAWS, REG	ULATIONS, STANDARDS AND GUIDANCE 17
	12.1.	Applicable Laws and Regulations17
	12.2.	Applicable Standards and Guidance
13.	MINIMUM	SECURITY CONTROLS

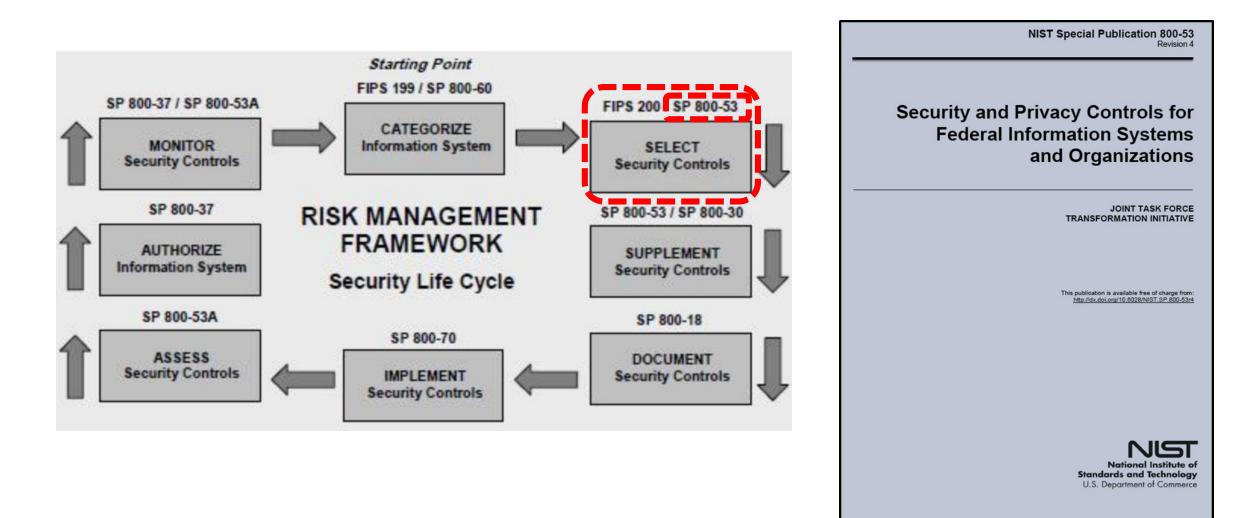


FIPS 200 Minimum Security Control Requirements

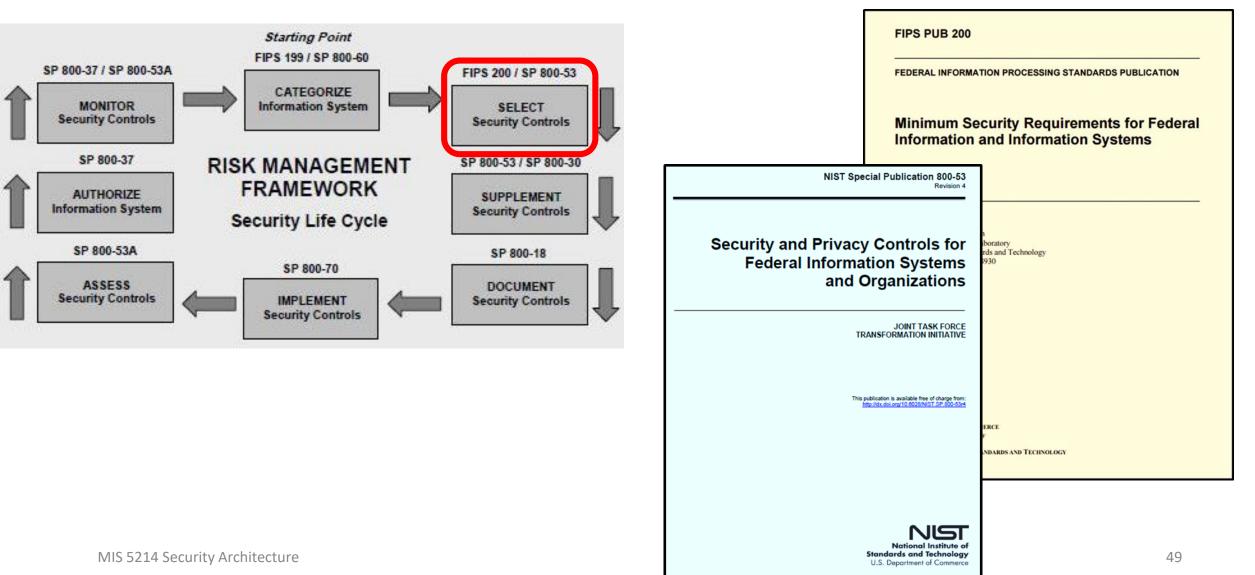
- 1. Access Control (AC)
- 2. Awareness and Training (AT)
- 3. Audit and Accountability (AU)
- 4. Certification, Accreditation, and Security Assessment (CA)
- 5. Configuration Management (CM)
- 6. Contingency Planning
- 7. Identification and Authentication
- 8. Incident Response (IR)
- 9. Maintenance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



NIST Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

> JOINT TASK FORCE TRANSFORMATION INITIATIVE

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

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

CNTL		PRIORITY	INITIAL CONTROL BASELINES				
NO.	CONTROL NAME		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	Accou	intability	•			
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		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	PO	Not Selected	Not Selected	Not Selected		
AU-14	Session Audit	PO	Not Selected	Not Selected	Not Selected		
AU-15	Alternate Audit Capability	PO	Not Selected	Not Selected	Not Selected		
AU-16	Cross-Organizational Auditing	PO	Not Selected	Not Selected	Not Selected		
	Security Assessn	nent ar	d 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)		

														,		INITIAI	CONTROL BAS	FLINES
							CNTL NO.		CNTL NO.						LOW	MOD	HIGH	
										-						2011	mob	
									SC-25 SC-26		in Nodes neypots			P		t Selected t Selected	Not Selected Not Selected	Not Selecter
									SC-27	_	atform-Independ	ant And	lications	P		t Selected	Not Selected	Not Selecter
								-	SC-28	-	otection of Inform			P		t Selected	SC-28	SC-28
								-						-	-		t Selected	Not Selecter
						CNTL			ONTRO		ME	E	INITIA	LCONTR	ROL BAS	ELINES	t Selected	Not Selecte
						NO.			UNITRO		UNIC	PRIOR	LOW	м	OD	HIGH	t Selected	Not Selecte
						SA-10	Develop	oper Cor	nfigurat	ion Ma	nagement	P1	Not Selected	S/	A-10	SA-10	t Selected	Not Selecte
						SA-11	Develop	oper Sec	curity Te	esting a	and Evaluation	P1	Not Selected		A-11	SA-11	t Selected	Not Selecte
						SA-12 SA-13	Supply			ion		P1 P0	Not Selected		elected	SA-12		Not Selecte
						SA-13	Trustwo								elected elected	Not Select		Not Selecte
				CNTL	CON	TROL NAM	-		PRIORITY		INITIAL CONTI	ROL BA	SELINES		elected	SA-15	t Selected	Not Selecte
				NO.	CON	TROL MAIN	2		P	LO	w N	IOD	HIGH		elected	SA-16	t Selected	Not Selecte
				PE-17	Alternate Work Si	te	_		P2	Not Se	lected PI	E-17	PE-17		elected	SA-10 SA-17	SC-39	SC-39
			1	PE-18	Location of Inform	ation System	Compone	ents i	P3	Not Se	lected Not S	elected	PE-18		elected	Not Select	ed t Selected	Not Selecte
				PE-19	Information Leaks					Not Se		elected			elected	Not Select		Not Selecte Not Selecte
				PE-20	Asset Monitoring	and Tracking			PO	Not Se	lected Not S	elected	Not Selecte	1 ot S	elected	Not Select	ed t Selected	Not Selecte Not Selecte
							-				_	1.1	PL-1	ot S	elected	Not Select	ed t Selected	Not Selecte
		CNTL		NTROL N		PRIORTY	INITI	IAL CO	NTROL	BASE	LINES	(3)	PL-1 PL-2 (3)	ot S	elected	Not Select	ed	
		NO.	co	WIROL N	wint:	OI84	LOW		MOD		HIGH					SC-1	SI-1	SI-1
		IR-3	Incident Respon	se Testina		P2 Not	Selected		IR-3 (2	2)	IR-3 (2)	·(1)	PL-4 (1)	S	C-1	SC-1		
		IR-4	Incident Handlin	9		P1	IR-4		IR-4 (1		IR-4 (1) (4)	1			C-2	SC-2	SI-2 (2)	SI-2 (1) (2) SI-3 (1) (2)
		IR-5	Incident Monitor			P1	IR-5		IR-5	_	IR-5 (1)	lected	Not Selecte		elected C-4	SC-3 SC-4	+3 (1) (2) + (2) (4) (5)	SI-3 (1) (2) SI-4 (2) (4) (5
		IR-0	Incident Reporti	ng		P1	IR-0		IR-6 (1)	IR-6 (1) IR-7 (1)	-8	PL-8		C-6	SC-4 SC-5	SI-5	SI-5 (1)
CNTL				È	INITIA	L CONTROL I	BASELINE	E\$)	IR-7 (1) IR-8	lected	Not Selecte		elected	Not Select	ed t Selected	SI-6
NO.		ONTROL	. NAME	PRIORITY	LOW	MOD		HIGH		ted	Not Selected	1 <u>. </u>	PS-1		3) (4) (5)	SC-7 (3) (4) (7) (8) (18) ((5) -7 (1) (7)	SI-7 (1) (2) (
CM-8	Configuratio	0.00		P1	CM-6	CM-8	-	CM-6 (1)		ted	Not Selected	2	PS-1 PS-2		(7) -8 (1)	SC-8 (1)		(7) (14) SI-8 (1) (2)
CM-0 CM-7	Least Functi			P1	CM-0 CM-7	CM-0 CM-7 (1) (2)		A-7 (1) (_		-3						
CM-8			ponent Inventory	P1	CM-8	CM-8 (1) (3)		A-8 (1) (2) (3)		MA-1	-4	PS-4 (2)		C-10	SC-10	SI-10	SI-10
CM-9	Configuration	Managem	oot Plan	P1	Not Selected	CM-9		(4) (5) CM-9			MA-2 (2)	-5	PS-5 PS-6		elected	Not Select SC-12 (1)	ed 01.11	SI-11
CM-10	Software Us			P2	CM-10	CM-10	-	CM-10	0	(2)	MA-3 (1) (2) (3) MA-4 (2) (3)	-0	PS-6 PS-7	50	2412	50-12 (1) SI-12	SI-12
CM-11	User-Installe			P1	CM-11	CM-11 CM		CM-11	1	2)	MA-4 (2) (3) MA-5 (1)	-8	PS-8	SC	2-13	SC-13	t Selected	Not Selecter
CP-1				ingency P	lanning CP-1			CP-1			MA-6					 SC-15	t Selected	Not Selecter
	Contingency Procedures	Planning P	oicy and			CP-1		CP-1				-1	RA-1		elected	Not Select	ed SI-16	SI-16
CP-2	Contingency	Plan		P1	CP-2	CP-2 (1) (3)		² -2 (1) ((4) (5) (MP-1 MP-2	-2	RA-2 RA-3		2-17	SC-17	t Selected	Not Selecte
CP-3																		
	Contingency	Training		P2	CP-3	CP-3		CP-3 (1)		MP-3	-			2-18	SC-18	_	Not delette
CP-4	Contingency Contingency		9	P2 P2	CP-3 CP-4	CP-3 CP-4 (1)		CP-3 (CP-4 (1)			MP-3 MP-4	(2) () RA-5 (1) (2)	4) 50	2-19	SC-19	=	Hut Selecte
CP-4 CP-5	Contingency Withdrawn	Plan Testir	9	P2	CP-4	CP-4 (1)	с	CP-4 (1)	(2)	s)	MP-3 MP-4 MP-5 (4)	(2) (5 ected		4) S(2-19 2-20	SC-19 SC-20	_	nu selete
CP-4	Contingency	Plan Testir prage Site					3) CP	CP-4 (1)	2) (3)	_	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3)) RA-5 (1) (2) (5)	4) S(2-19	SC-19	_	Not Selecte
CP-4 CP-5 CP-6 CP-7	Contingency Withdrawn Alternate Sto Alternate Pro	Plan Testin prage Site poessing Sit	0	P2 P1 P1	CP-4 Not Selected Not Selected	CP-4 (1) 	3) CP (3) CP	 	2) (3) 2) (3)	1)	MP-3 MP-4 MP-5 (4)		 RA-5 (1) (2) ((5) Not Selecte	4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20	SC-19 SC-20		HULSERVE
CP-4 CP-5 CP-6	Contingency Withdrawn Alternate Sto	Plan Testin prage Site poessing Sit	0	P2 P1	CP-4 Not Selected	CP-4 (1) 	3) CP (3) CP (2) CP	CP-4 (1) 2-6 (1) (2 7 (1) (2 (4) 8 (1) (2 (4)	2) (3) 2) (3) 2) (3) 2) (3)	_	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1)	lected) RA-5 (1) (2) ((5) Not Selecte SA-1	4) <u>S(</u> 4) <u>S(</u> 5) 50	2-19 2-20 2-21	SC-19 SC-20 SC-21		Hu Seleve
CP-4 CP-5 CP-6 CP-7	Contingency Withdrawn Alternate Sto Alternate Pro	Plan Testir prage Site poessing Sit nications Se	e rvices	P2 P1 P1	CP-4 Not Selected Not Selected	CP-4 (1) 	3) CP (3) CP (2) CP	CP-4 (1) 2-8 (1) (2 7 (1) (2 (4) 2-8 (1) (2 (4) 2-8 (1) (2 (4)	2) (3) 2) (3) 2) (3) 2) (3)	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1)) RA-5 (1) (2) ((5) Not Selecte SA-1 SA-2	4) <u>S(</u> 1 S(3 S(3 S(3 S(2-19 2-20 2-21 2-22	SC-19 SC-20 SC-21 SC-22		Hor Selecte
CP-4 CP-5 CP-6 CP-7 CP-8	Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information :	Plan Testir prage Site poessing Sit nications Se System Bac System Rec	e rvices kup	P2 P1 P1 P1 P1	CP-4 Not Selected Not Selected Not Selected	CP-4 (1) 	3) CP (3) CP (2) CP (2) CP	CP-4 (1) 2-6 (1) (2 7 (1) (2 (4) 8 (1) (2 (4)	2) (3) 2) (3) 2) (3) 2) (3) 2) (3)	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) Not Selected	-1 -2 -3		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		The delete
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10	Contingency Withdrawn Alternate Sto Alternate Pri Telecommun Information : Reconstitution	Plan Testir prage Site pocessing Sit nications Se System Bac System Rec on	e rvices kup overy and	P2 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected CP-9 CP-10	CP-4 (1) — CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) CP-10 (2	(3) CP (3) CP (2) CP (CP () CP	26 (1) (2 26 (1) (2 2-7 (1) (2 (4) 2-8 (1) (2 (4) 2-9 (1) (2 (5) (2-9 (1) (2)	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3)) (4)	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1)	-1 -1 -2 -3 (2)(5		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9	Contingency Withdrawn Alternate Sto Alternate Pro Telecommun Information : Reconstitution Alternate Co	Plan Testir prage Site pocessing Sit nications Se System Bac System Rec on	e rvices kup overy and	P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected Not Selected CP-9	CP-4 (1) 	C 3) CP- (3) CP- 2) CP- - CP-	2-8 (1) (2 2-8 (1) (2 (4) 2-8 (1) (2 (4) 2-9 (1) (2 (5) (7-10 (2) (10 Selection	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) (4) cted	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4	-1 -2 -3		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-8 CP-7 CP-8 CP-9 CP-10 CP-11	Contingency Withdrawn Alternate Sto Alternate Pri Telecommun Information : Reconstitution	Plan Testir prage Site processing Sit nications Se System Bac System Rec on mmunicatio	e rvices kup overy and ns Protocols	P2 P1 P1 P1 P1 P1 P1 P1	CP-4 	CP-4 (1) — CP-8 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) CP-10 (2	C C	26 (1) (2 26 (1) (2 2-7 (1) (2 (4) 2-8 (1) (2 (4) 2-9 (1) (2 (5) (2-9 (1) (2)	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) (4) cted cted	1)	MP-3 MP-6 (1) (2) (3) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-5	-1 -1 -2 -3 (2)(5		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-9 CP-10 CP-11 CP-12 CP-13	Contingency Withdrawn Alternate Str Alternate Pri Telecommun Information 3 Information 3 Information 3 Alternate Co Safe Mode	Plan Testir orage Site occessing Site isoations Se System Bac System Rec on mmunicatio	e rvices kup overy and ns Protocols hanisms Identificat	P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0	CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected Not Selected uthentication	CP-4 (1) CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) (2 CP-9 (1) (2 CP-9 (1) (2 CP-10 (2 Not Select Not Select	C C	CP-4 (1) 2-8 (1) (2 2-7 (1) (2 (4) 2-8 (1) (2 (4) 2-9 (1) (2 (5) iP-10 (2) lot Select lot Select	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) (4) cted cted cted	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4	-1 -1 -2 -3 (2)(5		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12	Contingency Withdrawn Alternate Str Alternate Pri Telecommun Information 3 Information 3 Reconstitutio Alternate Co Safe Mode Alternative 3	Plan Testir orage Site occessing Site isoations Se System Bac System Rec on mmunicatio	e rvices kup overy and ns Protocols hanisms	P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0	CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected	CP-4 (1) CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-8 (1) (2 CP-9 (1) CP-10 (2 Not Select Not Select	C C	2-8 (1) (2 2-7 (1) (2 (4) 2-8 (1) (3 (4) 2-9 (1) (2 (5) 2-9 (1) (2 (5) 2-9 (1) (2 (5) 2-9 (1) (2) (1) (2 (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) (4) cted cted cted	1)	MP-3 MP-4 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-2 PE-3 (1) PE-4 PE-5 PE-6 (1) (4) 	-1 -2 -3 1 (2) (6)) -5 -		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-9 CP-10 CP-11 CP-12 CP-13	Contingency Withdrawn Alternate Str. Alternate Pri Telecommun Information 1 Information 1 Reconstrutic Alternative So Safe Mode Alternative S Identification Procedures	Plan Testin prage Site pocessing Sit hications Se System Bac System Bac System Rec in mmunicatio Recurity Mec and Auther and Auther	e rvices kup overy and ns Protocols hanisms Identificat dentificat	P2 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0	CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected Not Selected uthentication	CP-4 (1) 	C C	CP-4 (1) 	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) cted cted cted 2) (3)	1)	MP-3 MP-4 MP-5 (4) MP-5 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-3 (1) PE-4 PE-5 PE-8 (1) (4) 	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2	Contingency Withdrawn Alternate Six Alternate Six Information 1 Information 1 Information 2 Reconstruits Alternative S Safe Mode Alternative S Identification Procedures Identification (Organizatio	Plan Testin prage Site pocessing Sit incations Se System Bac System Recon mmunicatio incurity Mec and Auther and Auther and Auther and Auther	e nvices kup overy and ns Protocols hanisms Identificat Identification Policy an atication	P2 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected Not Selected Unit Selected IA-1	CP-4 (1) CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) (2 CP-9 (1) (2 CP-9 (1) (2 CP-10 (2 Not Select Not Select	C C	CP-4 (1) 	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) cted cted cted 2) (3)	1)	MP-3 MP-5 (4) MP-5 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-3 (1) PE-4 PE-5 (1) (4) PE-9 (1) PE-9 (1) PE-9 PE-10	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		TROUGHER
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3	Contingency Withdrawn Alternate Str. Alternate Str. Alternate Prin Telecommun Information 1 Information 1 Information 2 Reconstitution Alternate Co Safe Mode Alternate Str. Procedures Identification (Organizatio Device Ident	Plan Testin prage Site pocessing Sit incations Se System Bac System Recon mmunicatio incurity Mec and Auther and Auther and Auther and Auther and Auther and Auther and Auther	e rvices kup overy and ns Protocols hanisms Identificat dentificat	P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P0 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 	CP-4 (1) — CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) CP-9 (1) CP-10 (2 Not Select Not Select Not Select IA-1 IA-2 (1) (2) (8) (11) (1 IA-3	C C	CP-4 (1) 	2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) 2) (3) cted cted cted 2) (3)	1)	MP-3 MP-4 MP-5 (4) MP-5 (1) (2) (3) MP-7 (1) Not Selected PE-1 PE-3 (1) PE-4 PE-5 PE-8 (1) (4) 	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		10.000
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4	Confingency Withdrawn Alternate SX Alternate SX Telecommun Information 1 Information 1 Information 2 Reconstruits Alternate Co Safe Mode Alternate Co Safe Mode Alternate Co Safe Mode Alternatics Identification (Organizatio Device Identification	Plan Testin prage Site pocessing Sit incations Se System Bac System Recon mmunicatio ecurity Mec and Authen and Authen	e vivices kup vivices kup vivices start over and over and one vivice start over and the vivice start over the	P2 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P0 P0	CP-4 — Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected Not Selected Id-1 Id-2 (1) (12) Not Selected Id-4	CP-4 (1) — CP-6 (1) (CP-7 (1) (2) CP-8 (1) (1) CP-8 (1) (2) CP-9 (1) CP-9 (1) CP-10 (2 Not Select Not Select Not Select IA-1 IA-3 IA-4	CP (3) CP (2) CP (2) CP (2) CP (2) CP (4) (4)	P-4 (1)) 	(2) (2) (3) (2) (3) (2) (3) (2) (3) (1) (4) (11) (11) (11)	1)	MP-3 MP-4 MP-5(1)(2)(3) MP-7(1) Not Selected PE-1 PE-2 PE-3(1) PE-4 PE-6(1)(4) 	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		10.000
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-5	Contingency Withdrawn Alternate Str. Alternate Str. Alternate Prin Telecommun Information 1 Information 1 Information 2 Reconstitution Alternate Co Safe Mode Alternate Str. Procedures Identification (Organizatio Device Ident	Plan Testin prage Site pocessing Sit incations Se System Bac System Recon mmunicatio ecurity Mec and Authen and Authen	e vivices kup vivices kup vivices start over and over and one vivice start over and the vivice start over the	P2 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P0 P0	CP-4 	CP-4 (1) — CP-6 (1) (2 CP-7 (1) (2) CP-8 (1) (2 CP-9 (1) CP-9 (1) CP-10 (2 Not Select Not Select Not Select IA-1 IA-2 (1) (2) (8) (11) (1 IA-3	CP (3) CP (2) CP (2) CP (2) CP (2) CP (4) (4)	P-4 (1) : 	(2) (2) (2) (3) (2) (3) (2) (3) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (1) (1) (1) (1) (2) (3)	1) .ted	MP-3 MP-4 MP-5 (4) (2) (3) MP-7 (1) Not Selected PE-1 PE-4 PE-5 (1) PE-4 PE-6 (1) (4) PE-6 (1) PE-6 (1) PE-10 PE-11 (1) PE-10 PE-11 (1) PE-12 PE-13 (1) (2)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		10.000
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6	Centingency Withdrawn Alternate Six Alternate Six Telecommun Information 1 Information 1 Information 2 Information 2 Alternate Co Safe Mode Alternate Co Safe Mode Alternate Co Device Ident Identification Device Ident Identification Device Ident Identification Authenticato	Plan Testin rage Site ocessing Sit isoations Se System Bac System Rec mmunicatio iecurity Mec and Auther and Auther and Auther and Sers) ification and nagement r Managem r Feedback	e nvices kup overy and ns Protocols hanisms identificat identification dentification ntication ant identification ent	P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected CP-9 CP-10 Not Selected Not Selected Not Selected Not Selected Not Selected Not Selected Not Selected IA-1 IA-2 (1) (12) Not Selected IA-4 IA-5 IA-4	CP-4 (1) 	CP (3) CP (2) CP (2) CP (2) CP (2) CP (4) (4)		(2) (2) (2) (3) (2) (3) (2) (3) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (1) (1) (1) (1) (2) (3)	1) .ted	MP-3 MP-4 MP-5(1)(2)(3) MP-7(1) Not Selected PE-1 PE-2 PE-3(1) PE-4 PE-6(1)(4) 	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-7 CP-8 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7	Centingency Withdrawn Alternate Str Alternate Str Telecommun Information 1 Information 1 Information 2 Safe Mode Alternate Co Safe Mode Alternate Str Identification (Organizatio Device Ident Identification Device Ident Identification Corpatiographic Authenticato Cryptograph	Plan Testin rage Site coessing Sit incations Se System Bac System Bac System Recon mmunicatio ecurity Mec and Authen and Authen and Authen and Authen and Authen and Authen ragement r Managem r Paedback ic Module A	rvices kup vovery and sovery and hanisms kentificat kentification foldentification ent uthentication	P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P0 P0	CP-4 	CP-4 (1) — — — — — — — — — — — — — — — — — — —	CP. (3) CP. (3) CP. (2) CP. CP. (4) CP. (4) (3) IA- (3) IA- (3) IA-		(2) (2) (2) (3) (2) (3) (2) (3) (14) (14) (14) (14) (11) (11) (11) (11	1) .ted	MP-3 MP-6 (4) MP-6 (1) (2) (3) MP-7 (1) MP-7 (1) MP-7 (1) PE-1 PE-3 (1) PE-4 PE-3 (1) PE-4 PE-6 (1) PE-6 (1) PE-6 (1) PE-13 (1) (2) (3) (3) PE-14 (1) (2) (3)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-6 IA-7 IA-8	Configency Withdrawn Alternate Str Alternate Str Telecommun Information 1 referentiation Alternate Co Safe Mode Alternative S Identification Crganization Device Ident Identification Device Ident Identification Crganization Authenticato Cryptograph	Plan Testin rage Site prage Site prage Site sourcessing Sit inications Se System Bac System Recon- mmunicatio iecurity Mec and Authen- and Authen- r Managem r Feedback ic Module A and Authen- ic Module A and Authen- and A	orvices wup overy and ns Protocols Annisms Mentificat Noticitation Policy an tication ent uthentication uthentication	P2 P1 P1 P1 P1 P1 P1 P1 P0 P0 P0 P0 P0 P0 P0 P0 P0 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected Not Selected Not Selected IA-1 IA-2 (1) (12) IA-5 (1) (12) IA-6 IA-7 (1) (2) (3)	CP-4 (1) 	CP. CP. CP. CP. CP. CP. CP. CP.		(2) (2) (3) (2) (3) (3) (2) (3) (3) (4) (14) (14) (11) (11) (11) (11) (2) (3) (2) (3) (2) (3)	1) .ted	MP-3 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) MP-7 (1) (2) MP-7 PE-3 PE-3 MP-7 PE-3 PE-3 (1) (4) PE-12 PE-13 PE-12 PE-13 (1) (2) (3) PE-14 PE-15 (1) PE-14 PE-15 (1)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 4) <u>S(</u> 5)	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		100 00000
CP-4 CP-5 CP-5 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9	Configency Withdrawn Alternate Ste Alternate Pri Telecommun Information : Information : Information : Reconstruits Alternative S Safe Mode Alternative S Identification (Organizatio Device Ident Identification Cryptograph Identification Cryptograph Identification Cryptograph Identification Service Iden	Plan Testir prage Site processing Sit incations Se System Bac System System System Sy	e nvices kup overy and ns Protocols hanisms identification hiteation Policy an infection if Authentication ant uthentication hiteation Non- d Authentication	P2 P1 P1	CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected Not Selected Not Selected IA-1 IA-2 (1) (12) Not Selected IA-4 IA-5 (1) (11) Not Selected IA-7 IA-5 (1) (2) Not Selected IA-7 IA-5 (1) (2) IA-7 IA-5 (1) (2) IA-7 IA-5 (1) (2) IA-7 IA-5 (1) (2) IA-7 IA-5 (1) (2) IA-7 I	CP-4 (1) 	C C 3) CP-2, 3) CP C CP		(2) (2) (2) (3) (3) (3) (2) (3) (2) (3) (14) (14) (15) (11) (11) (11) (11) (11) (11) (11	1) .ted	MP-3 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) MP-7 (1) (2) MP-7 PE-3 PE-3 MP-7 PE-3 PE-3 (1) (4) PE-12 PE-13 PE-12 PE-13 (1) (2) (3) PE-14 PE-15 (1) PE-14 PE-15 (1)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 3 <u>S(</u> 3 <u>S(</u> 5 <u>S(</u> 5	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-9 CP-10 CP-10 CP-10 CP-10 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10	Configency Withdrawn Alternae St Alternae St Alternae St Alternae St Alternae Pr Telecommun Information 1 Information 1 Information 2 Safe Mode Alternative 2 Identification Proceedures Identification (Organizatio Obvice Ident Identification Authenticato Authenticato Cryptograph Identification Service Ident Adaptive Ident	Plan Testin orage Site cocessing Sit vications Se System Bac System Bac exartly Mec and Authent and Authent and Authent and Authent ification and anal Users) ification and al Users) ification and al Users)	orvices wup overy and ns Protocols Annisms Mentificat Noticitation Policy an tication ent uthentication uthentication	P2 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1 P1	CP-4 Not Selected Not Selected CP-9 CP-9 Not Selected CP-10 Not Selected uthentication IA-2 (1) (12) IA-2 (1) (12) IA-3 (1) (2) (3) IA-3 (1) (2)	CP-4 (1) 	C C 3) CP, (3) CP, CP, CP, CP, CP, CP, CP, CP,		(2) (2) (3) (2) (3) (3) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (2) (3) (11) (11) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (3) (2) (3) (3) (2) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (3) (3) (3) (3) (3) (3) (3) (3	1) .ted	MP-3 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) MP-7 (1) (2) MP-7 PE-3 PE-3 MP-7 PE-3 PE-3 (1) (4) PE-12 PE-13 PE-12 PE-13 (1) (2) (3) PE-14 PE-15 (1) PE-14 PE-15 (1)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 3 <u>S(</u> 3 <u>S(</u> 5 <u>S(</u> 5	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-5 CP-7 CP-8 CP-9 CP-10 CP-10 CP-11 CP-12 CP-13 IA-1 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9	Configency Withdrawn Alternate Ste Alternate Pri Telecommun Information : Information : Information : Reconstruits Alternative S Safe Mode Alternative S Identification (Organizatio Device Ident Identification Cryptograph Identification Cryptograph Identification Cryptograph Identification Service Iden	Plan Testin orage Site cocessing Sit vications Se System Bac System Bac exartly Mec and Authent and Authent and Authent and Authent ification and anal Users) ification and al Users) ification and al Users)	e vivices kup overy and ns Protocols hanisms identification ritication ent uthentcation ent uthentcation d Authentication d Authentication d Authentication d Authentication	P2 P1 P1	CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected Not Selected Not Selected IA-1 IA-2 (1) (12) Not Selected IA-4 IA-5 (1) (17) Not Selected IA-7 IA-5 (1) (17) Not Selected IA-7 IA-5 (1) (17) Not Selected Not Selected Not Selected Not Selected	CP-4 (1) 	C C 3) CP, (3) CP, CP, CP, CP, CP, CP, CP, CP,		(2) (2) (3) (2) (3) (3) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (2) (3) (11) (11) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (2) (3) (3) (2) (3) (3) (2) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (2) (3) (3) (3) (3) (3) (3) (3) (3) (3) (3	1) .ted	MP-3 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) MP-7 (1) (2) MP-7 PE-3 PE-3 MP-7 PE-3 PE-3 (1) (4) PE-12 PE-13 PE-12 PE-13 (1) (2) (3) PE-14 PE-15 (1) PE-14 PE-15 (1)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 3 <u>S(</u> 3 <u>S(</u> 5 <u>S(</u> 5	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		
CP-4 CP-5 CP-6 CP-7 CP-9 CP-10 CP-10 CP-10 CP-10 CP-12 CP-13 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10	Contingency Withdrawn Alternate Str Alternate Str Alternate Str Alternate Str Information 1 Information 1 Information 2 Reconstitution Alternative S Identification Device Ident Identification Corganization Device Ident Identification Corganization Sarute Alternative Identification Corganization Sarute Alternative Identification Sarute Identification Adaptive Identification	Plan Testin rrage Site cocessing Sit is cocessing Sit is source and a second second source and a second second and Auther and Auther and Auther and Auther (Testation and and Second Second Second (Testation and a second Second (Testation and a second Second (Testation and a second (Testation and (Testation and (Te	e vivices kup overy and ns Protocols hanisms identification rotocalon ent uthentcation ent uthentcation d Authentication d Authentication	P2 P1 P1 P0 P0 P0 P0 P0 P0 P0 P1	CP-4 Not Selected Not Selected CP-0 CP-10 Not Selected Not Selected Not Selected Not Selected IA-1 IA-2 (1) (12) Not Selected IA-4 IA-5 (1) (17) Not Selected IA-7 IA-5 (1) (17) Not Selected IA-7 IA-5 (1) (17) Not Selected Not Selected Not Selected Not Selected	CP-4 (1) 	C C 3) CP, (3) CP, CP, CP, CP, CP, CP, CP, CP,		(2) (2) (3) (2) (3) (3) (1) (4) (14) (14) (14) (14) (11) (11)	1) .ted	MP-3 MP-5 (4) MP-6 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) (3) MP-7 (1) (2) MP-7 (1) (2) MP-7 PE-3 PE-3 MP-7 PE-3 PE-3 (1) (4) PE-12 PE-13 PE-12 PE-13 (1) (2) PE-14 PE-14 PE-15 (1) (2) (3) PE-14 PE-15 (1)	-1 -1 -2 -3 (2) (6)) -5 -5 - - -8		4) <u>S(</u> 3 <u>S(</u> 3 <u>S(</u> 5 <u>S(</u> 5	2-19 2-20 2-21 2-22 2-22	SC-19 SC-20 SC-21 SC-22 SC-22 SC-23		

TABLE D-2: SECURITY CONTROL BASELINES

CNTL			INITIAL CONTROL BASELINES								
NO.	CONTROL NAME	PRIORITY	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	PO	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	PO	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	PO	Not Selected	Not Selected	Not Selected						
AC-24	Access Control Decisions	PO	Not Selected	Not Selected	Not Selected						
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected						

													CNTL			NTRO			PRIORTY		INITIAL	CONTROL BAS	ELINES
													NO.		cc	MIRO	LN	AME	PRIO		LOW	MOD	HIGH
													SC-2	5 75	in Nodes		_		PO	Not	Selected	Not Selected	Not Selecte
													SC-2		oneypots				P0		Selected	Not Selected	Not Selecte
													SC-2		atform-Indep	endent /	Appli	cations	PO		Selected	Not Selected	Not Selecte
													SC-2		otection of In				P1		Selected	SC-28	SC-28
										in.				1							1	t Selected	Not Selecte
											CNTL		CONTR		AME		L	INITIAL	CONTROL	BASE	ELINES	t Selected	Not Selecte
											NO.		CONTR	OL NA	AME			LOW	MOD		HIGH	t Selected	Not Selecte
										H	SA-10 D	hevelone	r Configura	tion Ma	Inement	P		Not Selected	SA-10		SA-10	t Selected	Not Selecte
										h					and Evaluation			Not Selected	SA-11		SA-11		
													hain Protec	tion		P		Not Selected	Not Sele		SA-12	t Selected	Not Selecte
						,		-			SA-13 T	rustwort	hiness			P		Not Selected	Not Sele		Not Selecter		Not Select
							CNTL						È		INITIAL CO	NTROL	BAS	ELINES	ot Sele		Not Selecter SA-15	t Selected	Not Select
							NO.		CONT	ROL	NAME		PRIORTY		w	MOD		HIGH	ot Sele	cted	58-10	t Selected	Not Select
						-													ot Sele		SA-16	SC-39	SC-39
						-	PE-17		te Work Site n of Informat		Contras Con		P2 P3	Not Se		PE-17		PE-17 PE-18	ot Sele		SA-17	t Selected	Not Select
						-			tion Leakag		system con	nponents				lot Selec		Not Selected	ot Seler		Not Selecter Not Selecter		Not Select
						1			Monitoring an		acking		PO	Not Se		lot Selec		Not Selected	ot Sele		Not Selecter	t Selected	Not Selecte
						1						1	Planning									t Selected	Not Select
										≿		INITIA	L CONTRO	LBAS	ELINES	4	_	PL-1	ot Sele		Not Selecter		Not Select
				CN	ITL O.	cor	TROL	NAME		PRIORTY	-				1	(3		PL-2 (3)	ot Sele	cied	Not Selecter		
										×.	LO	w	MO	D	HIGH		_	 PL-4 (1)	SC-1		SC-1	SI-1	SI-1
					R-3	Incident Respon	se Testin	9		P2			IR-3		IR-3 (2))		PL-4 (1)	-			SI-2 (2)	SI-2 (1) (2
					24	Incident Handlin				P1			IR-4		IR-4 (1) (-		SC-2		SC-2	-3 (1) (2)	SI-3 (1) (2
					2-5	Incident Monitor		_		P1 P1			IR-		IR-5 (1)		ted	Not Selected	ot Selei		SC-3 SC-4	(2) (4) (5)	SI-4 (2) (4)
				LIF	<-6	Incident Reporti	ng	1		_			IR-6	1)	IR-6 (1)		_	PL-8	SC-5		SC-5	SI-5	SI-5 (1)
		CNTL					E		INITIAL	cor	TROL BAS	ELINES		/	IR-7 (1)	ec	ted	Not Selected	ot Sele		Not Selecter	t Selected	SI-6
		NO.		CON	TRO	NAME	PRIORITY		low		MOD		HIGH	ted	Not Select	ted .		DC 1	-7 (3) (4) (5)	SC-7 (3) (4) (5) -7 (1) (7)	SI-7 (1) (2)
		011.0												ted	Not Select		_	PS-1 PS-2	(7) SC-8 (1)	(7) (8) (18) (2 SC-8 (1)		(7) (14)
		CM-6 CM-7	Configuration Least Fund	on Sett	angs V		P1		2M-8 2M-7		CM-6 7 (1) (2) (4)	CM-7	-6 (1) (2) (1) (2) (5)	-		-3	-	PS-2 PS-3		4		-8 (1) (2)	SI-8 (1) (2
		CM-8				nponent Inventory	P1			CM	8 (1) (3) (5)	CM-8	(1)(2)(3)	-	MA-1	4		PS-4 (2)	SC-10)	SC-10	SI-10	SI-10
					_					_		(*	4) (5)		MA-2 (2) .5		PS-5	ot Sele		Not Selecter	SI-11	SI-10
NTL					È	INITIA	L CONTR	IOL BAS	ELINES		A-9 1-10		CM-9 CM-10	(2)	MA-3 (1) (2			PS-8	SC-12	2	SC-12 (1)	SI-12	SI-12
NO.	CON	TROL N	AME		PRIOR					_	1-10		M-10	2)	MA-4 (2)			PS-7 PS-8	SC-13	3	SC-13	t Selected	Not Selecte
					_	LOW	м	OD	HIGH					·	MA-5 (1) 10		P 3-8				t Selected	Not Select
						Training					2-1	(CP-1	1	MA-8	- 1	_	RA-1	SC-16		SC-15	t Selected	Not Selecte
AT-1	Security Awarene Procedures	ess and Tr	aining Policy a	and	P1	AT-1	A	T-1	AT-1		1) (3) (8)	08.2	(1) (2) (3)	-	MP-1	-2		RA-2	ot Sele		Not Selecter		SI-16
AT-2	Security Awarene				P1	AT-2		2 (2)	AT-2 ((4)	(5) (8)		MP-2	-3		RA-3	SC-17 SC-18		SC-17 SC-18	t Selected	Not Selecte
AT-3	Role-Based Secu		9		P1	AT-3		T-3	AT-3		2-3		P-3 (1)		MP-3	-		-	SC-16		SC-19	_	
AT-4 AT-5	Security Training Withdrawn	Records		-	P3	AT-4	A	T-4	AT-4	_	4 (1)	CP-	4 (1) (2)		MP-4) (5)	RA-5 (1) (2) (4) (5)	SC-20)	SC-20		
Allo	Windrawn		Audit	t and A	Accou	ntability	· · · ·			_	(1) (3)	CP-6	(1) (2) (3)	<u>*)</u>	MP-5 (4 MP-6 (1) (2		ted	Not Selected	SC-21		SC-21	-	
AU-1	Audit and Account	tability Po	licy and		P1	AU-1	A	U-1	AU-1	_	1) (2) (3)	CP-7	(1) (2) (3) (4)	0	MP-0 (1) (2 MP-7 (1								
AU-2	Procedures Audit Events			_	P1	AU-2			AU-2 ((1)(2)		(4)	ted	Not Select		_	SA-1	SC-22	2	SC-22		
AU-2 AU-3	Audit Events Content of Audit F	Peoperie			P1 P1	AU-2 AU-3		2 (3) 3 (1)	AU-2 (AU-3 (1)		(1)(2)		(4)			_			SC-23	3	SC-23		
AU-4	Audit Storage Ca				P1	AU-4		U-4	AU-4		9 (1)	CP-9	(1) (2) (3)		PE-1	2		SA-2 SA-3	ot Sele		SC-24		
AU-5	Response to Aud	it Process	ing Failures		P1	AU-5	A	U-5	AU-5 (1)		10 (2)	CP-1	10 (2) (4)	1	PE-2	3) (9)	SA-3 SA-4 (1) (2) (9)	-				
AU-6	Audit Review, Ana	alysis, and	Reporting	T	P1	AU-6	AU-6	(1) (3)	AU-6 (1) (3) (5)				PE-3 (1			(10)					
AU-7	Audit Reduction a	nd Report	Generation	+	P2	Not Selected	AU	7 (1)	(6) AU-7 (1)	elected		Selected Selected		PE-4	-5	_	SA-5					
AU-8	Time Stamps				P1	AU-8		8(1)	AU-8 (1)	elected		Selected		PE-5	-	-		-				
Q-UA	Protection of Aud	it Informat	ion		P1	AU-9	AU	9 (4)	AU-9 (2) (3) (4)			10	PE-6 (1)	(4)	-	SA-8	1				
NU-10	Non-repudiation				P2 P3	Not Selected AU-11		elected	AU-10		i-1	1	IA-1	-	PE-8 (1) (2)	SA-9 (2)	1				
U-11 U-12	Audit Record Ret	ention			P3 P1	AU-11 AU-12		I-11 I-12	AU-11 AU-12 (1) (2) (3)	[A-2]	(1) (2) (3)		PE-9		_						
U-12 U-13	Monitoring for Info	mation (lisolosure		PO	AU-12 Not Selected		elected	Not Sele		1) (12)	(4) (8	(1) (2) (3) 3) (9) (11) (12)	1	PE-10								
U-14	Session Audit				PO	Not Selected		elected	Not Sele				(12) IA-3	1	PE-11 (1								
W-15	Alternate Audit Ca				PO	Not Selected		elected	Not Sele		-4		IA-4	3)	PE-12 PE-13 (1)								
U-16	Cross-Organizatio	onal Audit	ng		PO	Not Selected	Not S	elected	Not Sele	cted) (2) (3)	IA-5	(1) (2) (3)	3)	PE-13 (1) (3)	(2)							
CA-1	Country Ann			sessme	P1	d Authorization CA-1	c		CA-1		1)		(11) IA-0		PE-14								
	Security Assessm Policies and Proc		outorization								-7		IA-7	1	PE-15 (1								
CA-2	Security Assessm				P2	CA-2		2(1)	CA-2 (1)) (2) (3)	IA-8	(1) (2) (3)	1-	PE-16								
CA-3 CA-4	System Interconn Withdrawn	ections	_	-	P1	CA-3	CA	3 (5)	CA-3 (5)	4) elected		(4) Selected	1									
CA-4 CA-5	Plan of Action and	d Mileston	**	+	 P3	CA-5	0	 A-5	CA-5	-	elected		Selected	1									
CA-0	Security Authoriza				P2	CA-6		A-0	CA-0		elected		Selected]									
CA-7	Continuous Monit	toring			P2	CA-7		7 (1)	CA-7 (
CA-8	Penetration Testin				P2	Not Selected	Not S		CA-8		1-1		IR-1										
	Internal System C	Connection	s Config		P2 n Ma	CA-9 nagement	C	A-9	CA-9		1-2	IR-3	2 (1) (2)	1									
					n Ma	CM-1	C	W-1	CM-1		-												
CA-9	Configuration Mar						-				_												
CA-9 CM-1	Configuration Mar Procedures					CM-2		1) (3) (7)	CM-2 (1) (2) (3	0												
CA-9	Configuration Mar Procedures Baseline Configur				P1	CM-2	CM-2 (1) (3) (7)	0		·												
CA-9 CM-1	Procedures Baseline Configur	ration	rol		P1 P1	CM-2 Not Selected		-3 (2)	(7) CM-3 (1)	(2)	_												
CA-9 CM-1 CM-2 CM-3 CM-4	Procedures	ration ange Cont inalysis		+			CM		0	1)	-												

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



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 20899-8830

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	СР
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 /	Assessi	ment		
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	PO	Not Selected	Not Selected	Not Selected

FAMILY: RISK ASSESSMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:

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

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

of the risk assessment policy and associated

nization-defined frequency]; and

prganization-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
----	----------	----------	--------------

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

RA-I	Control Summary Information		
Responsible Role:			
Parameter RA-1(a)			
Parameter RA-1(b)	(1):		
Parameter RA-1(b)	(2):		
Implemented Partially implem Planned	Implementation Status (check all that apply): Implemented Partially implemented Planned Alternative implementation		
Service Provide Service Provide			

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

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

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

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

Control Enhancements: None.

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

Priority and Baseline Allocation:

P1	LOW RA-2	MOD RA-2	HIGH RA-2	57
----	----------	----------	-----------	----

ntative reviews

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

RA -2

SSP – Control Inventory Example

RA-2

	RA-2	Control Summary Information
	Responsible Role:	
SECURITY CATEGORIZATION	Implementation Stat	tus (check all that apply):
Control: The organization:	Implemented	
a. Categorizes information and the information system in accordance with applicable federal	Partially impleme	nted
laws, Executive Orders, directives, policies, regulations, standards, and guidance;	Planned	
b. Documents the security categorization results (including supporting rationale) in the security	Alternative imple	mentation
plan for the information system; and	Not applicable	
c. Ensures that the authorizing official or authorizing official designated representative reviews	Control Origination	check all that apply):
and approves the security categorization decision.	Service Provider (
	Service Provider 5	
		Hybrid (Corporate and System Specific)
	Configured by Cu	stomer (Customer System Specific)
	Provided by Custo	omer (Customer System Specific)
	Shared (Service P	rovider and Customer Responsibility)
	Inherited from pr	e-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 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]];

RA-3 RISK ASSESSMENT

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]];
- 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.

Control Ennancements. INOILE.

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

Priority and Baseline Allocation:

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

r there g the

e

ive

ion junt

on

rcing ition of c or

access

on

ilso be ecurity

of must

the 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 Role	
Parameter RA-3(b):
Parameter RA-3(c):
Parameter RA-3(d):
Parameter RA-3(ie):
Implementation	Status (check all that apply):
Implemented	
🗆 Partially imple	emented
🗆 Planned	
Alternative in	nplementation
Not applicable	e
Control Originati	on (check all that apply):
Service Provi	der Corporate
Service Provi	der System Specific
Service Provi	der Hybrid (Corporate and System Specific)
Configured b	y Customer (Customer System Specific)
Provided by (Customer (Customer System Specific)
🗆 Shared (Servi	ce Provider and Customer Responsibility)
Inherited from	n 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???