Managing Enterprise Cybersecurity MIS 4596

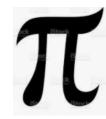
Class 3

1

Agenda

- Quiz: 100 digits of Pi
- National Institute of Standards and Technology (NIST)
 - Cybersecurity Framework
 - Risk Management Framework
- Applying the NIST Risk Management Framework
- Milestone 1 Assignment

Quiz



You have five minutes to write out the first 100 digits of pi, from memory, on a sheet of paper

• You need to close your laptop and put your phone face down on the table or away in your bag or pocket

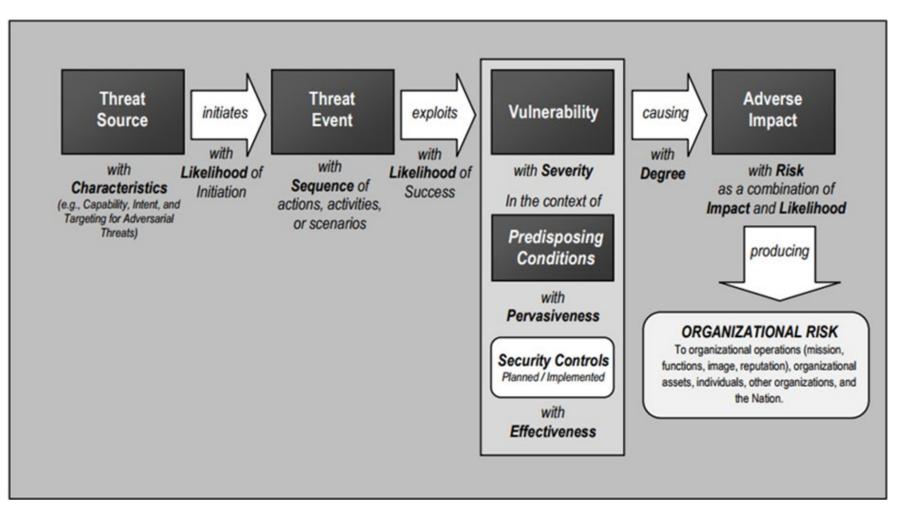
Goal: Help you develop a Security Mindset

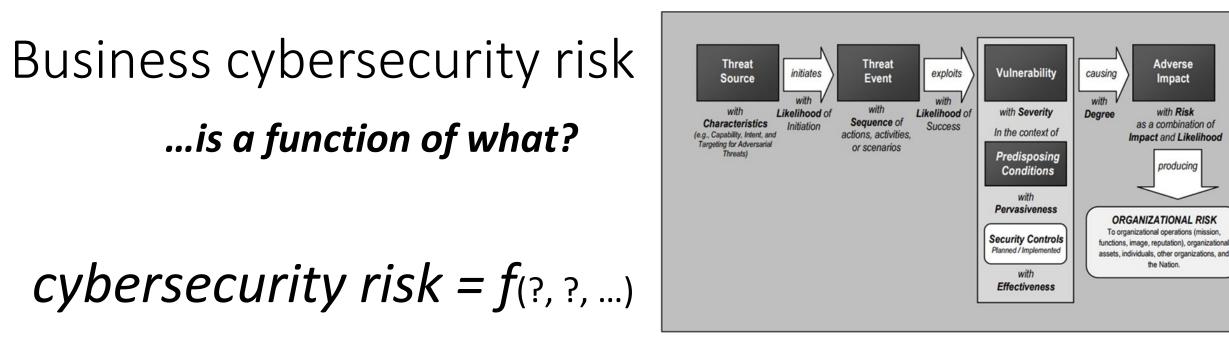
Agenda

- Quiz: 100 digits of Pi
- National Institute of Standards and Technology (NIST)
 - Cybersecurity Framework
 - Risk Management Framework
- Applying the NIST Risk Management Framework
- Milestone 1 Assignment

Business cybersecurity risk

... is a function of what?





f(threats, vulnerabilities, assets) f(threat, (vulnerability * lack of control), (asset * dependencies))

Results in impacts which have an adverse effect on:

- Organizational operations
- Assets
- individuals

Federal Information Security Management Act (FISMA) of 2002 Federal Information Security Modernization Act (FISMA) of 2014

Recognizes importance of information security to the economy and national security

- Requires each government organization to provide information security for information and information systems supporting their operations and assets
 - Including those provided or managed by another agency, contractors, or other sources
- Made NIST responsible for developing standards, guidelines, and associated methods and techniques for providing adequate information security for all agency operations and assets (excluding national security systems)



NIST's "Cybersecurity Framework"

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

IDENTIFY	What assets need protection?
PROTECT	What safeguards are available?
DETECT	What techniques can identify incidents?
RESPOND	What techniques can contain impacts of incidents?
RECOVER	What techniques can restore capabilities?

NIST Cybersecurity Framework

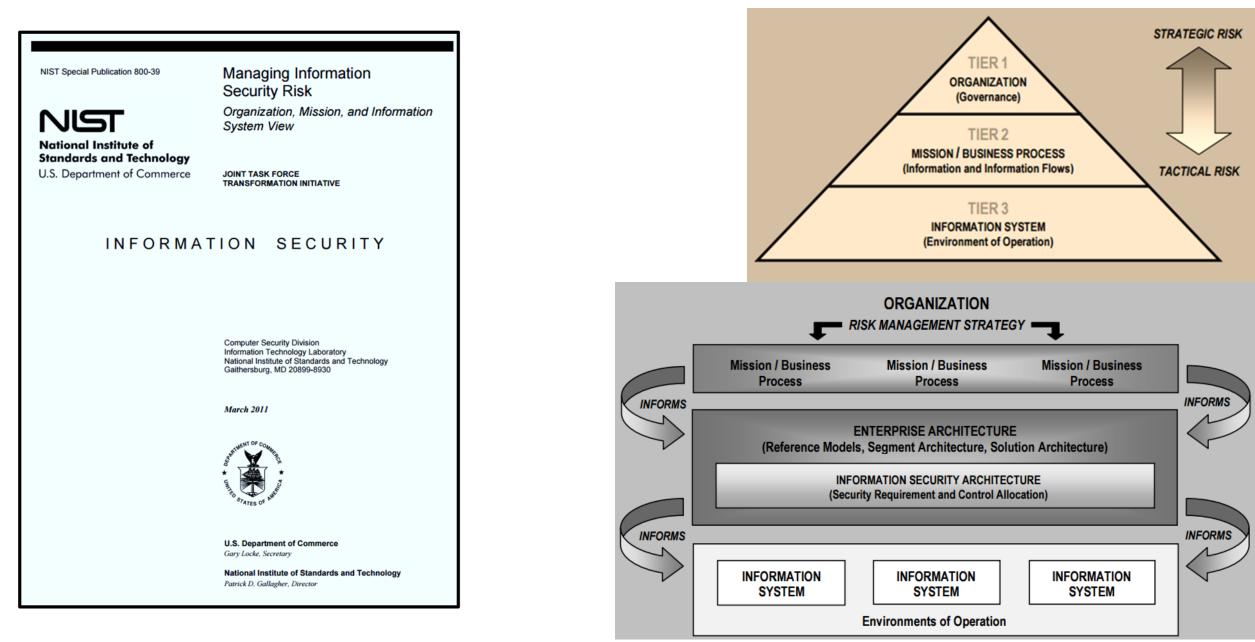
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control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

Cybersecurity Maturity Model Certification (CMMC) levels



Is used to assess an organization's cybersecurity capability maturity level, and recommend steps for improvement

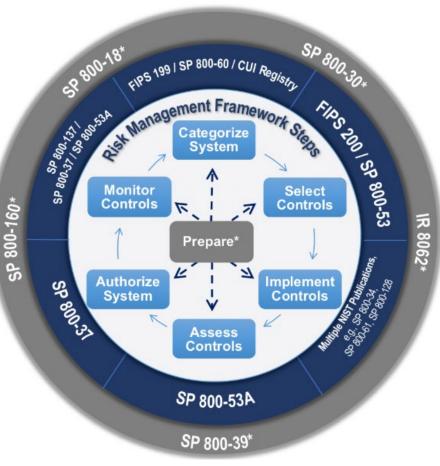
NIST's Risk Management Framework



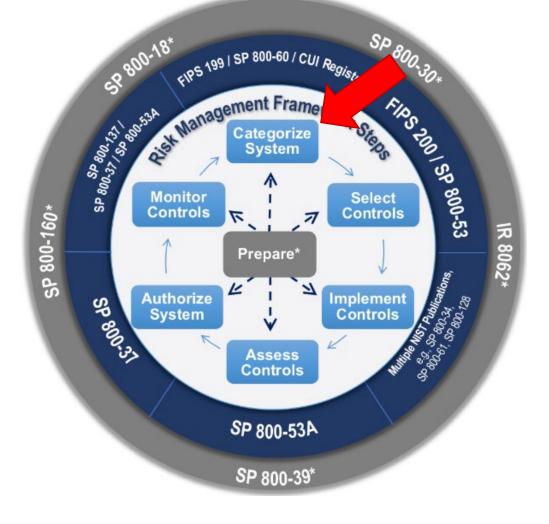
Security Categorization & Selecting a Baseline of Cybersecurity Risk Controls

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

NIST Special Publication 800-37 Revision 2 **Risk Management Framework for** Information Systems and Organizations A System Life Cycle Approach for Security and Privacy JOINT TASK FORCE This publication is available free of charge from December 2018 U.S. Department of Commerce Wilbur L. Ross, Jr., Secretary National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



1st Step in cybersecurity is security categorization (i.e. risk assessment)



- i. Inventory the data content of the information systemii. Determine the security categorization of the information based on potential impacts a breach of
 - confidentiality, integrity and availability will have on organizational operations, assets, or individuals based FIPS 199 standard

Risk is based on impact of a security breach

		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.

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 Ariden L. Bement, Jr., Director In the Risk Management Framework (RMF) likelihood of a breach is treated as 100%

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

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 are the security categorizations of these datasets?

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

What are the security categorizations of the geodatabases?

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

What is the overall security categorization of the information system containing these datasets?

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

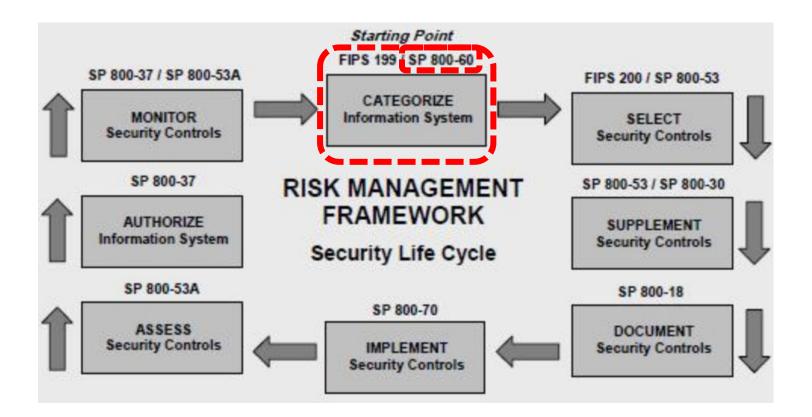
Agenda

✓ 100 Digits of Pi Quiz

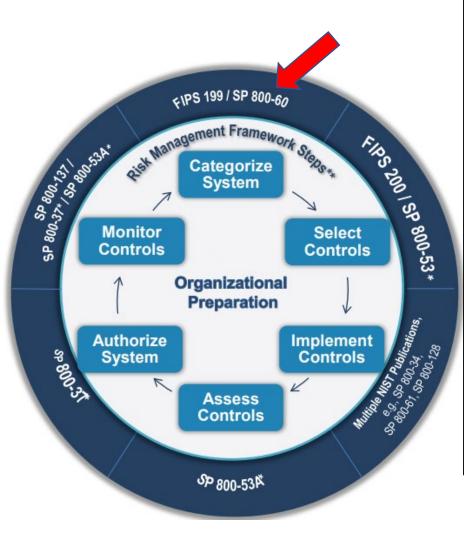
✓ National Institute of Standards and Technology (NIST)
 ✓ Cybersecurity Framework
 ✓ Risk Management Framework

- Applying the NIST Risk Management Framework
- Milestone 1 Assignment

NIST Risk Management Framework



A guide for provisional security categorization



NIST Special Publication 800-60 Volume I Revision 1



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

Information and Information Systems to Security Categories Kevin Stine **Rich Kissel** William C. Barker Jim Fahlsing

Guide for Mapping Types of

INFORMATION SECURITY

Jessica Gulick

Volume I:



August 2008



U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY James M. Turner, Deputy Director

NIST Special Publication 800-60 Volume II Revision 1



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

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine **Rich Kissel** William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY James M. Turner, Deputy Director

Found at NIST and on the Lecture Materials page of the MIS Community website

1/25/2024

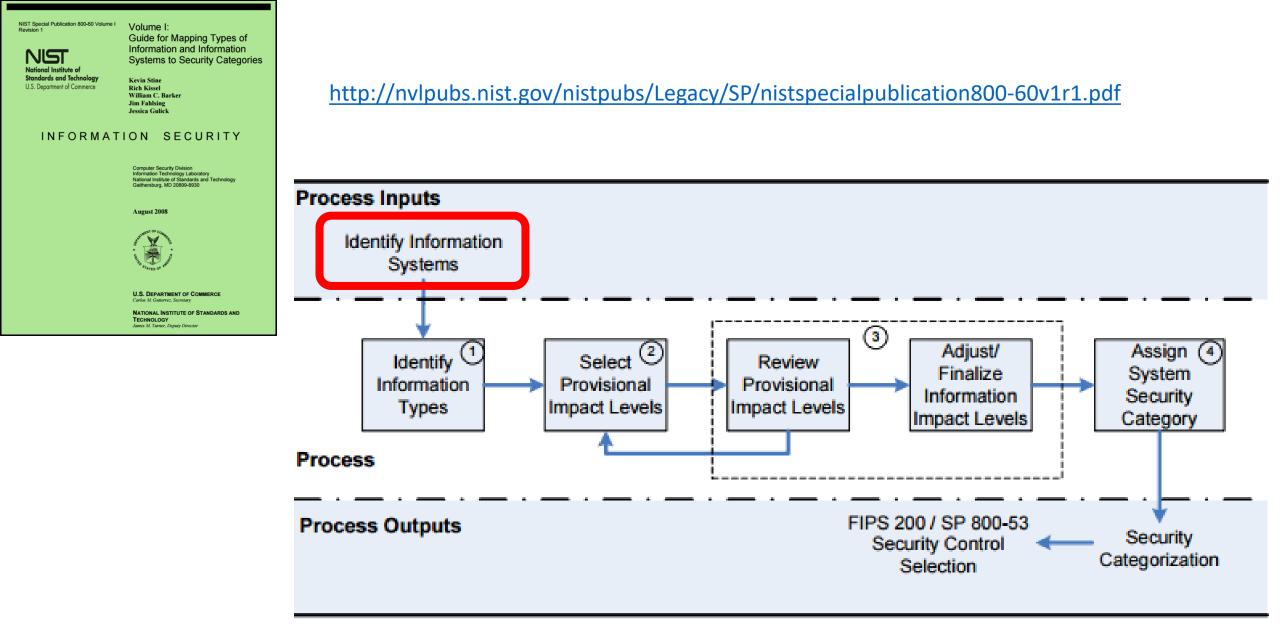
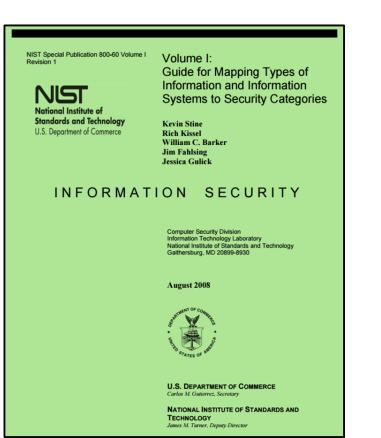


Figure 2: SP 800-60 Security Categorization Process Execution

2 Broad types of Information and Information Systems

1. Mission-based Information & Information Systems

2. Management and Support Information & Information Systems



Mission-based Information and Information Systems

- 1. Defense and National Security
- 2. Homeland Security
- 3. Intelligence Operations
- 4. Disaster Management
- 5. International Affairs and Commerce
- 6. Natural Resources
- 7. Energy
- 8. Environmental Management
- 9. Economic Development
- 10. Community and Social Services
- 11. Transportation
- 12. Education
- 13. Workforce Management

14. Health

- 15. Income Security
- 16. Law Enforcement
- 17. Litigation and Judicial Activities
- ce 18. Federal Correctional Activities
 - 19. General Sciences and Innovation
 - 20. Knowledge Creation and Management
 - 21. Regulatory Compliance and Enforcement
 - 22. Public Goods Creation and Management
 - 23. Federal Financial Assistance
 - 24. Credit and Insurance
 - 25. Transfers to State/Local Governments
 - 26. Direct Services for Citizens

Disaster Management Information Types

Table 4: Mission-Based Information

Mission Areas and Information

Energy Supply

Forecasting

Financial Sector Overs

D.1 Defense & National Security Strategic National & Theater Defense Operational Defense Tactical Defense **D.2 Homeland Security**

Border and Transportation Security Key Asset and Critical Infrastructure Protection Catastrophic Defense Executive Functions of the Executive Office of the President (EOP) **D.3 Intelligence Operations**

Intelligence Planning Intelligence Collection Intelligence Analysis & Production Intelligence Dissemination

D.4 Disaster Management Disaster Monitoring and Prediction Disaster Preparedness and Planning Disaster Repair and Restoration Emergency Response

DAS INTERNATIONAL ATTAILS OF Commerce Foreign Affairs International Development and Humanitarian Aid Global Trade **D.6 Natural Resources** Water Resource Management Conservation, Marine and Land Management Recreational Resource Management and Tourism Agricultural Innovation and Services

D.4 Disaster Management Disaster Monitoring and Prediction D.7 End Energy Conservation a Disaster Preparedness and Planning Energy Resource Man Energy Production **D.8** Environmenta **Disaster Repair and Restoration** Environmental Monito Environmental Remed Pollution Prevention a **D.9 Economic D** Emergency Response Business and Industry Intellectual Property F

Industry Sector Income Stabilization D.10 Community & Social Services Homeownership Promotion Community and Regional Development Social Services Postal Services **D.11 Transportation**

Ground Transportation Water Transportation Air Transportation Space Operations **D.12** Education

Elementary, Secondary, and Vocational Education Higher Education Cultural and Historic Preservation Cultural and Historic Exhibition D.13 Workforce Management Training and Employment Labor Rights Management Worker Safety

D.16 Law Enforcement Criminal Apprehension Criminal Investigation and Surveillance Citizen Protection Leadership Protection Property Protection Substance Control Crime Prevention Trade Law Enforcement **D.17 Litigation & Judicial Activities** Judicial Hearings Legal Defense Legal Investigation Legal Prosecution and Litigation Resolution Facilitation **D.18 Federal Correctional Activities** Criminal Incarceration Criminal Rehabilitation **D.19 General Sciences & Innovation** Scientific and Technological Research and Innovation Space Exploration and Innovation

Civilian Operations NIST Special Publication 800-60 Volume Volume I: Guide for Mapping Types of Information and Information NIST Systems to Security Categories indards and Techn Kevin Stine Rich Kissel William C. Barker Jim Fahlsing Jessica Guliel INFORMATION SECURITY August 2008 U.S. DEPARTMENT OF COM

NATIONAL INSTITUTE OF STANDARDS AND

TECHNOLOGY

D.25 Transfers to State/ Local Governments Formula Grants Project/Competitive Grants Earmarked Grants State Loans D.26 Direct Services for Citizens Military Operations

D.24 Credit and Insurance

Mode of Delivery]

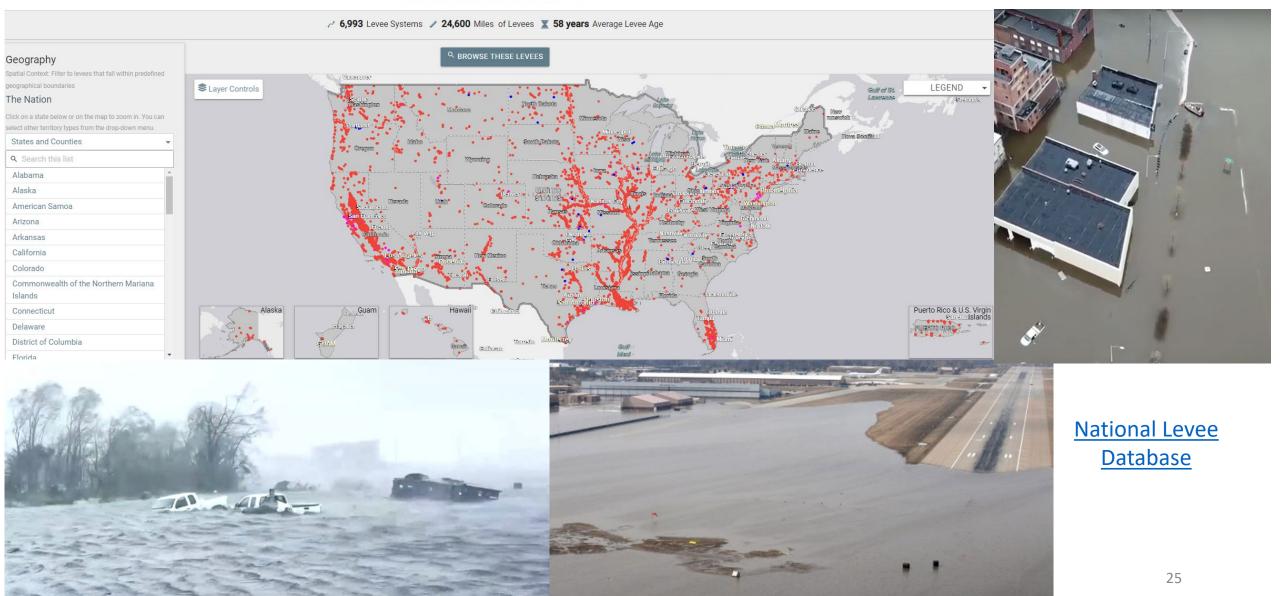
Loan Guarantees

General Insurance

Direct Loans

Disaster Management Information System Example

Levees of The Nation •



NIST Special Publication 800-60 Volume II Revision 1



Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 August 2008

U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY James M. Turner, Deputy Director

2. Select Provisional Impact Levels for the identified information system

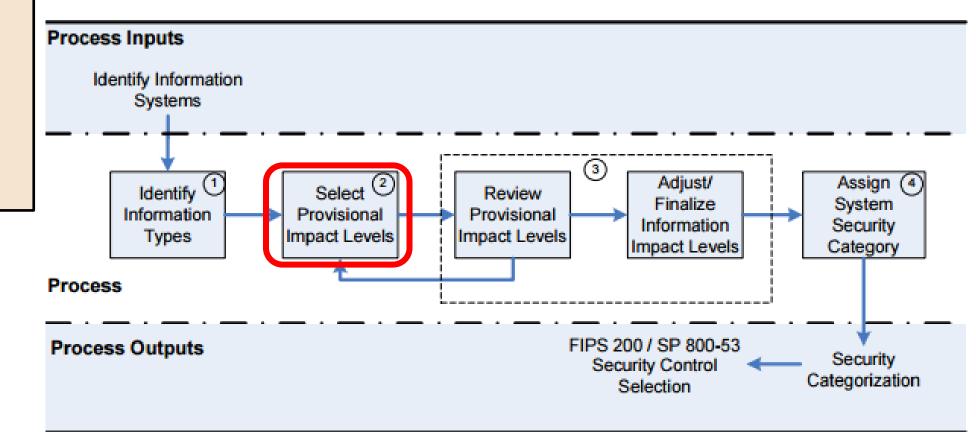


Figure 2: SP 800-60 Security Categorization Process Execution

NIST Special Publication 800-60 Volume II Revision 1



Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine Rich Kissel William C. Barker Annabelle Lee Jim Fahlsing

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

August 2008



U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY James M. Turner, Deputy Director

Disaster Management Information Types

APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS	102
D.1 Defense and National Security	
D.2 Homeland Security	108
D.2.1 Border and Transportation Security Information Type	
D.2.2 Key Asset and Critical Infrastructure Protection Information Type	110
D.2.3 Catastrophic Defense Information Type	111
D.2.4 Executive Functions of the Executive Office of the President (EOP) Information	
Туре	112
D.3 Intelligence Operations	113
D.4 Disaster Management	115
D.4.1 Disaster Monitoring and Prediction Information Type	
D.4.2 Disaster Preparedness and Planning Information Type	
D.4.3 Disaster Repair and Restoration Information Type	118
D.4.4 Emergency Response Information Type	119

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Disaster Management Information Impact

D.4 Disaster Management

Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made. Compromise of much information associated with any of the missions within the disaster management mission area may seriously impact the security of a broad range of critical infrastructures and key national assets.

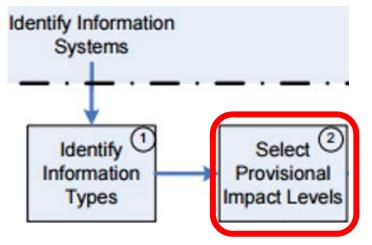
Exercise

• Open up an Excel spreadsheet, and organize it in the manner illustrated below

Information Types	Confidentiality	Integrity	Availability
Disaster Monitoring and Prediction			
Disaster Preparedness and Planning			
Disaster Repair and Restoration			
Emergency Response Information Type			

• Using <u>NIST SP 800-60 V.2 R1</u> determine the Impact Levels for the Disaster Information Types

Disaster Management Information Types



D.4.1 Disaster Monitoring and Prediction Information Type

Disaster monitoring and prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. [Some disaster management information occurs in humanitarian aid systems under the International Affairs and Commerce line of business (e.g., State Department disaster preparedness and planning).] The recommended provisional categorization of the disaster monitoring and protection information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

D.4.2 Disaster Preparedness and Planning Information Type

Disaster preparedness and planning involves the development of response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The recommended provisional categorization of the disaster preparedness and planning information type follows:

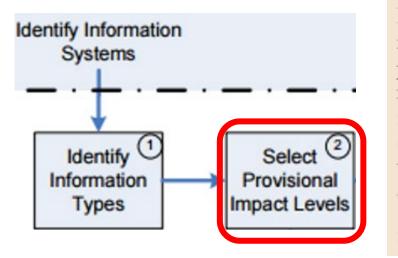
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

D.4.3 Disaster Repair and Restoration Information Type

Disaster repair and restoration involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The recommended provisional categorization of the disaster repair and restoration information type follows:

Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

Disaster Management Information Types



D.4.4 Emergency Response Information Type

Emergency Response involves the immediate actions taken to respond to a disaster (e.g., wildfire management). These actions include providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. Impacts to emergency response information and the information systems that process and store emergency response information could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions. The recommended provisional categorization of the emergency response information type follows:

Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Exercise

• Determine the Summary Impact Levels for the Disaster Information Types

Information TypesConfidentialityIntegrityAvailabilitySummary ImpactDisaster Monitoring and PredictionLowHigh4Disaster Preparedness and PlanningLowLow2	Disaster Management Information Systems						
Disaster Monitoring and Prediction Low High High ? Disaster Preparedness and Planning Low Low ?							
Disaster Preparedness and Planning Low Low Cow ?	Information Types	Confidentiality	Integrity	Availability	Level		
	Disaster Monitoring and Prediction	Low	High	High	?		
Director Densis and Destantion law law law 2	Disaster Preparedness and Planning	Low	Low	Low	?		
Disaster Repair and Restoration Low Low Low Low	Disaster Repair and Restoration	Low	Low	Low	?		
Emergency Response Information Type Low High High ?	Emergency Response Information Type	Low	High	High	?		

Determine the Overall Impact Levels for the Disaster Information Types

Disaster Manage	ment Infor	mation	Systems	
				Summary Impact
Information Types	Confidentiality	Integrity	Availability	Level
Disaster Monitoring and Prediction	Low	High	High	High
Disaster Preparedness and Planning	Low	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low	Low
Emergency Response Information Type	Low	High	High	High
Information System Impact Ratings:	?	?	?	

Determine the overall security categorization of a Disaster Information System

Disaster Manage	Confidentiality		Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	High
Disaster Preparedness and Planning	Low	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low	Low
Emergency Response Information Type	Low	High	High	High
Information System Impact Ratings:	Low	High	High	?

Determine the overall security categorization of a Disaster Information System

Disaster Manage	ment Infor	mation	Systems	
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	High
Disaster Preparedness and Planning	Low	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low	Low
Emergency Response Information Type	Low	High	High	High
Information System Impact Ratings:	Low	High	High	High

What synonyms should you use to explain the meaning of low, moderate, or high impact breaches?

	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.						

NIST Special Publication 800-60 Volume I Revision 1 Volume I



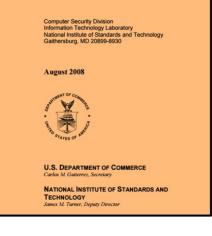
Guide for Mapping Types of Information and Information Systems to Security Categories

Standards and Technology U.S. Department of Commerce

Rich Kissel William C. Barker Jim Fahlsing Jessica Gulick

INFORMATION SECURITY

Kevin Stine



Once categorized, select security control baseline for the information system

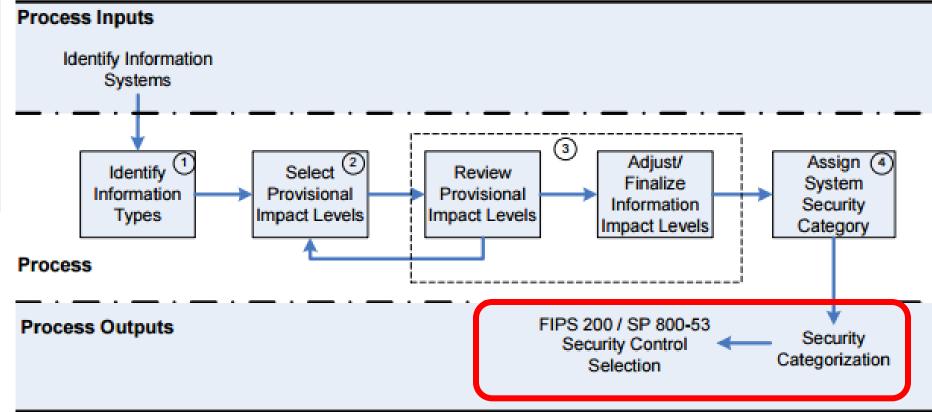


Figure 2: SP 800-60 Security Categorization Process Execution

Selecting cybersecurity risk controls



FIPS 199 categorization is used to select among <u>3 impact-based baselines</u> of <u>security</u> <u>controls</u>

ted Not Selecte

I Not Select Not Select SC-39 Not Select Not Select

Not Select Not Select Not Select

SI-8 (1) (2

 SI-10

 I
 SI-11

 2
 SI-12

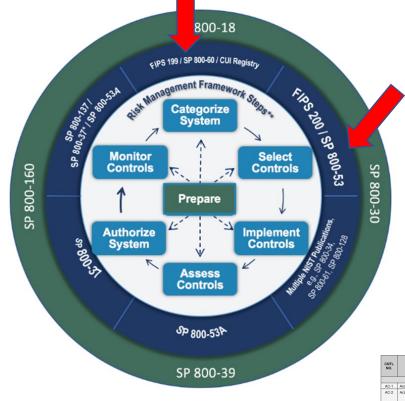
 cted
 Not Selected

 cted
 Not Selected

 cted
 Not Selected

 SI-10
 SI-12

cted Not Selected



Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	High
Disaster Preparedness and Planning	Low	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low	Low
Emergency Response Information Type	Low	High	High	High
Information System Impact Ratings:	Low	High	High	High

															CNT			_			4		NITIAL CO	ONTROL
															NO.		c	ONT	ROLN	IAME	PRIORTY	LOW		MOD
															SC-2		nin Nodes				PO	Not Selec		MOD Not Select
															SC-2 SC-2		oneypots					Not Selec		Not Select
															SC-2	7 PI	atform-Inde	pende	nt Appl	ications		Not Selec	ted 1	Not Select
															SC-2	8 Pi	rotection of	Inform	ation al	Rest	P1	Not Selec		SC-28
																			≿	INITIAL C	ONTROL	ONTROL BASELINES		
													NTL NO.		CONTR				PRIOR	LOW	MOD		нюн	
													A-10 A-11	Devel	loper Configur. Ioper Security	ition Ma Testing	inagement and Evaluat	ion	P1 P1	Not Selected Not Selected	SA-10 SA-11		SA-10 SA-11	
												S	A-12	Suppl	ly Chain Prote	tion			P1	Not Sel	Not Select	d S	SA-12	t Select
								-	_			s	A-13	Trust	worthiness			_	PO	Not Sel	Not Select		Selected	
2								CP	m.		000	ROL			PRIORITY		INITIAL	ONTR	OL BA	SELINES	of Select		SA-15	t Select
3								N	0.		CONI	ROL	AMIE		PRK	Ð	w	м	OD	HIGH	ot Select	d .	SA-10	t Select
											le Work Sit			_	P2		elected	PE		PE-17	ot Selecti	ed S	SA-17	SC-39 t Select
											n of Inform		stern Co	mpon			elected		elected	PE-18 Not Selected	ot Select	d Not	Selected	t Select
{								PE	-19 1	forma	ition Leaka Nonitoring a	ge ed Tra	kina		P0 P0	Not S Not S			elected elected	Not Selected	ot Select		Selected	t Select
·									20 11						Planning	10010		100.0		10100000	1			t Select
2					1							Ł		IN	TIAL CONTRI	L BAS	EL	,	4	PL-1	of Select		Selected	t Select
						CNTL NO.		CONTR	OL NA	ME		PRIORTY				-			(3)	PL-2 (3)	-			SI-1
					-	-								W	MC		HIG		(1)	PL-4 (1)	SC-1		SC-1	
					ŀ	IR-3	Incident I	Response 1 Handling	esting			P2 P1	Not S	electe R-4	d IR-3		IR-3		-		SC-2		SC-2	SI-2 (2)
						IR-5	Incident I	Initoring				P1		R-5	R		IR-5		- lected	Not Selected	ot Selecti		SC-3	-3 (1) (2
				_		IR-6	Incident P	Reporting				P1	IF	2-0	IR-6	(1)	IR-6 IR-7		8	PL-8	SC-4 SC-5		SC-4 SC-5	SI-6
				CNT					È		INITIAL	LCONT	ROL BA	SELI		<u>)</u>	IR-/	1)	lected	Not Selected	ot Select		Selected	tSelect
				NO.	CC	ONTRO	LNAME		PRIORTY	L	.ow		100		HIGH	sted	Not Sel	cted	1	PS-1	-7 (3) (4) (7)	(5) SC-7 (7) (8	7 (3) (4) (5) 8) (18) (21)	-7 (1) (
				CM-	Configuration	Settings	_	_	P1	c	-M-0		M-0		CM-6 (1) (2)	:ted	Not Sel	icted	-2	PS-2	SC-8 (1)		IC-8 (1)	-8 (1) (
					7 Least Function	ality			P1		M-7		(1) (2) (4		M-7 (1) (2) (5)				-3	PS-3	 SC-10	- I	 SC-10	
				CM-I	8 Information Sy	stem Co	nponent in	ventory	P1	0	-M-8		(1) (3) (5	s) c	M-8 (1) (2) (3) (4) (5)	_	MA-2		5	PS-4 (2) PS-5	of Select		Selected	SI-10
						Ł		INITIAL C	ONTROL	BASE	ELINE	-	A-9		CM-9 CM-10	(2)	MA-3 (1)		-0	PS-6	SC-12	SC	C-12 (1)	SI-12
		CNTL NO.	CON	TROL	NAME	PRIORT	1.00		MOD		ню	_	H10	+	CM-10 CM-11	2)	MA-4 () (3)	.7	PS-7 PS-8	SC-13		SC-13	t Select
						ess and		v	MOU		HIG	н				1	MA-5 MA		-	Para				t Select
		AT-1 S	ecurity Awaren	ess and	Awaren Training Policy and		Training AT-		AT-1	_	AT-	-1	2-1		CP-1	-			-1	RA-1	SC-15 pt Select		SC-15 Selected	t Select
			rocedures iecurity Awarene			P1	AT-	_	AT-2 (AT-2	-) (3) (8) C	(4) (5) (8)		MP-		-2	RA-2 RA-3	SC-17		SC-17	SI-10
			tole-Based Seco			P1	AT-		AT-3	.)	AT-		2.3	+	(+) (0) (0) CP-3 (1)	1	MP- MP-	2			SC-18		SC-18	_
		AT-4 S	ecurity Training	Record	s TROL BASELINE	P3	AT-		AT-4		AT-	4	4 (1)		CP-4 (1) (2)		MP-	4	(2) (5)	RA-5 (1) (2) (4)	SC-19 SC-20		SC-19 SC-20	-
		TABLE	D-2: SECURIT	YCON									(1) (3)	0	 P-6 (1) (2) (3)	6)	MP-5		lected	Not Selected	SC-21		SC-21	-
CNTL				λin	INITIA	L CONT	ROL BASE	ELINE		-	AU	-1) (2) (3) C	P-7 (1) (2) (3) (4)	1)	MP-8 (1) MP-7							
NO.	CON	ROL NAN	IE	PRIORITY	LOW		IOD	HIG	н		AU-2	(3)	(1)(2)		(4) (P-8 (1) (2) (3)	ted	Not Sel	octed	4	SA-1	SC-22	4	SC-22	
			Acce	ss Con	trol						AU-3 (1) (2)	9(1)		(4)	_	PE		2	SA-2	SC-23		SC-23	
AC-1	Access Control Po	licy and Pro		P1	AC-1		C-1	AC		_	AU- AU-5 (1				P-9 (1) (2) (3) (5)				-3	SA-3	ot Selecti	id (SC-24	
AC-2	Account Manager	vent		P1	AC-2	AC-2	(1) (2) (3) (4)	AC-2 (1) (4) (5) (1	(2) (3)	0	AU-8 (1)	(3) (5)	10 (2)	1	CP-10 (2) (4)		PE-3		(2) (9)	SA-4 (1) (2) (9) (10)				
								(13)	-	(6) AU-7		elected		Not Selected		PE		-5	SA-5	1			
AC-3 AC-4	Access Enforcem Information Flow 8			P1 P1	AC-3 Not Selected		.C-3 .C-4	AC			AU-8	(1)	elected		Not Selected Not Selected	-	PE-		<u> </u>		-			
AC-5	Separation of Dut			P1	Not Selected	1	C-5	AC	5	_	AU-9 (2)	(3) (4)				0	PE-6 () (4)	-8	SA-8	1			
AC-6	Least Privilege			P1	Not Selected	AC-6	1) (2) (5)	AC-6 (1) (5) (9)	(2) (3)	d	AU-		-1		IA-1		PE-8		(2)	SA-9 (2)]			
AC-7	Unsuccessful Log	on Attempts		P2	AC-7	1	C-7	AC	7		AU-12 ((1) (3)) (2) (3) 1) (12)		A-2 (1) (2) (3) 4) (8) (9) (11) (12)	1—	PE-		-					
AC-8	System Use Notifi			P1	AC-8		.C-8	AC		d d	Not Sel Not Sel	lected lected			(12)		PE-11		1					
AC-9 AC-10	Previous Logon (A Concurrent Sessio		cation	P0 P3	Not Selected Not Selected		elected	Not Sel		d	Not Sel	lected	-3	+	IA-3 IA-4		PE-		1					
AC-11		in como		P3	Not Selected		-11 (1)	AC-11		d	Not Sel	lected) (2) (3))	A-5 (1) (2) (3)	3)	PE-13 (1) (2)						
AC-12	Session Terminat	on		P2	Not Selected	A	C-12	AC-	12	-	CA-	.1	.8	+	(11) IA-8	<u> </u>	PE-		4					
AC-13 AC-14	Withdrawn Permitted Actions	without I don	Vication or	 P3	AC-14		 C-14	AC-		_			-7		IA-7	1—	PE-15 PE-		1					
	Authentication	manout roen	ancaborror	10	202-14		0.114	~~		-	CA-2 (CA-3	(5)) (2) (3) 9)	0	A-8 (1) (2) (3) (4)	-								
AC-15	Withdrawn					Alot		And Par	hotes				elected		Not Selected									
AC-16 AC-17	AC-16 Security Attributes AC-17 Remote Access		P0 P1	Not Selected AC-17	AC-1	selected 7 (1) (2)	Not Sel AC-17 (1) (2)						Not Selected Not Selected	1									
AC-18	Wireless Access	_		P1	AC-18		(4) 18 (1)	(3) (AC-18 (CA-7	(1)				1								
								(5		d	CA		-1	ſ	IR-1 IR-2 (1) (2)	-								
	Access Control fo Use of External In			P1 P1	AC-19 AC-20		19 (5) 0 (1) (2)	AC-19 AC-20			CA			-	as/2 (1) (2)	1								
AC-20 AC-21			orentis	P1 P2	AC-20 Not Selected		0 (1) (2) C-21	AC-20			CM	-1	1											
AC-22	Publicly Accessibl	e Content		P3	AC-22		C-22	AC-	22	(7)	CM-2 (1) (7)	(2) (3)	1											
AC-23	Data Mining Prote Access Control De			P0 P0	Not Selected Not Selected		selected	Not Sel		-	(7) CM-3 (1) (2)												
AC-24 AC-25	Reference Monito			P0 P0	Not Selected Not Selected		selected	Not Sel		_	CM-4	(1)												
											CM-5 (1)		J											

CNTL			INITIAL CONTROL BASELINES						
NO.	CONTROL NAME	PRIORTY	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	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	ion 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				

Agenda

✓ 100 Digits of Pi Quiz

✓ National Institute of Standards and Technology (NIST)

- ✓ Cybersecurity Framework
- ✓ Risk Management Framework
- ✓ Applying the NIST Risk Management Framework
- Milestone 1 Assignment

Milestone 1 – Risk Assessment Report

Milestone 1 Assignment is found in Canvas

Your assignment is to apply the NIST Risk Management Framework and create a risk assessment report for managers of a (fictitious) company that owns and depends on financial information contained in a financial management system

Financial management involves the aggregate set of accounting practices and procedures that allow for the accurate and effective handling of all a business' revenues, funding, and expenditures. <u>NIST SP 800-60 Volume 2</u> identifies a set of business functions and associated types of data typically supported by and included in financial management information systems. What are they?

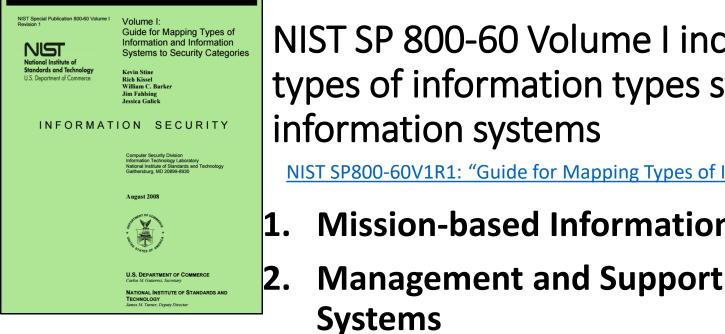
Your risk assessment assignment requires that you introduce and discuss:

- 1. Security objectives and potential impacts defined in Federal Information Processing Standard 199: "Standards for Security Categorization of Federal Information and Information Systems"
- 2. Methodology for assigning impact levels to information and information system types described in NIST Special Publication 800-60 Volume I
- Provisional security categorizations assigned to the financial management information types by NIST Special Publication 800-60 Volume II
- 4. You Determination of an overall security categorization for the financial information management system (FIMS) based on the provisional security categorization of the FMIS data types

How should you proceed in getting started with Milestone 1 ?

- 1. Inventory content of information in the Financial Information Management System (FIMS)
 - Use NIST SP 800-60v1.r1 and 800-60v2.r1
 - Determine the security categorization of the information contained within the FIMS
- 2. Determine the overall security categorization of the FIMS
- 3. Translate the FIMS' security categorization into non-technical language of organizational risk that a senior manager can understand and relate to

NIST SP800-60V2R1: "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"



NIST SP 800-60 Volume I includes tables that identify broad types of information types stored in a wide variety of

NIST SP800-60V1R1: "Guide for Mapping Types of Information and Information Systems to Security Categories"

- **Mission-based Information & Information Systems**
- Management and Support Information & Information
 - **Services Delivery Support Functions** i.

ii. **Resource Management Functions**

HINT: Use Volume 1's tables to identify which section of Volume II will contain the security categorizations you need for the data types found in your organization's Financial Information Systems

NIST SP 800-60 Volume II Revision 1, Volume II: "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"

Agenda

National Institute of Standards and Technology (NIST)
 Cybersecurity Framework
 Risk Management Framework
 Applying the NIST Risk Management Framework

✓ Milestone 1 Assignment