Unit #2

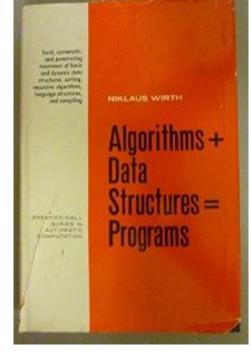
MIS5214 – Security Architecture

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 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



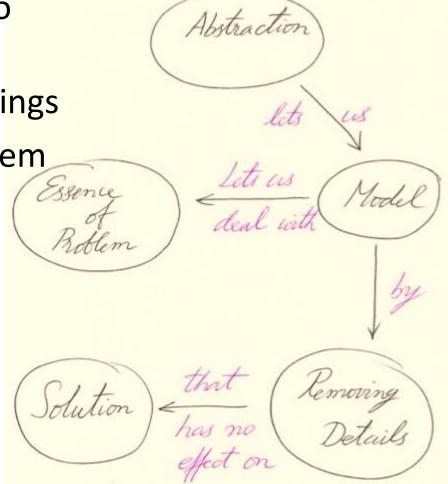
What is meant by the term "abstraction"?

 A fundamental human capability that enables us to deal with complexity

Its purpose is to limit the universe so we can do things

Selective examination of certain aspects of a problem

- Its goal is the purposeful isolation of important aspects and suppression of unimportant aspects (i.e. omitting details)
 - Purpose determines what is and what is not important
 - All abstractions are incomplete and inaccurate but this is their power and does not limit their usefulness
- Many different abstractions of the same thing are possible
 - Depending on the purpose for which they are made The problem solving context explains the source of their intent



What is a conceptual model?



- Are abstractions of things for the purpose of understanding them
- Enable dealing with systems that are too complex to understand directly
- Omit 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
- Process

System

- Aid 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
- Serve several purposes
 - Testing a physical entity before building it
 - Communicating a shared understanding of the system with stakeholders, users, developers, information system auditors and testers

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

Models are ways to describe reality

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

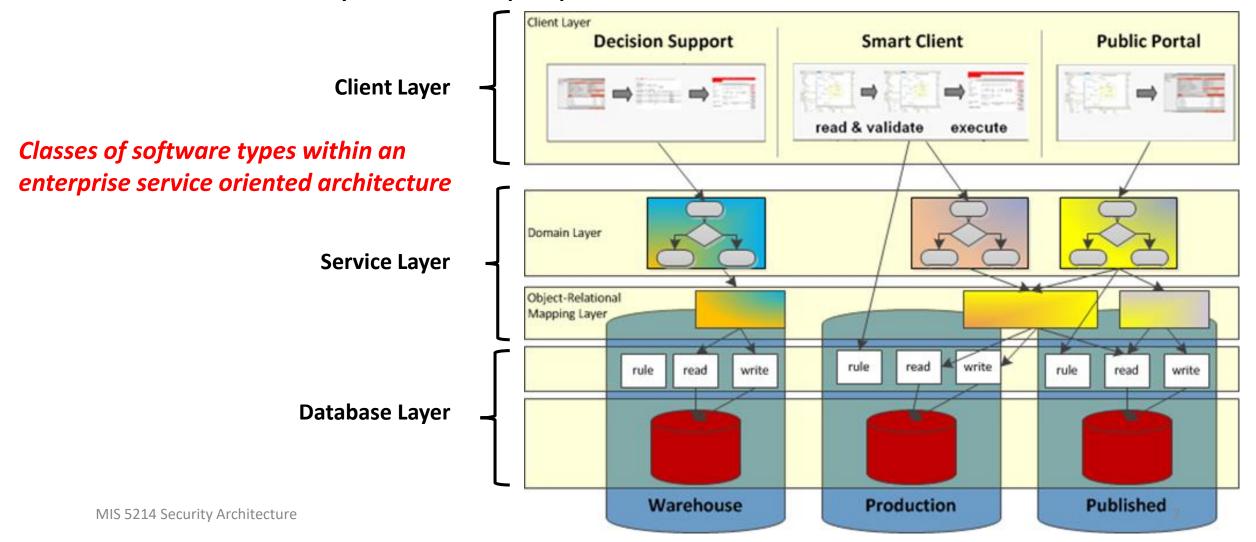
Building blocks of models is a small collection of abstraction mechanisms

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

Abstractions help the designer understand, classify, and model reality

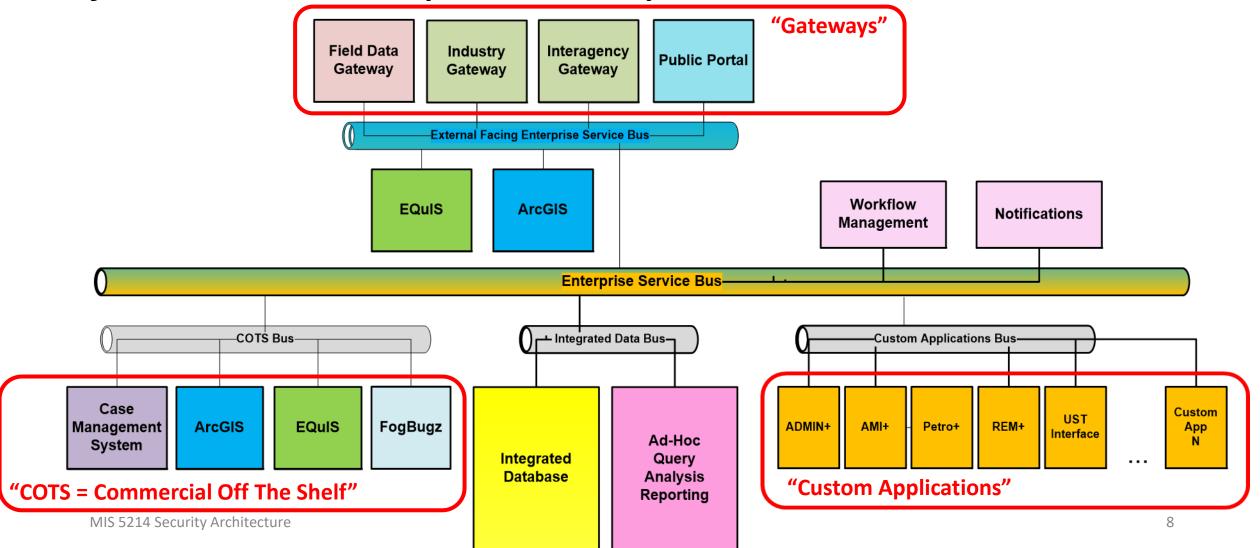
Classification

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



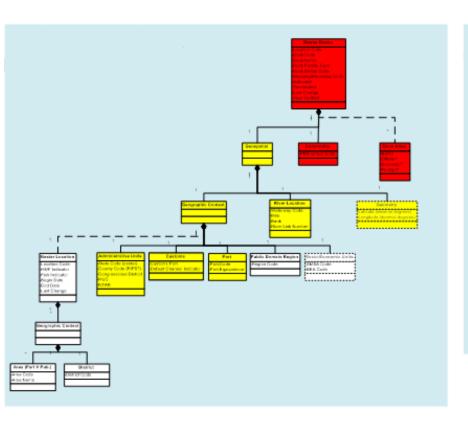
Aggregation

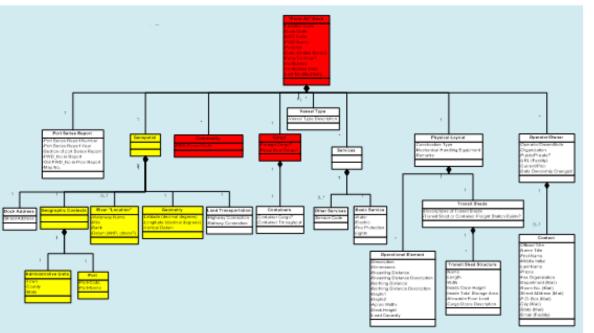
An aggregation abstraction defines a new composite class from a set of other classes that represent it components

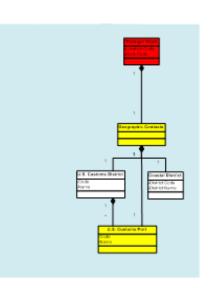


Classification and Aggregation

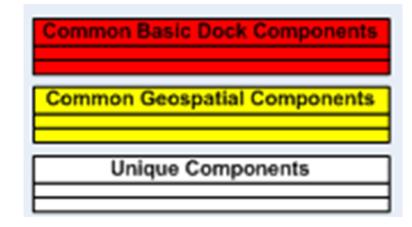
- Are the two basic abstractions used for
 - Building data structures within databases and conventional programming languages
 - Building and organizing computational processes within applications
 - Building and organizing applications within systems
 - Building and organizing minor systems and applications within major systems

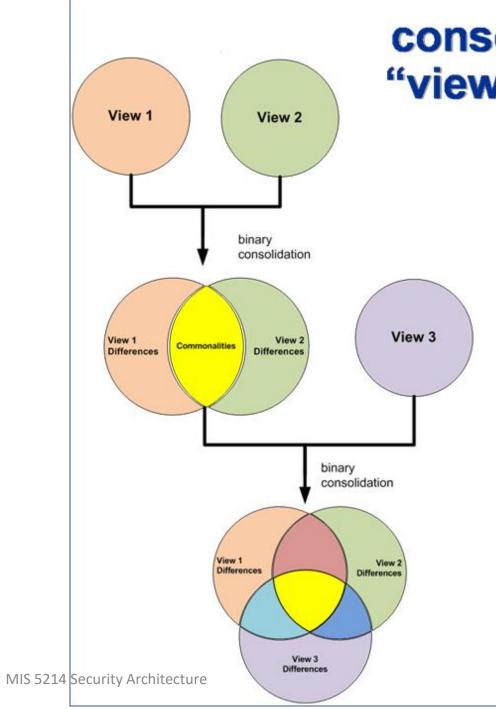






Information models from disparate business units

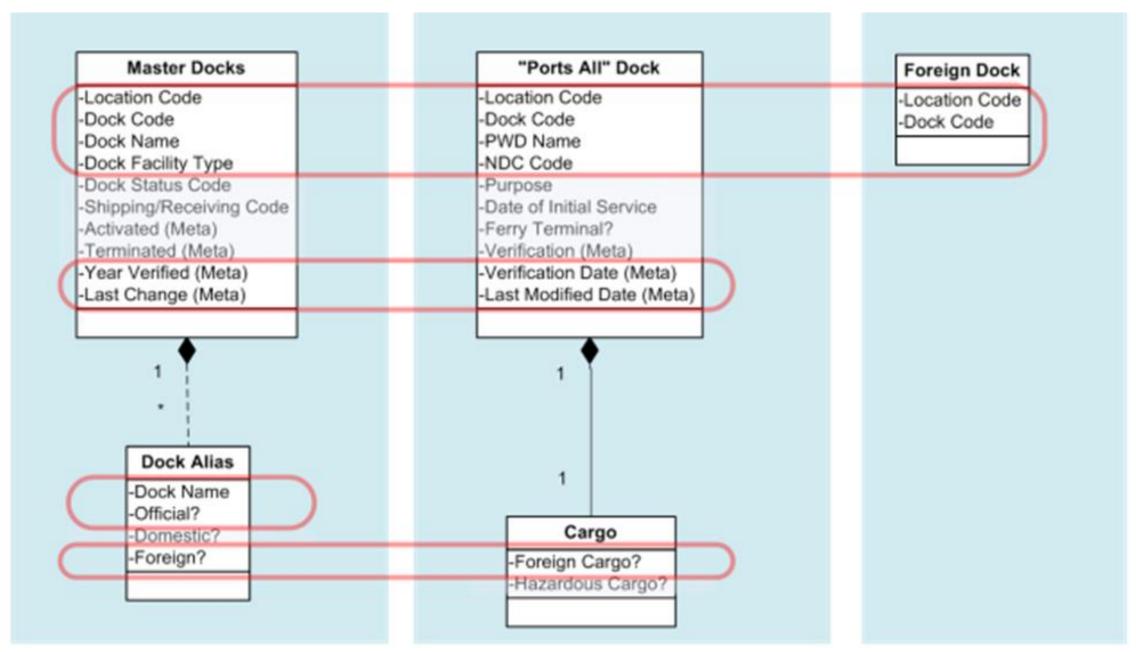


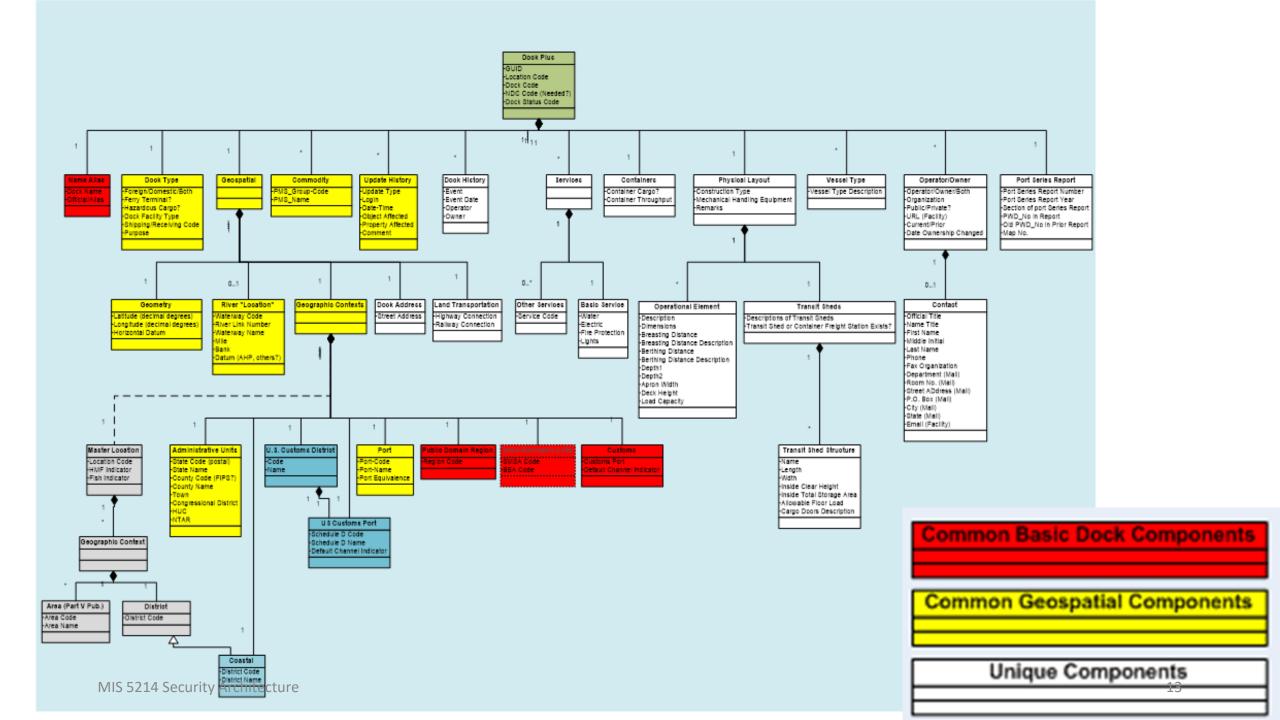


consolidation methodology "view integration"

model integration achieved by:

- Identifying,
- 2. Resolving, and
- 3. Consolidating
 - Commonalities (and synonyms)
 and
 - Differences (and homonyms)



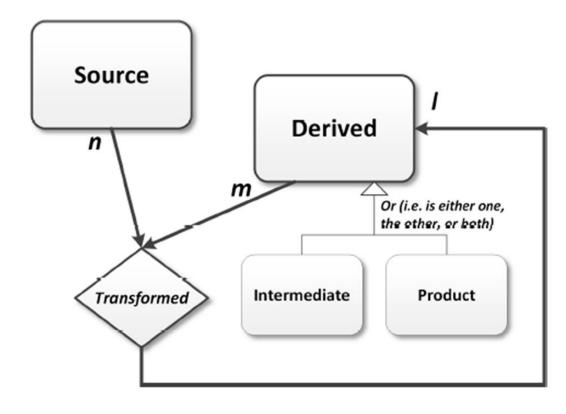


Generalization

- A generalization abstraction defines a subset relationship between elements of two more classes
- In generalization, all the abstractions defined for the generic class (super-class) are inherited by all the subset classes (sub-class)

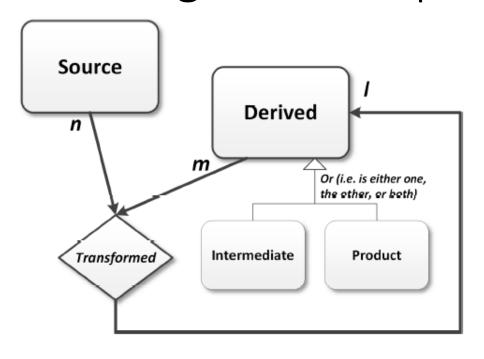
 $Datasets = \{Dataset_i : i = source, derived\},\$

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

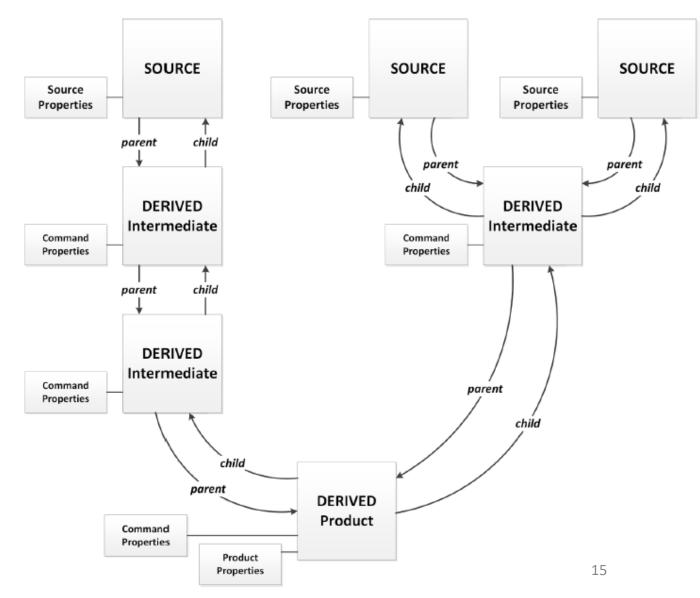


Data lineage metadata model

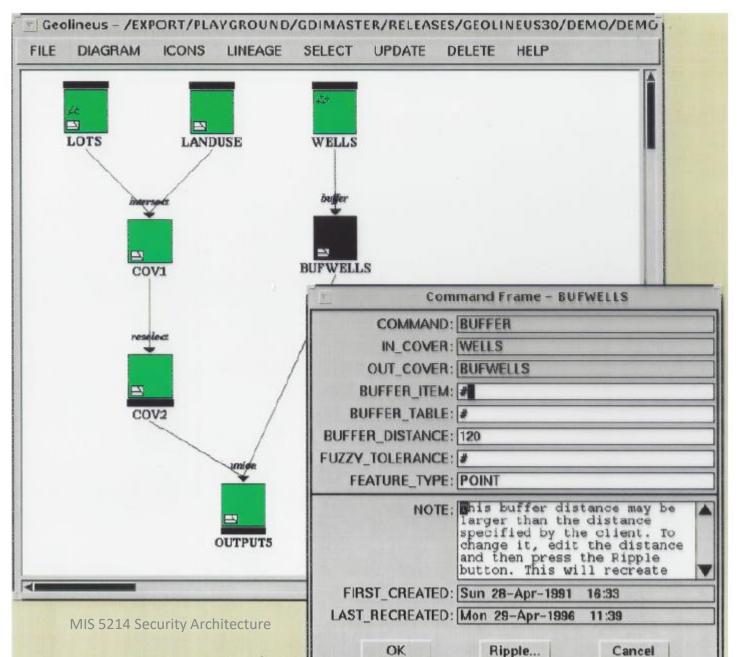
Generalization enables partitioning objects and structuring common properties and methods

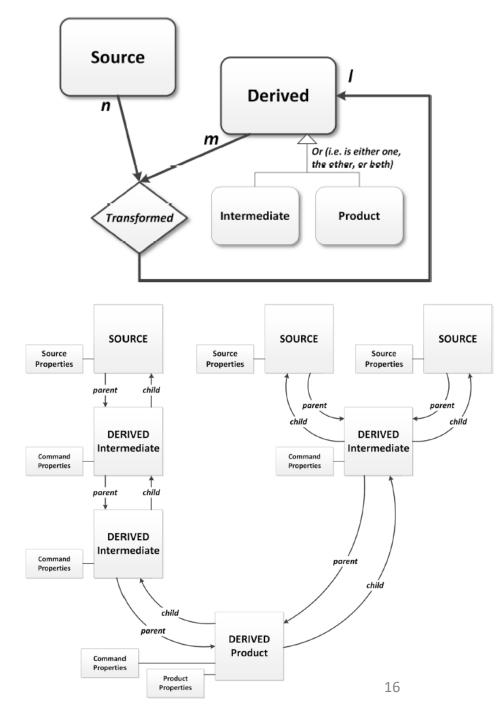


Example of generalizations of different types of datasets

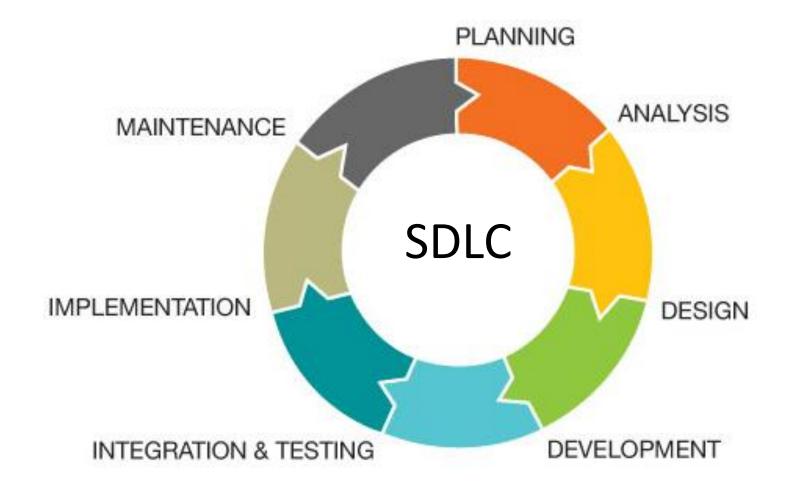


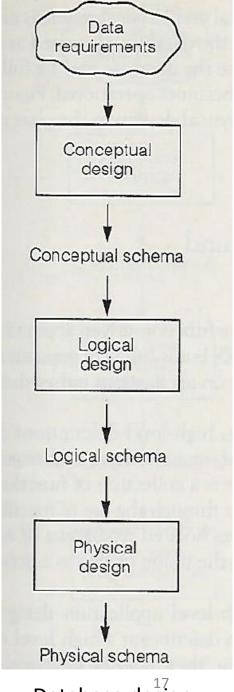
Data Lineage Metadata System





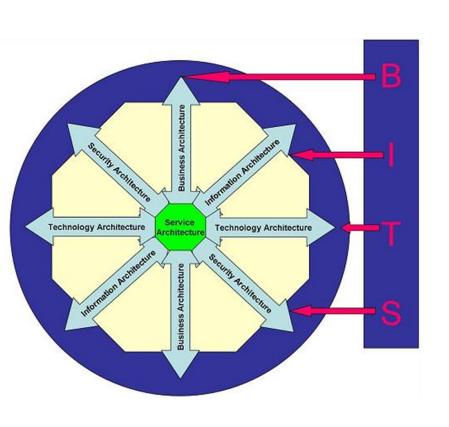
Conceptual models of information system design and development...





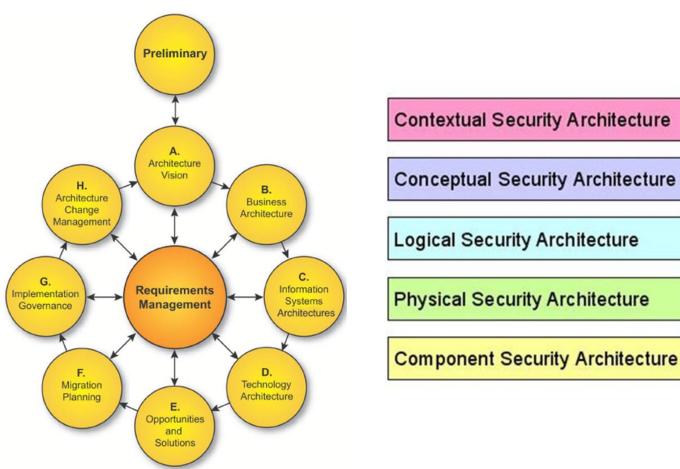
Database design

Models help us understand enterprise information systems and their security



Horatio Huxham's BITS

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



The Open Data Group Architecture Framework (TOGAF) Version 9.1

Sherwood Applied Business Security
Architecture

Operational

ഗ

ecurity

Architecture

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

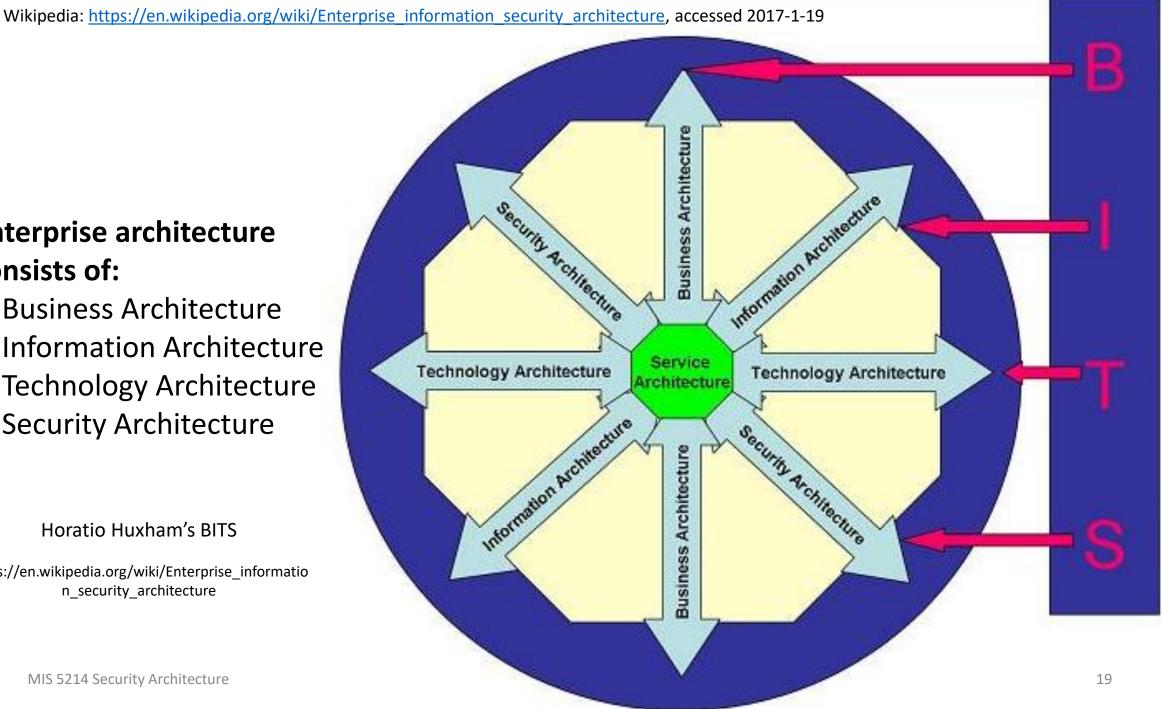
http://www.sabsa.org/white_paper

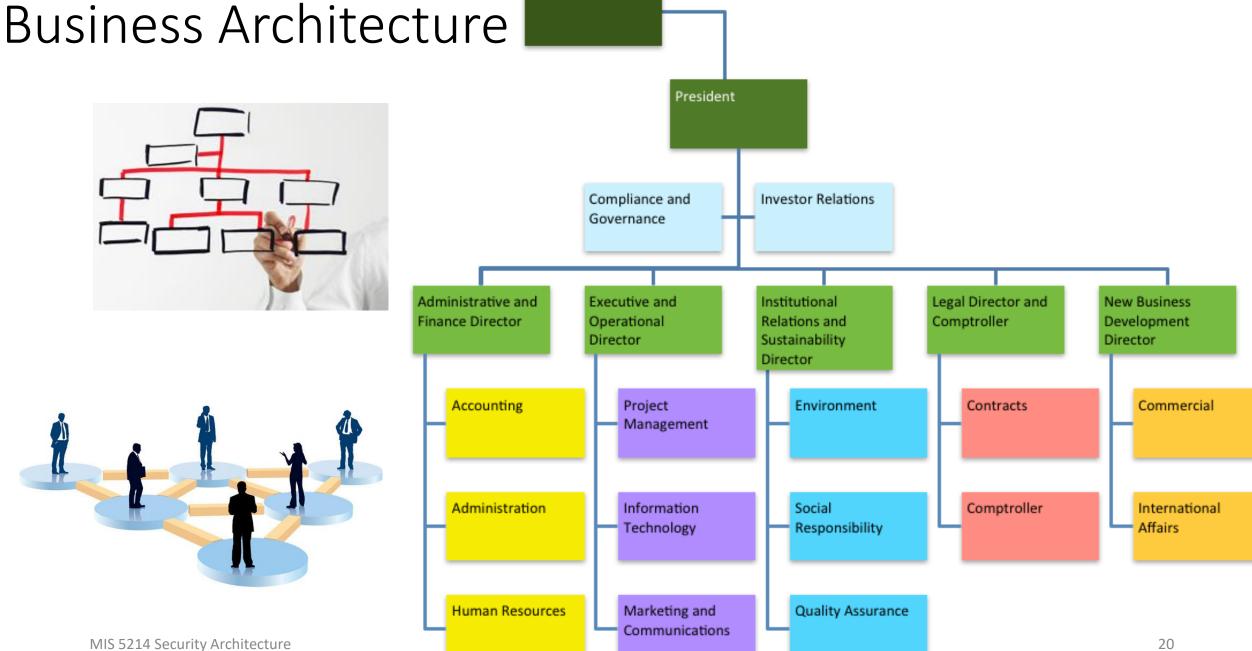
Enterprise architecture consists of:

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

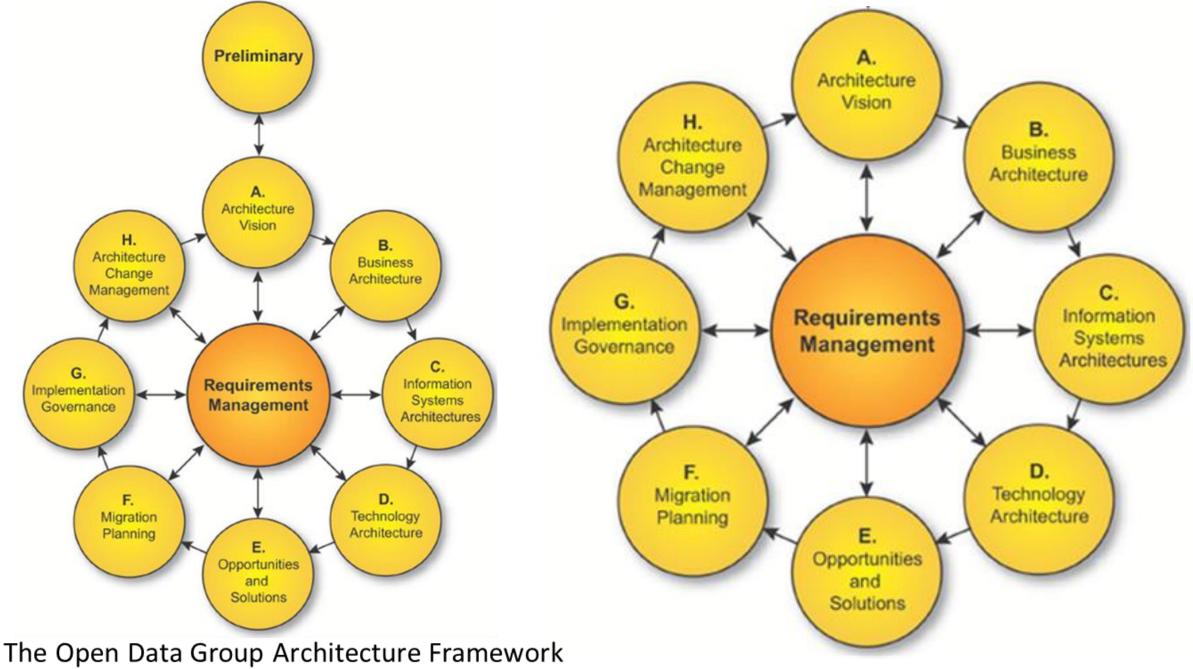
Horatio Huxham's BITS

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





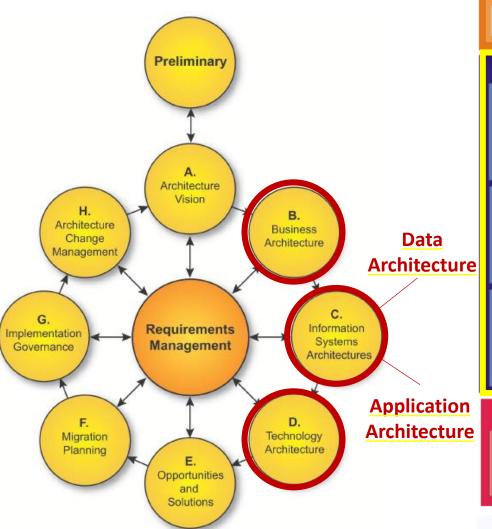
Board of Directors

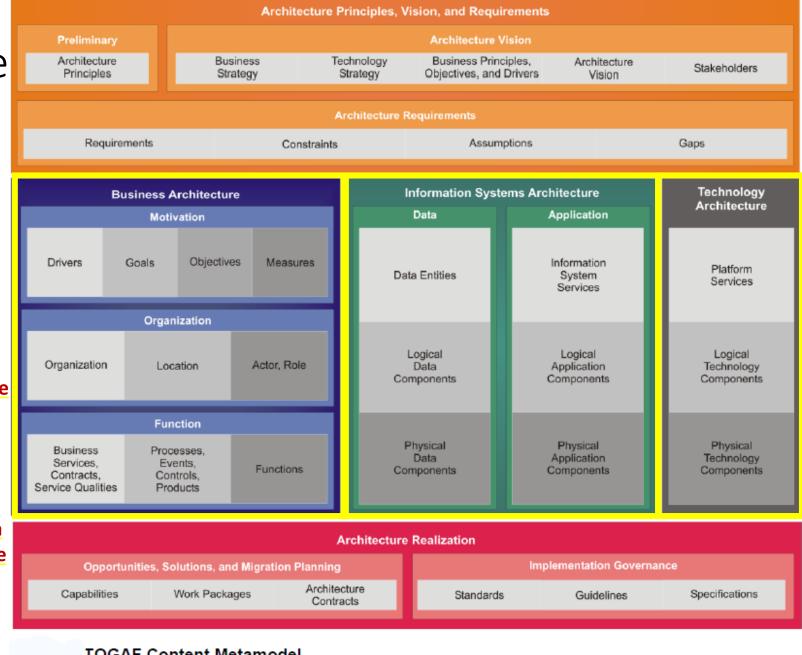


ne Open Data Group Architecture Framework

MIS 5214 Security Ar(hite AF) Version 9.1

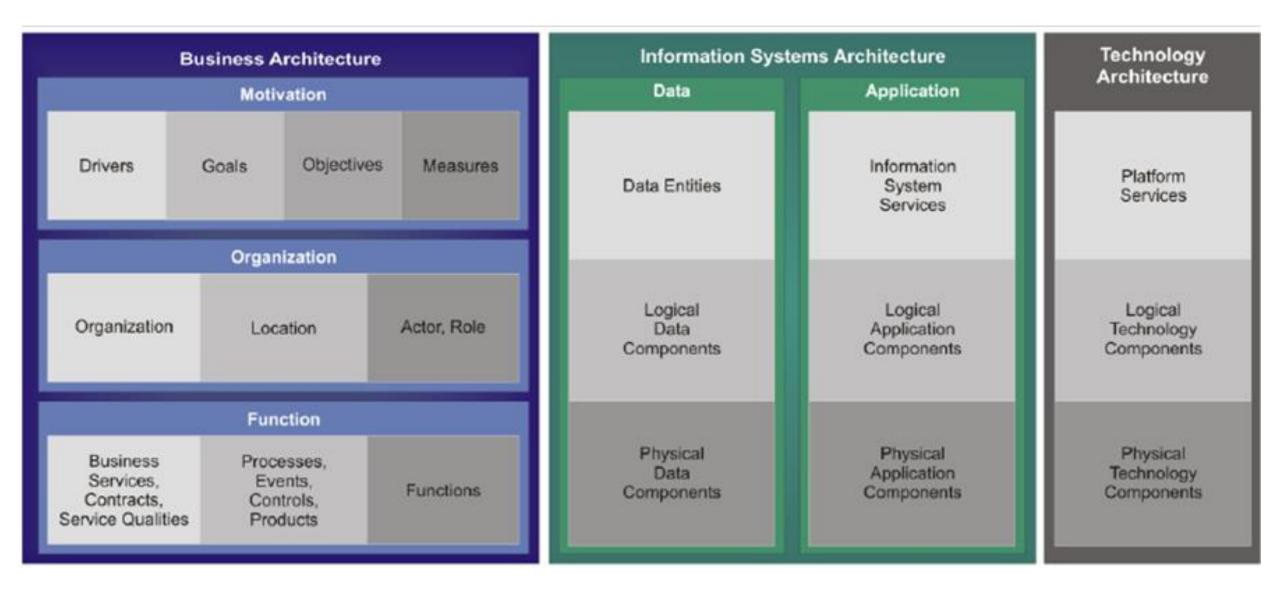
Information Architecture



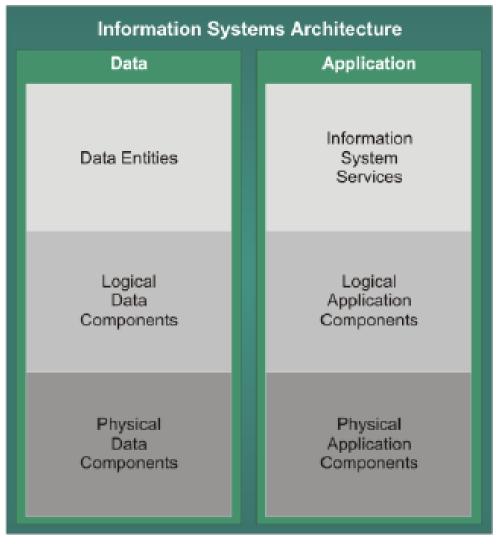


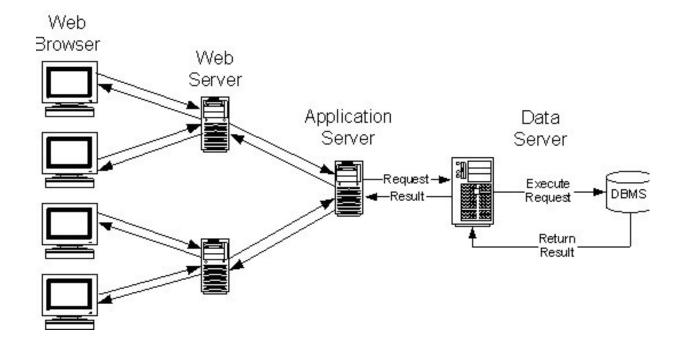
TOGAF Content Metamodel

Information Architecture



Conceptual models of Information Systems

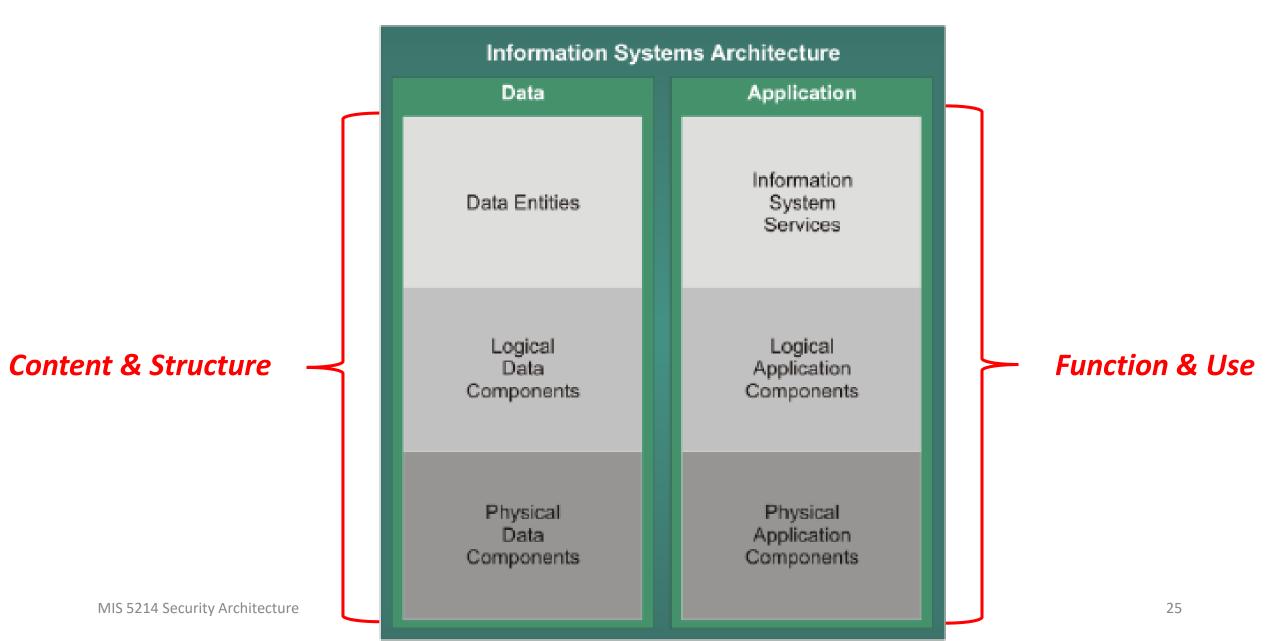




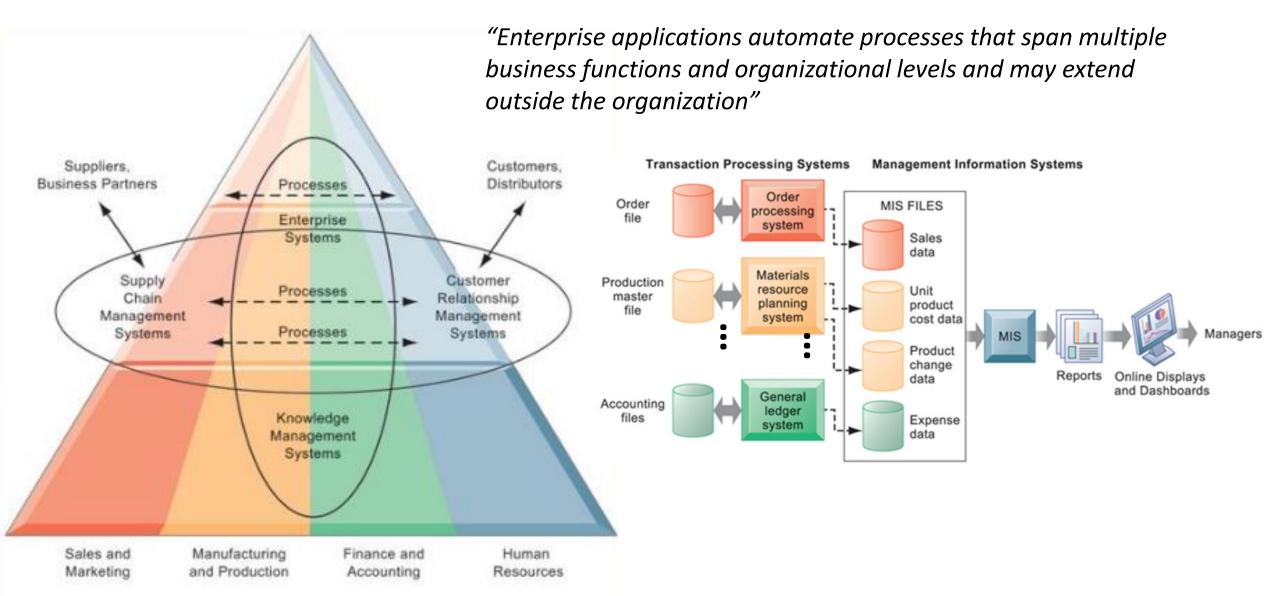
Content & Structure ecurity Architecture

Function & Use

Conceptual models of Information Systems



Information Systems – Models of Information Flows



Important Security Architecture Model:

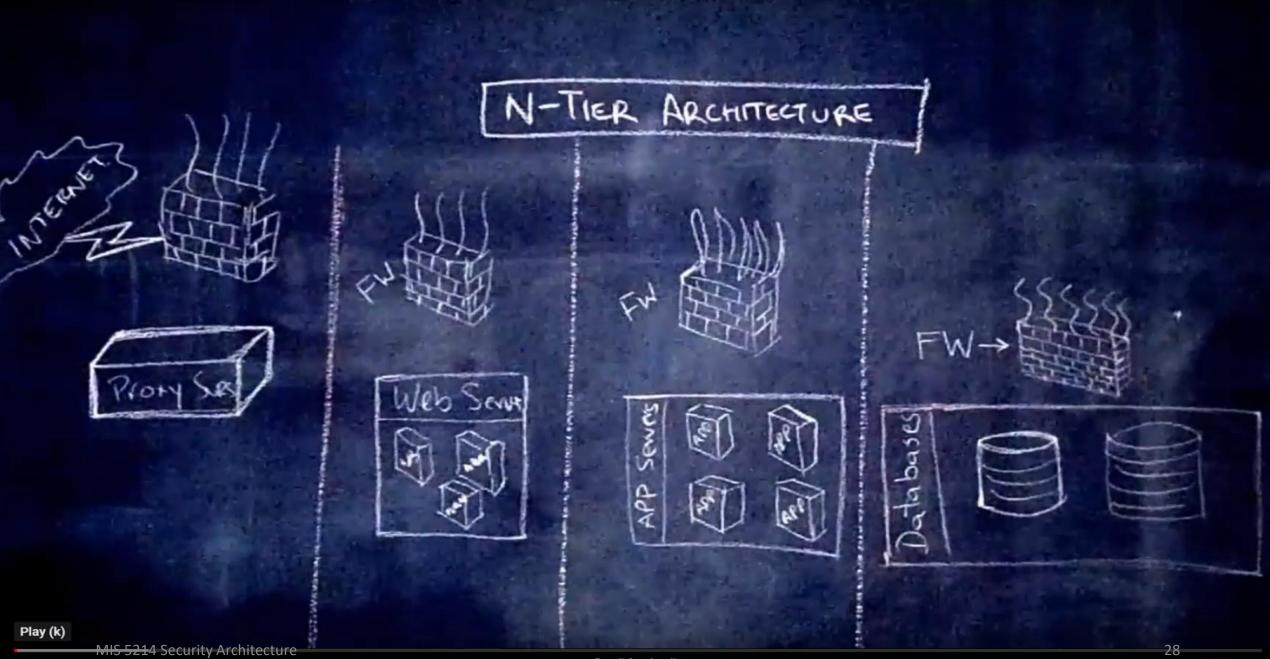
Defense in Depth

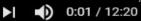
Also known as:

Layered Security

We will studying elements of layered security moving forward...



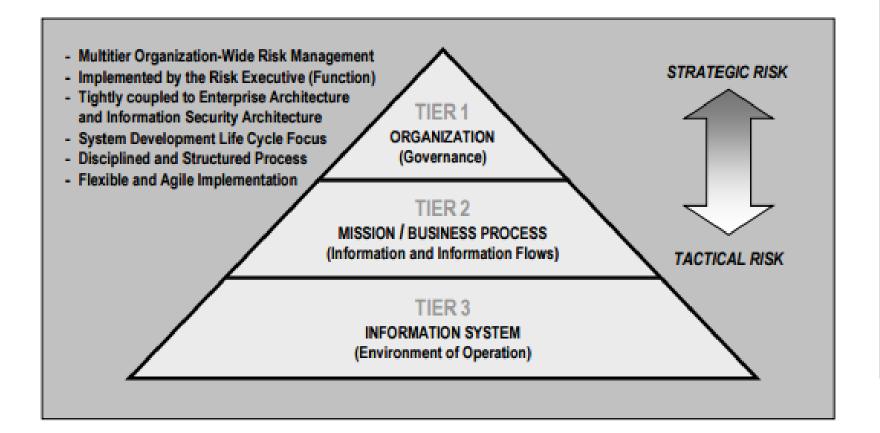




Exercise: Draw an N-Tier Architecture for a Web-Based System

- 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
- Draw an N-Tier Architecture for the web-based system

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

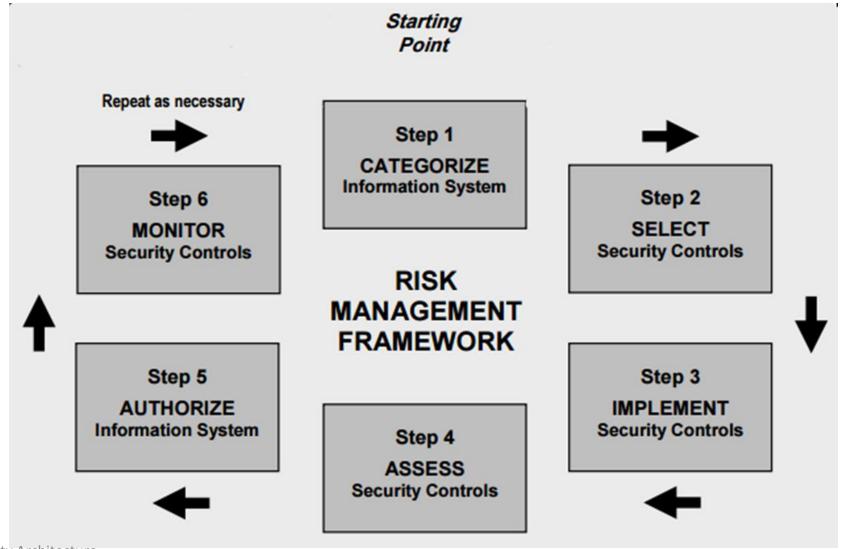
INCLUDES UPDATES AS OF 06-05-2014: PAGE IX



U.S. Department of Commerce Gary Locke, Secretary

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

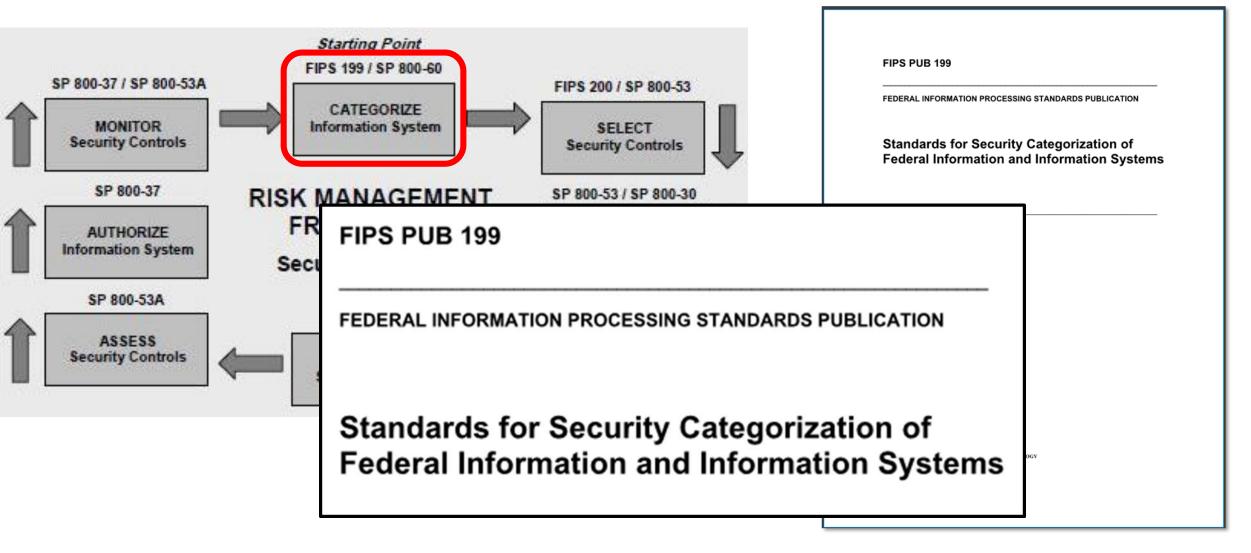
NIST Risk Management Framework



MIS 5214 Security Architecture

31

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



Transformation of ordinal qualitative risk categories to interval quantitative risk measures

Likelihood RSK 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)

01527a

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

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

Limited Treat Impact Waterability		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					

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



Lindbeed Rick 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)

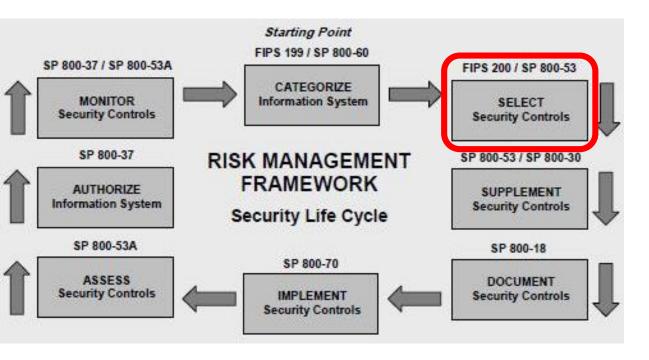
Low (1 to 10)

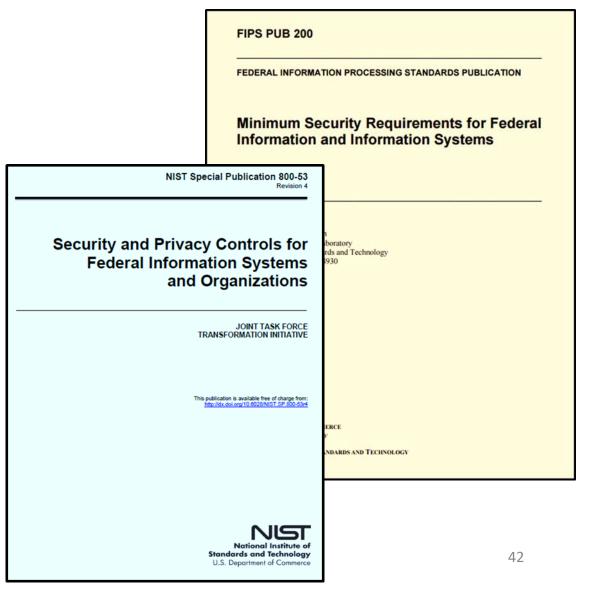
- ?

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	41 1

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



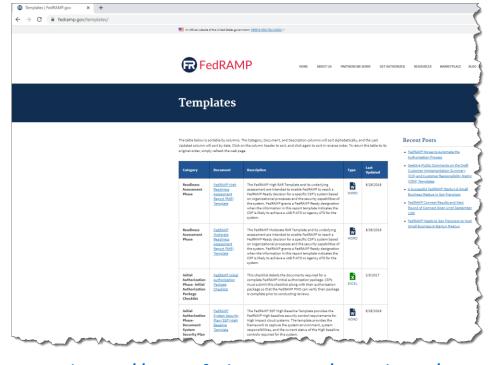


Agenda

- ✓ 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)





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

Information System Security Plan (SSP)

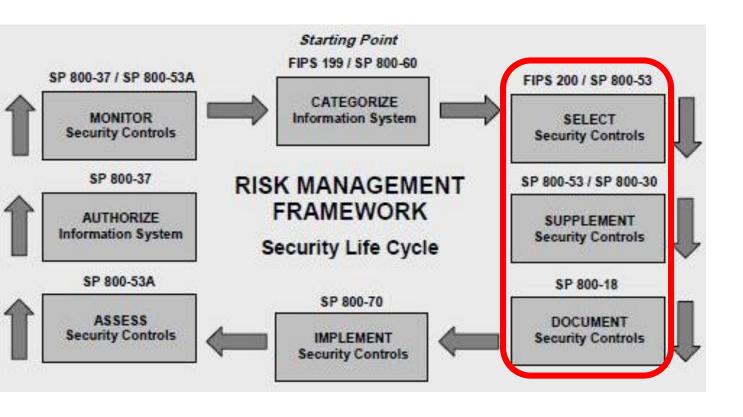




Table of Contents

1	INF	ORMATION SYSTEM NAME/TITLE1
2	INF	ORMATION SYSTEM CATEGORIZATION1
	2.1	Information Types1
	2.2	Security Objectives Categorization (FIPS 199)
	2.3	E-Authentication Determination3
3	INF	ORMATION SYSTEM OWNER4
4	AU	THORIZING OFFICIAL4
5	OTH	HER DESIGNATED CONTACTS4
6		IGNMENT OF SECURITY RESPONSIBILITY5
7		ORMATION SYSTEM OPERATIONAL STATUS6
8	INF	ORMATION SYSTEM TYPE7
	8.1	Cloud Service Models7
	8.2	Cloud Deployment Models8
	8.3	Leveraged Authorizations8
9	GEN	NERAL SYSTEM DESCRIPTION9
	9.1	System Function or Purpose9
	9.2	Information System Components and Boundaries9
	9.3	Types of Users9
	9.4	Network Architecture11
1	O SYS	TEM ENVIRONMENT AND INVENTORY11
	10.1	Data Flow
	10.2	Ports, Protocols and Services
1	1 SYS	TEM INTERCONNECTIONS
1	2 LAV	VS, REGULATIONS, STANDARDS AND GUIDANCE16
	12.1	Applicable Laws and Regulations
	12.2	Applicable Standards and Guidance
1	3 MIN	IIMUM SECURITY CONTROLS

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

FedRAMP SSP – first step: Security Objectives Categorization

Table of Contents

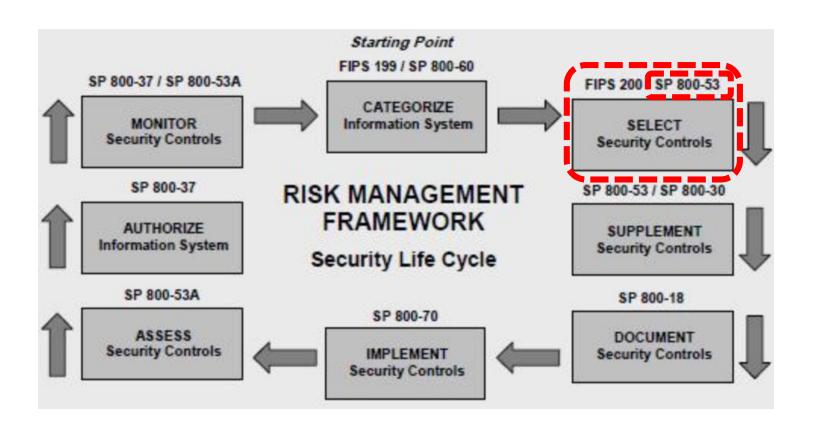
1	INF	ORMATION SYSTEM NAME/TITLE	1
2	INF	ORMATION SYSTEM CATEGORIZATION	1
	2.1	Information Types	1
	2.2	Security Objectives Categorization (FIPS 199)	3

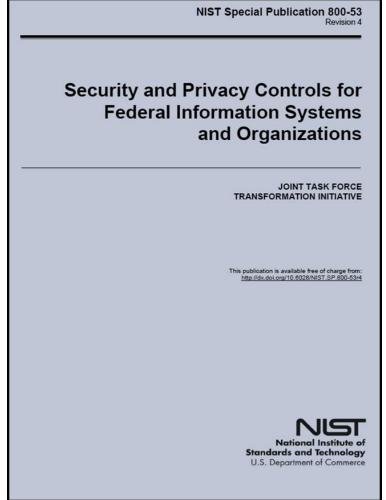
FIPS 200 Minimum Security Control Requirements

- 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





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

														CN	_					ORTY		INITIAL C	ONTROL BAS	ELINES
														N		CON	TROL	NA	ME	PRIOF		LOW	MOD	HIGH
															-	Thin Nodes Honeypots				P0 P0			Not Selected Not Selected	Not Selected Not Selected
															-	Platform-Indeper	dent Ap	plica	ations	PO	_		Not Selected	Not Selected
														sc		Protection of Info				P1	Not	Selected	SC-28	SC-28
																	2		INITIAL (ONTRO	OL BASE	ELINES	t Selected	Not Selected
												NO.		CONT	rrol	NAME	RIOR	H					t Selected t Selected	Not Selected Not Selected
																	8		LOW	MO		HIGH	t Selected	Not Selected
												SA-10		veloper Configu		Management ng and Evaluation	P1		Not Selected Not Selected	SA-		SA-10 SA-11	-	
												SA-12		pply Chain Prot		ig and Evaluation	P1		Not Selected	Not Sel		SA-11	t Selected	Not Selected
								_				SA-13		ustworthiness			P0	١	Not Selected	Not Se	lected	Not Selected	t Selected	Not Selected
									CNTL							INITIAL CON	TROL B	ASE	LINES	ot Se		Not Selected	t Selected t Selected	Not Selected Not Selected
									NO.		CONTRO	L NA	ME	RIOR		LOW	MOD	T	HIGH	ot Se	lected	SA-15	t Selected	Not Selected
									55.43											ot Se		SA-16	SC-39	SC-39
									_		te Work Site n of Information	Systen	n Comp	P2 conents P3			PE-17 Selecte	d	PE-17 PE-18	ot Se		SA-17 Not Selected	t Selected	Not Selected
											tion Leakage			P0			Selecte		Not Selected	ot Se		Not Selected	t Selected	Not Selected
									PE-20 A	sset N	Monitoring and T	racking		PO	_	Selected Not	Selecte	d	Not Selected	ot Se	lected	Not Selected	t Selected t Selected	Not Selected Not Selected
					ь									Planning			1		PL-1	ot Se	lected	Not Selected	t Selected	Not Selected Not Selected
						CNTL			TDO: NO	мп	Ì.			INITIAL CONTI	ROL BA	ASELINES	(3)		PL-1 PL-2 (3)	ot Se		Not Selected		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
						NO.		CON	TROL NA	ME	Gag		LOW	M	IOD	HIGH						60.1	SI-1	SI-1
					ŀ	IR-3	Incident R	esponse	e Testing		P	2 N	lot Sele	cted IR-	3 (2)	IR-3 (2)	(1)		PL-4 (1)	sc	-1	SC-1	01.2 (2)	CI 2 (1) (2)
						IR-4	Incident H	landling			P	1	IR-4	IR-	4 (1)	IR-4 (1) (4)				SC		SC-2	SI-2 (2) -3 (1) (2)	SI-2 (1) (2) SI-3 (1) (2)
						IR-5	Incident N				P		IR-5		R-5	IR-5 (1)	ecte	d	Not Selected	ot Se		SC-3 SC-4	(2) (4) (5)	SI-4 (2) (4) (5)
						IR-6	Incident R	eporting			P		IR-6		6 (1)	IR-6 (1)	-8		PL-8	SC		SC-5	SI-5	SI-5 (1)
				CNT		ONTRO	L NAME		YES		INITIAL CO	NTROL	L BASE	LINES		IR-8	ecte	d	Not Selected	ot Se	lected	Not Selected	t Selected	SI-6
				NO.		JNTROI	LINAME		PRIC	ı	.ow	MOD	•	HIGH	tec	_		Т	PS-1	-7 (3) (7	(4) (5))	SC-7 (3) (4) (5 (7) (8) (18) (21		SI-7 (1) (2) (5) (7) (14)
				CM-6	6 Configuration	Settings			P1	C	CM-6	CM-6	3	CM-6 (1) (2)	:tec	Not Selected	-2		PS-2	SC-8		SC-8 (1)	-8 (1) (2)	SI-8 (1) (2)
				CM-	7 Least Function	nality			P1			1-7 (1) (CM-7 (1) (2) (5			-3		PS-3					
				CM-	8 Information Sy	stem Cor	mponent Inv	entory	P1	C	CM-8 CN	N-8 (1) ((3) (5)	CM-8 (1) (2) (3 (4) (5)	3)	MA-1			PS-4 (2) PS-5	SC- ot Se		SC-10 Not Selected	SI-10	SI-10
						>		INITIAL	CONTROL	BASE	ELINES	VI-9		CM-9	(2)	MA-2 (2) MA-3 (1) (2) (3) 6		PS-6	SC-		SC-12 (1)	SI-11 SI-12	SI-11 SI-12
		CNTL NO.	con	NTROL	NAME	RIORET		- 1				1-10		CM-10	- 2)	MA-4 (2) (3)			PS-7	SC-	13	SC-13	t Selected	SI-12 Not Selected
						8	LOW	1	MOD		HIGH	1-11		CM-11		MA-5 (1)	-8	_	PS-8	-			t Selected	Not Selected
						ess and						P-1		CP-1	_	MA-6	-1	T	RA-1	SC-		SC-15	t Selected	Not Selected
		AT-1	Security Awaren Procedures	ess and	Training Policy and	P1	AT-1		AT-1		AT-1	n e	3) (8)	CP-2 (1) (2) (3	3)	MP-1	-2		RA-2	ot Se		Not Selected	SI-16	SI-16
		AT-2	Security Awaren			P1	AT-2		AT-2 (2	2)	AT-2 (2)			(4) (5) (8)	1	MP-2	-3	4	RA-3	SC-		SC-17 SC-18	t Selected	Not Selected
		AT-3	Role-Based Sec Security Training			P1 P3	AT-3		AT-3 AT-4		AT-3 AT-4	P-3		CP-3 (1) CP-4 (1) (2)		MP-3	(2)	(5)	RA-5 (1) (2) (4)	SC-		SC-19		
		TABL	E D-2: SECURI	TY CON	TROL BASELINE		A1-4		A1-4	т			•)	CP-4 (1) (2)	47	MP-4 MP-5 (4)		_	(5)	SC-	20	SC-20		
							NTROL BASELINE		1150			_	(3)	CP-6 (1) (2) (3		MP-6 (1) (2) (ecte 3)	d	Not Selected	SC-	21	SC-21		
CNTL NO.	CON	TROL NA	ME	DRITT	INITIA	LCONT	NOL BASE	LINES			AU-1	1) (2) (3)	CP-7 (1) (2) (3 (4)	- /	MP-7 (1)				SC-	22	SC-22		
NO.				8	LOW	M	IOD	н	IIGH		AU-2 (3)	(1)	(2)	CP-8 (1) (2) (3) tec	Not Selected	-1		SA-1					
			Acce	ss Con	trol						AU-3 (1) (2)	9 (1)	(4) CP-9 (1) (2) (3	3)	PE-1	-2		SA-2	SC-	23 lected	SC-23 SC-24	_	
AC-1	Access Control Pi		rocedures	P1	AC-1		C-1		IC-1	-	AU-4 AU-5 (1) (2)			(5)	_		-3	I	SA-3	0136	ecie0	30-24		
AC-2	Account Manager	nent		P1	AC-2	AC-2 ((1) (2) (3) (4)	AC-2 ((1) (2) (3) (11) (12))	AU-6 (1) (3) ((2)	CP-10 (2) (4)		PE-2 PE-3 (1)	(2) ((9)	SA-4 (1) (2) (9) (10)					
					40.7			(13)	_	(6) AU-7 (1)	ele	cted	Not Selected	_	PE-4	-5		SA-5					
AC-3	Access Enforcem		nt	P1 P1	AC-3	_	C-3 C-4		IC-3 IC-4	-	AU-7 (1) AU-8 (1)		cted cted	Not Selected Not Selected	_	PE-5				-				
AC-4 AC-5	Information Flow I Separation of Dut		in.	P1	Not Selected Not Selected		C-5		IC-4 IC-5		AU-9 (2) (3) (<u>)</u>	PE-6 (1) (4)	-8		SA-8	1				
AC-6	Least Privilege			P1	Not Selected	AC-6 ((1) (2) (5)	AC-6 ((1) (2) (3)	d	AU-10	V-1		IA-1	7-	PE-8 (1)	(2)		SA-9 (2)					
AC-7	Unsuccessful Log	on Attempt	le	P2	AC-7		(10) (C-7		9) (10) AC-7	-	AU-11 AU-12 (1) (3) (2	2) (3)	IA-2 (1) (2) (3)	PE-9		_						
AC-8	System Use Notif			P1	AC-8		IC-7		IC-7	d	Not Selected	1) ((12)	(4) (8) (9) (11 (12))	PE-10								
AC-9	Previous Logon (A	Access) No	tification	P0	Not Selected		Selected		Selected	d	Not Selected	i (-3		IA-3		PE-11 (1) PE-12								
AC-10	Concurrent Session	on Control		P3	Not Selected		Selected		C-10	d	Not Selected Not Selected		$\overline{}$	IA-4	3)	PE-13 (1) (2 (3))							
AC-11	Session Lock	ion		P3	Not Selected		-11 (1)		-11 (1)		Not Selected	11)	2) (3)	IA-5 (1) (2) (3 (11))	(3) PE-14								
AC-12 AC-13	Session Terminat Withdrawn	ruff .		P2	Not Selected	A	C-12	A	C-12		CA-1	1-6		IA-6		PE-14 PE-15 (1)								
AC-14	Permitted Actions	without Ide	entification or	P3	AC-14	A	C-14	A	C-14		CA-2 (1) (2)	1-7	2) (3)	IA-7 IA-8 (1) (2) (3		PE-16								
AC-15	Authentication Withdrawn				-						CA-3 (5)	4)		(4)										
AC-15 AC-16	Security Attributes	3		P0	Not Selected	Not S	Selected	Not S	Selected				cted cted	Not Selected Not Selected										
AC-17	Remote Access			P1	AC-17	AC-1	7 (1) (2)	AC-1	7 (1) (2)	_	CA-5 CA-6	_	cted	Not Selected										
						(3	3) (4)	(3	3) (4)		CA-0 CA-7 (1)													
AC-18	Wireless Access			P1	AC-18	AC-	-18 (1)	AC-1	8 (1) (4) (5)	d	CA-8	₹-1	$\overline{}$	IR-1										
AC-19	Access Control fo			P1	AC-19		-19 (5)	AC-	-19 (5)		CA-9	₹-2		IR-2 (1) (2)										
AC-20	Use of External In		Systems	P1	AC-20		0 (1) (2)		0 (1) (2)		CM-1													
AC-21 AC-22	Information Sharin Publicly Accessible			P2 P3	Not Selected AC-22		C-21 C-22		C-21 C-22															
AC-23	Data Mining Prote			PO	Not Selected		Selected		Selected	(7)	CM-2 (1) (2) ((7)	3)												F-0
AC-24	Access Control D			P0	Not Selected		Selected		Selected		CM-3 (1) (2))												50
AC-25	Reference Monito	r		P0	Not Selected	Not S	Selected	Not S	Selected	_	CM-4 (1)	21												
										_	CM-5 (1) (2) (0)												

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			INITIAL CONTROL BASELINES						
NO.	CONTROL NAME	PRIORITY	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	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)				

									CNT		,				È		INITIAL	. co	NTROL BASE	LINES
									NO			CONT	ROL	NAME	PRIOR		LOW		MOD	HIGH
									SC-2		hin Nodes				P0	Not	t Selected	No	ot Selected	Not Selected
									SC-2		oneypots				P0		t Selected		ot Selected	Not Selected
									SC-2		latform-In				PO		t Selected	No	ot Selected	Not Selected
									SC-2	28 P	rotection	of Inform	ation	at Rest	P1	Not	t Selected		SC-28	SC-28
													È	INITIAL	CONTRO	L BASI	ELINES		t Selected	Not Selected
							CNTL NO.		CONTI	ROL N	AME		PRIOR					=	t Selected t Selected	Not Selected Not Selected
													_	LOW	MOI		HIGH		t Selected	Not Selected
							SA-10	Developer	Configur	ation M	anagemen	t	P1	Not Selected	SA-1		SA-10			
							SA-11 SA-12	Developer Supply Ch			and Evalu	ation	P1	Not Selected Not Selected	SA-1 Not Sele		SA-11 SA-12	_	t Selected	Not Selected
								Trustworth		ction			PO	Not Selected	Not Sel		Not Selecti	ed	t Selected	Not Selected
											IMPTIA	CONTR		SELINES	ot Sele		Not Select		t Selected	Not Selected
				CNTL NO.	CON	TROL	NAME		PRIORT		INITIA	CONTR	OL BA	SELINES	ot Sele	ected	SA-15		t Selected	Not Selected
				NU.					8	L	ow	M	OD	HIGH	ot Sek	ected	SA-16	-	t Selected	Not Selected
				PE-17	Alternate Work Si	te			P2	Not S	elected	PE	-17	PE-17	ot Sele		SA-17		SC-39 t Selected	SC-39 Not Selected
				PE-18	Location of Inform		System C	omponents	P3		elected		elected	PE-18	ot Sele		Not Select		t Selected	Not Selected
				PE-19	Information Leaks				P0		elected		elected				Not Selecti		t Selected	Not Selected
			-	PE-20	Asset Monitoring	and Tr	acking		Planning	Not S	elected	Not Si	elected	Not Selected	ot Sele	ected	Not Select	ed	t Selected	Not Selected
	1												1-1	PL-1	ot Sele		Not Select		t Selected	Not Selected
		CNTL	COM	TROL N	IAME	PRIORITY		INITIAL	CONTR	UL BAS	ELINES		(3)	PL-2 (3)	ot Sel	ected	Not Select	ed		
		NO.	CON	RUL	MINE.	PRIK	ı	.ow	МС	00	н	вн							SI-1	SI-1
		IR-3	Incident Response	- Testing		P2	Not 5	Selected	IR-3	_		3 (2)	(1)	PL-4 (1)	SC-	1	SC-1			
		IR-4	Incident Handling	resurg		P1		R-4	IR-4	(1)	IR-4	(1) (4)	<u> </u>	-	SC-	2	SC-2		SI-2 (2)	SI-2 (1) (2)
		IR-5	Incident Monitoring	9		P1		R-5	IR-			5 (1)	lected	Not Selected	ot Sele		SC-3		(2) (4) (5)	SI-3 (1) (2) SI-4 (2) (4) (5)
		IR-8	Incident Reporting			P1		R-8	IR-6	(1)		3 (1)	-8	PL-8	SC-		SC-4	_	SI-5	SI-4 (2) (4) (5) SI-5 (1)
				<u> </u>	INITIA	L CON	TROL B	ASELINES)		7 (1)	lected		SC- ot Sele		SC-5 Not Selecti		t Selected	SI-6
CNTL NO.	С	ONTROL	. NAME	PRIORTY						ted		l-8 elected			-7 (3)		SC-7 (3) (4)		-7 (1) (7)	SI-7 (1) (2) (5)
					LOW		MOD	н	IGH	ted		elected	-1	PS-1	(7)		(7) (8) (18) (21)		(7) (14)
CM-6	Configuration			P1	CM-6		CM-6		3 (1) (2)				-2	PS-2 PS-3	SC-8	(1)	SC-8 (1)	_	-8 (1) (2)	SI-8 (1) (2)
CM-7 CM-8	Least Function			P1	CM-7 CM-8		(1) (2) ((1) (2) (5)				-3	PS-4 (2)	SC-1	0	SC-10	-		
CM-8	Information S	lystem Con	ponent Inventory	PI	CM-8	CM-	3 (1) (3) ((1) (2) (3) (5)	_	M	2 (2)	-5	PS-5	ot Sele		Not Selecti	ed	SI-10	SI-10
CM-9	Configuration			P1	Not Selected		CM-9		M-9	(2)) (2) (3)	-6	PS-6	SC-1	2	SC-12 (1)	SI-11 SI-12	SI-11 SI-12
CM-10	Software Usa		ions	P2 P1	CM-10 CM-11				M-10	2)		(2) (3)	-7	PS-7	SC-1	2	SC-13	-	t Selected	Not Selected
CM-11	User-Installed	Software	Contin	gency P		-	CM-11	CI	M-11	-		5 (1)	-8	PS-8	301			\dashv	t Selected	Not Selected
CP-1	Contingency	Planning P		P1	CP-1		CP-1		P-1	1_	M	1-8		RA-1	SC-1	15	SC-15		t Selected	Not Selected
	Procedures									-			-2	RA-2	ot Sele		Not Select	ed	SI-16	SI-16
CP-2	Contingency	ncy Plan		P1	CP-2		2 (1) (3) (8) CP-2 ((4)	CP-2 (1) (2) (3) (4) (5) (8)		MP-	-1	-3	RA-3	SC-1		SC-17 SC-18		t Selected	Not Selected
CP-3	Contingency			P2	CP-3		CP-3		-3 (1)		M	0.3	-	_	20.1		SC-18	-		
CP-4 CP-5	Contingency	Plan Testir	g	P2	CP-4	C	P-4 (1)	CP-4	(1)(2)	4=	M		(2) (5	5) RA-5 (1) (2) (- (5)	4) SC-2		SC-20			
CP-6	Withdrawn Alternate Sto	rano Cito		P1	Not Selected	-	-6 (1) (3)	CDA	1) (2) (3)	1)		5 (4)	lected					_		
CP-7	Alternate Pro		0	P1	Not Selected		(1)(2)(3) CP-7 (1) (2) (3)	1)		7 (1)	-		SC-2		SC-21			
				P1		L.,			(4)	ted	Not S		-1	SA-1	SC-2	2	SC-22			
CP-8	Telecommuni	ications Se	rvices	P1	Not Selected	CP	48 (1) (2)		(1) (2) (3) (4)				_		SC-2	3	SC-23			
CP-9	Information S	ystem Bac	kup	P1	CP-9	C	P-9 (1)	CP-9 ((1) (2) (3) (5)		PI	-1	-2	SA-2	ot Sele		SC-24			
CP-10	Information S	ystem Rec	overy and	P1	CP-10	0	P-10 (2)		0 (2) (4)	1-	PI	-2	-3	SA-3 () SA-4 (1) (2) (1	2)					
	Reconstitution	n				_				-	PE-	_	1)	(10)	,					
CP-11 CP-12	Alternate Cor Safe Mode	mmunicatio	ns Protocols	P0	Not Selected Not Selected		Selecter		elected elected	1=		-4	-5	SA-5						
CP-13	Alternative Se	ecurity Med	hanisms	PO	Not Selected		Selecter		elected	0	PE e	(1) (4)	-	+ -						
				n and A	uthentication					<u>"</u>	PE-0	(1) (4)	-8	SA-8						
IA-1	Identification Procedures	and Auther	ntication Policy and	P1	IA-1		IA-1	L	A-1	1-	PE-	B (1)	(2)	SA-9 (2)						
IA-2	Identification	and Auther	ntication	P1	IA-2 (1) (12)	IA-2	(1) (2) (3) IA-2 (1) (2) (3)		PE]							
	(Organization	al Users)			.,,,	(8)	(11) (12)	(4) (8)	(9) (11) 12)	_		-10	-							
IA-3	Device Identi	fication and	Authentication	P1	Not Selected		IA-3		A-3	1.—	PE-	1 (1)	1							
IA-4	Identifier Man			P1	IA-4		IA-4		A-4	3)		(1) (2)	1							
IA-5	Authenticator	Managem	ent	P1	IA-5 (1) (11)	IA-5	(1) (2) (3 (11)	IA-5 (1) (2) (3) 11)	-	(3)	1							
IA-6	Authenticator	Feedback		P2	IA-6		IA-6		A-8	1-	PE		-							
IA-7	Cryptographic			P1	IA-7		IA-7	l l	A-7	1—	PE-		1							
IA-8	Identification Organization	and Auther		P1	IA-8 (1) (2) (3)	IA-8	(1) (2) (3	B) IA-8 (1) (2) (3)	ľ	PE	-10	J							
IA-9			d Authentication	PO	Not Selected	Not	Selected	Not 9	(*) Selected	1										
IA-10	Adaptive Iden	tification a	nd Authentication	PO	Not Selected	Not	Selected	i Not S	elected	1										
IA-11	Re-authentica	ation		P0	Not Selected	Not	Selected	Not S	elected	4										
IR-1	Incline F			lent Res	ponse IR-1		IR-1		R-1	-										
IR-1 IR-2	Incident Resp		y and Procedures	P1	IR-1 IR-2		IR-1		R-1 (1) (2)	Н										
				1.2	11174	_		1112	(1)(4)	-										

TABLE D-2: SECURITY CONTROL BASELINES 32

CNTL		PRIORITY	INITIAL CONTROL BASELINES					
NO.	CONTROL NAME	PRIOR	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			

																		 		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	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-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	Н.	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 (4) (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-2		SC-23			
AU-4 AU-5	Audit Storage Ca Response to Aud			P1	AU-4 AU-5	AL AL		AU-5 (1			((5)			-3		SA-3	ot Sele	ected	SC-24			
AU-8	Audit Review, An			P1	AU-6	AU-6		AU-6 (1)		10 (2)	CP-10	0 (2) (4)	_	PE-2 PE-3 (1)	(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	PO	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		20	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	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													

AC-1

NIST Special Publication 800-53

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/10.8028/NIST.SP.800-53r4



FAMILY: ACCESS CONTROL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:

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

Supplemental Guidance: This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1 LOW AC-1 MOD AC-1 HIGH AC-1 53	Р
-----------------------------------	---

Control Family: Access Control

How many access controls are relevant to the web-based system you began designing for managing the data of public utilities for the small town?

NIST Special Publication 800-53

Revision 4

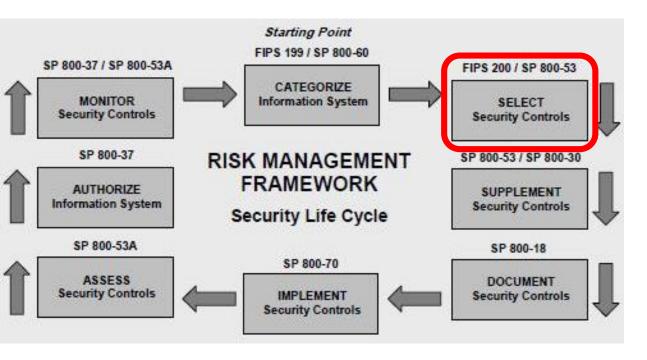
Security and Privacy Controls for Federal Information Systems and Organizations

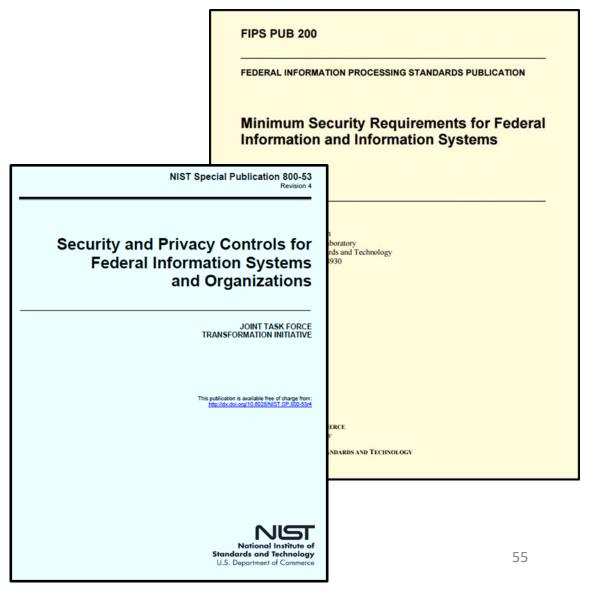
JOINT TASK FORCE TRANSFORMATION INITIATIVE

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



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





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

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 /	\ssessi	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	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:

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

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

scope, roles, responsibilities, rganizational entities, and compliance;

risk assessment policy and associated

n-defined frequency]; and zation-defined frequency].

iment of policy and procedures for the control enhancements in the RA family. cutive Orders, directives, regulations, es and procedures at the organization procedures unnecessary. The policy can icy for organizations or conversely, can nature of certain organizations. The general and for particular information

systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30, 800-100.

Priority and Baseline Allocation:

P1 LOW RA-1 MOD RA-1 HIGH RA-1 59

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 60
----	----------	----------	--------------

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.

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.	Security Objectives Categorization (FIPS 199)
3.	INFORMATI	ON SYSTEM OWNER4
4.	AUTHORIZI	NG OFFICIALS4
5.	OTHER DES	IGNATED CONTACTS4
6.	ASSIGNMEN	NT OF SECURITY RESPONSIBILITY5
7.	INFORMATI	ON SYSTEM OPERATIONAL STATUS6
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 Purpose9
	9.2.	Information System Components and Boundaries9
	9.3.	Types of Users
	9.4.	Network Architecture
10.	SYSTEM EN	VIRONMENT AND INVENTORY12
	10.1.	Data Flow
	10.2.	Ports, Protocols and Services
11.	SYSTEM INT	TERCONNECTIONS
12.	LAWS, REGI	ULATIONS, STANDARDS AND GUIDANCE17
	12.1.	Applicable Laws and Regulations
	12.2.	Applicable Standards and Guidance
12	MINIMIM	SECURITY CONTROLS 18

System Security Plan and FIPS 199, FIPS 200 and SP800-53...

L4.	ACRONYMS		392
L5.	ATTACHMENTS.		393
	Attachment 1	Information Security Policies and Procedures	395
	Attachment 2	User Guide	396
	Attachment 3	Digital Identity Worksheet	397
	Introductio	on and Purpose	397
	Informatio	n System Name/Title	397
	Digital Ider	ntity Level Definitions	397
	Review Ma	ximum Potential Impact Levels	398
	Digital Ider	ntity Level Selection	399
	Attachment 4	PTA/PIA	400
	Privacy Ove	erview and Point of Contact (POC)	400
		cable Laws and Regulations	
		cable Standards and Guidance	
		nally Identifiable Information (PII)eshold Analysis	
	_	fying Questions	
		nation	
		Rules of Behavior	
	Attachment 6	Information System Contingency Plan	404
	Attachment 7	Configuration Management Plan	405
	Attachment 8	Incident Response Plan	406
	Attachment 9	CIS Workbook	407
	Attachment 10	FIPS 199	408
	Introductio	n and Purpose	408
	Scope 4	08	
	System Des	scription	408
	Methodolo	gy	409
	Attachment 11	Separation of Duties Matrix	411
	Attachment 12	FedRAMP Laws and Regulations	412
	Attachment 12	FodPAMD Inventory Workhook	//42

SSP – Control Inventory Example

Control Class	Control Family	Implemented	Partial	Planned	Alternate	NA	System	Empty	FedRamp	Investment
	Risk Assessment	2	5	1	2	1	11		10	110%
Management		1	2	1	_		4	2	6	67%
	System & Service Acquisition		_				Ö	22	22	0%
Management					1		1	14	15	7%
Technical	Identification & Authentication	9	3	8		9	29		27	107%
Technical	Access Control	4	3	28	1	13	49		43	114%
Technical	Audit & Accountability	1	3	13		4	21		19	111%
Technical	System & Communication Protection	17	8	9	1	5	40		32	125%
Operational	Personnel Security	6	1			2	9		9	100%
Operational	Physical & Environmental Protection					19	19	1	20	95%
Operational	Contingency Planning	1	2	24			27		24	113%
Operational	Configuration Management	8	6	11		5	30	1	26	115%
Operational	Maintenance						0	11	11	0%
Operational	System & Information Integrity		5	16		8	33		28	118%
Operational	Media Protection	2				3	5	7	10	50%
Operational	Incident Response						0	18	18	0%
Operational	Awareness & Training			5			5		5	100%
	Total:	55	38	116	5	69	283	76	325	87%

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 of security control families

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 of security control families
- Bonus: Threat Modeling exercise...

STRIDE

Threat model created by Microsoft, based 6 categories of threats:

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

STRIDE threats and desired properties they impact

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

<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

Break up into groups of 2 or 3:

- Pretend you are security professionals
 - A car company tasked you with thinking through the security implications of the modern car computer systems
- Start with the blue suit of cards ("Human Impact"), consider what impacts to people would result if an attacker misused modern car systems like the attack you just witnessed
 - Either think about one car, or think about the entire car product line
 - Rank order the cards from most relevant
 - Explain your 3 top choices

University of Washington Security Cards

A security threat brainstorming activity

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

University of Washington Security Cards

A security threat brainstorming activity

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

STRIDE Threat 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
 - Either think about one car, or think about the entire car product line
 - Rank order the threats from most relevant
 - Explain your 3 top choices

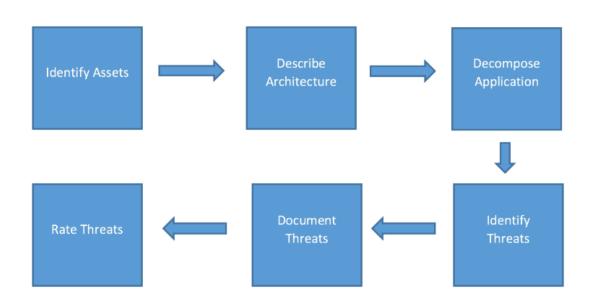
Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

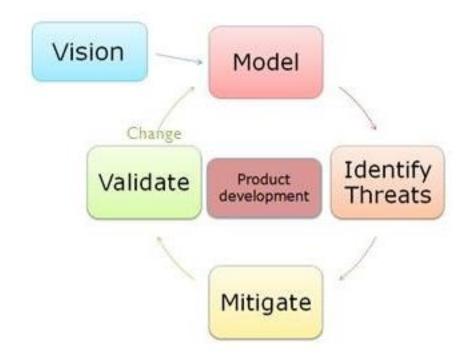
Threat Modeling

• Can be a full-time job for cyber security professionals

• Is now a skill information systems designers, developers and

architects need to have





Agenda

- ✓ 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
- ✓ Bonus: Threat Modeling exercise...