Managing Enterprise Cybersecurity MIS 4596

Class 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

100 Digits of Pi Quiz

- Share solutions
- Vote on best solutions
- Lessons learned
- Goal: Think like an attacker…

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

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

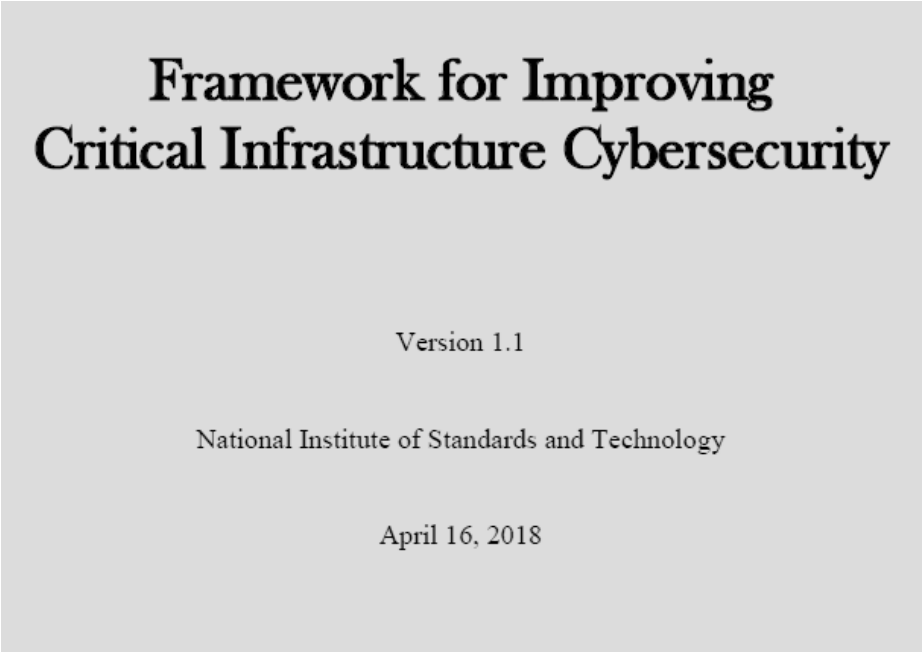
Recognizes importance of information security to the economy and national security

- 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)

https://www.dhs.gov/fisma

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

NIST's "Cybersecurity Framework"

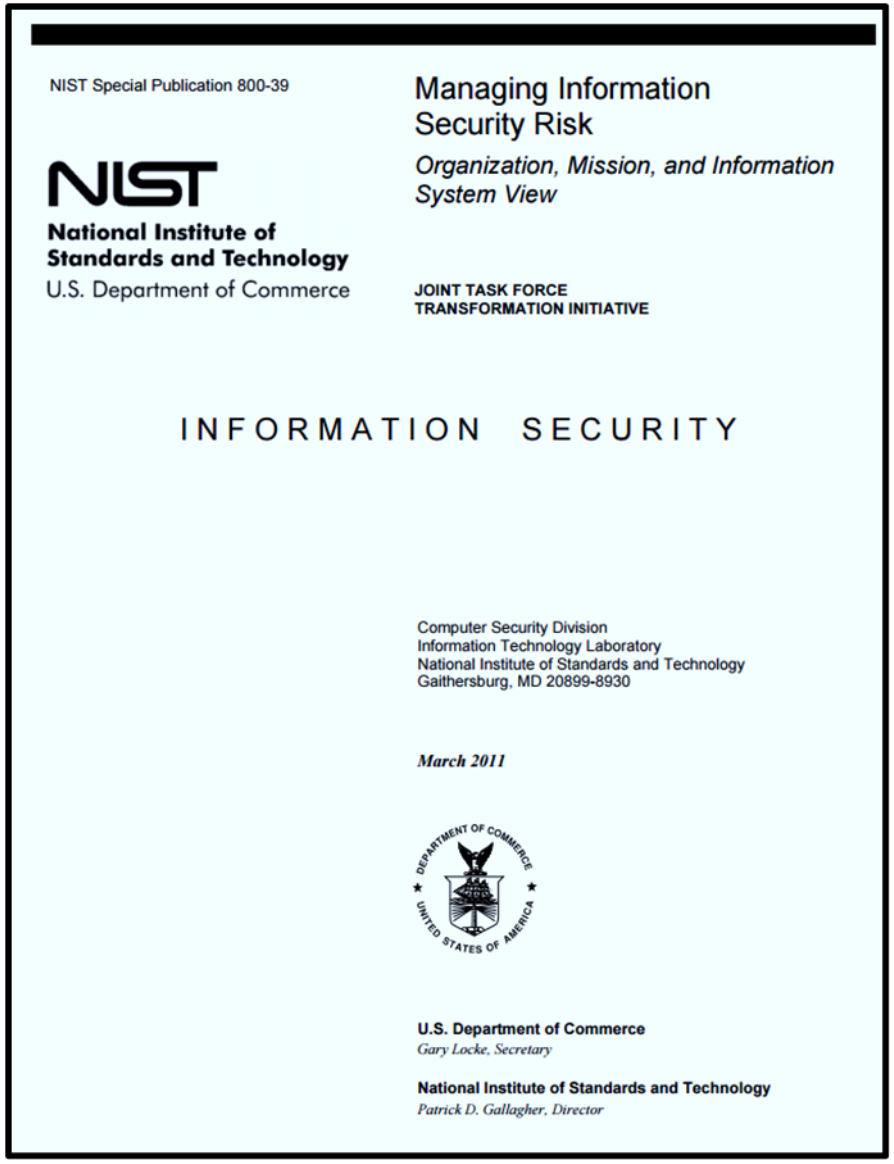

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

NIST's Risk Management Framework



NIST Special Publication 800-39

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

Managing Information Security Risk

Organization, Mission, and Information System View

JOINT TASK FORCE TRANSFORMATION INITIATIVE

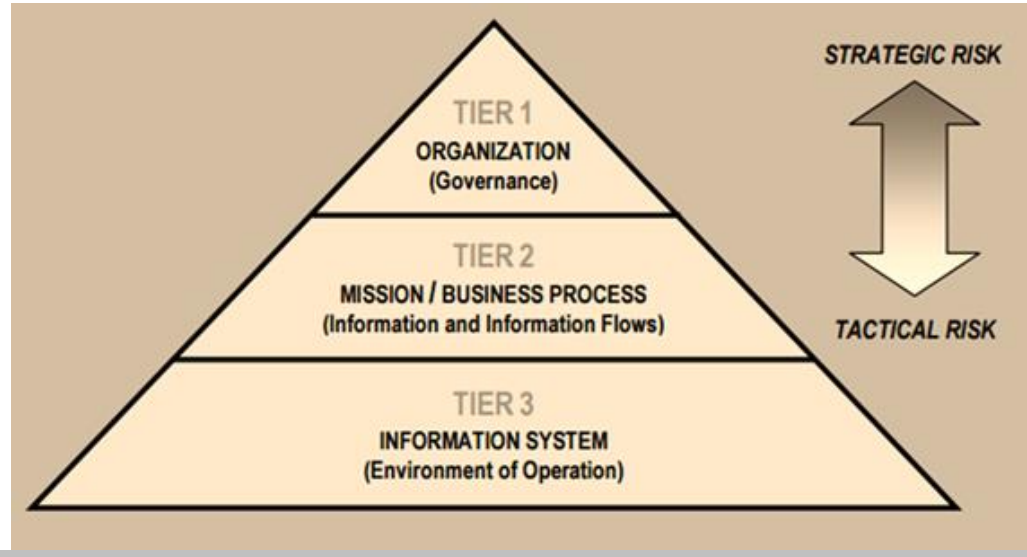
INFORMATION SECURITY

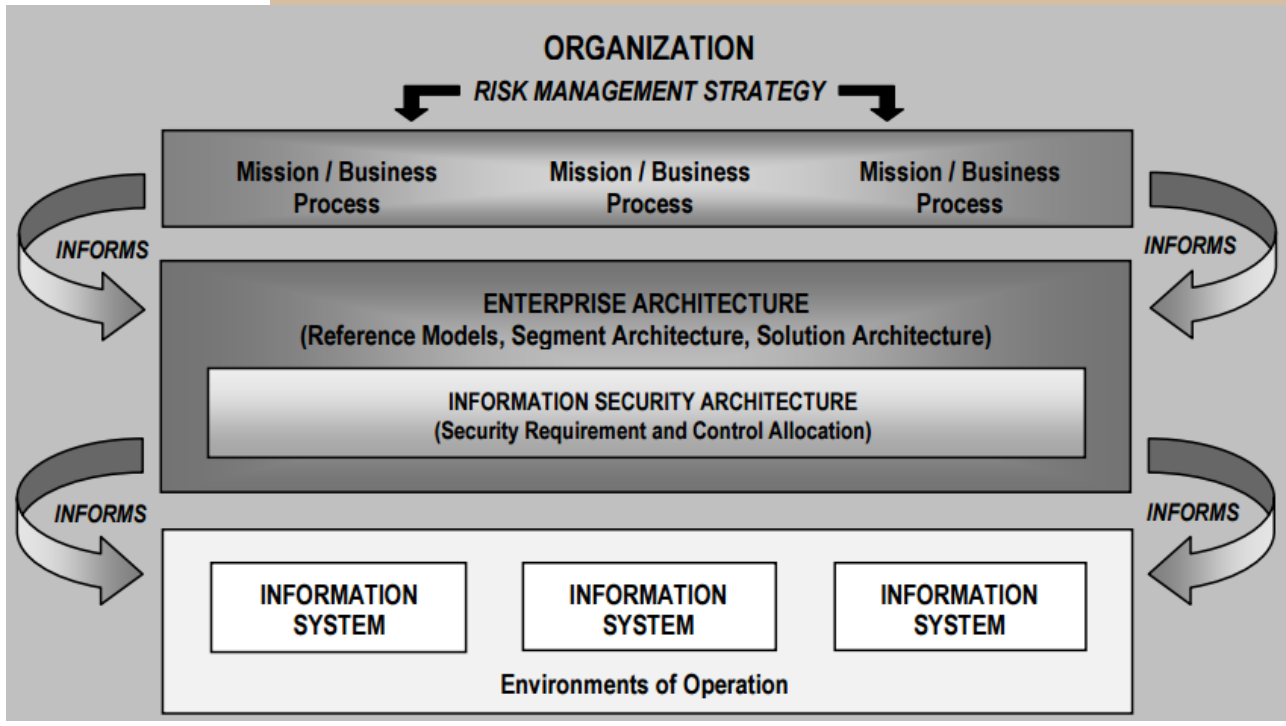
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2011

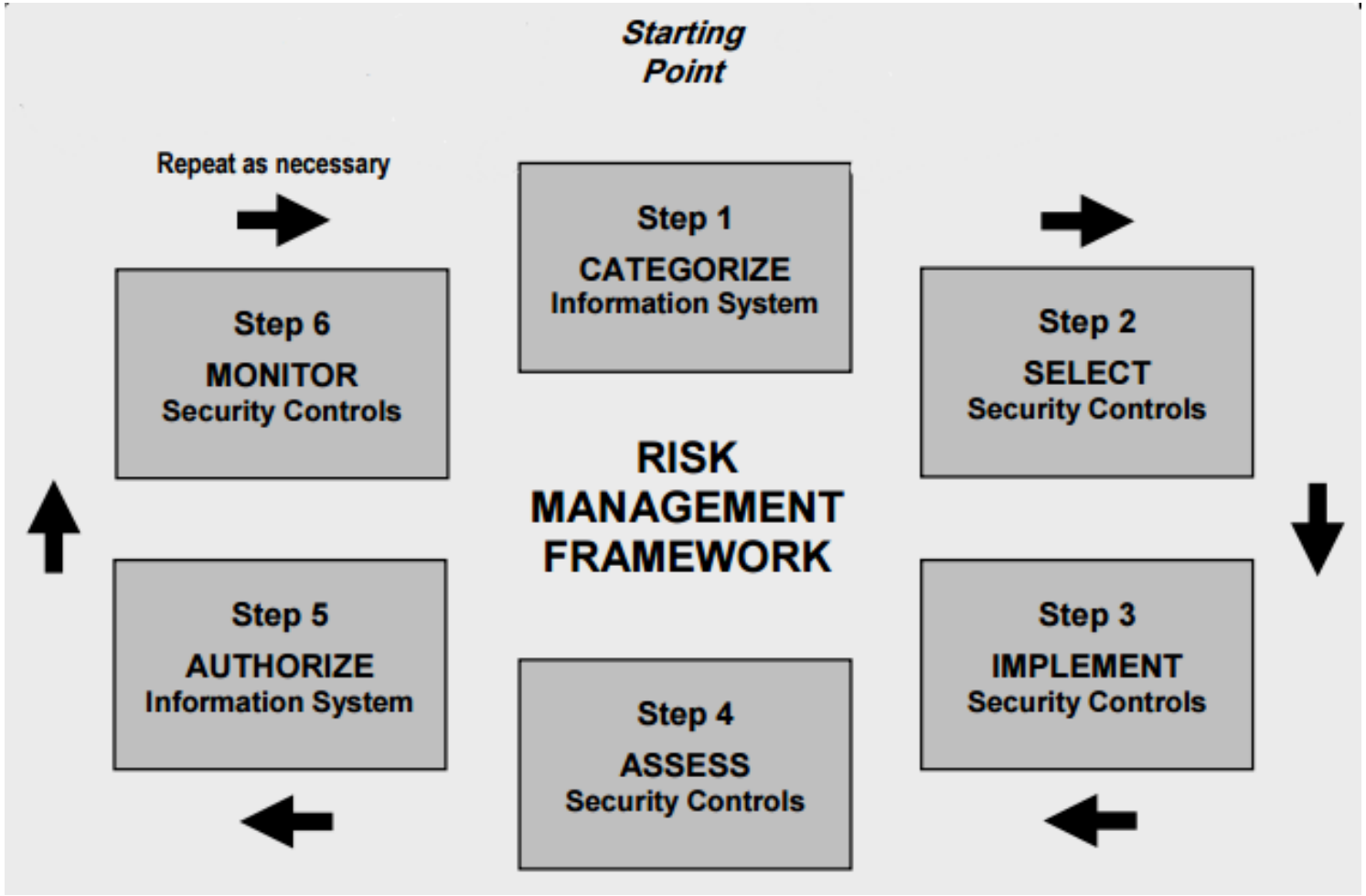
U.S. Department of Commerce
Gary Locke, Secretary

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

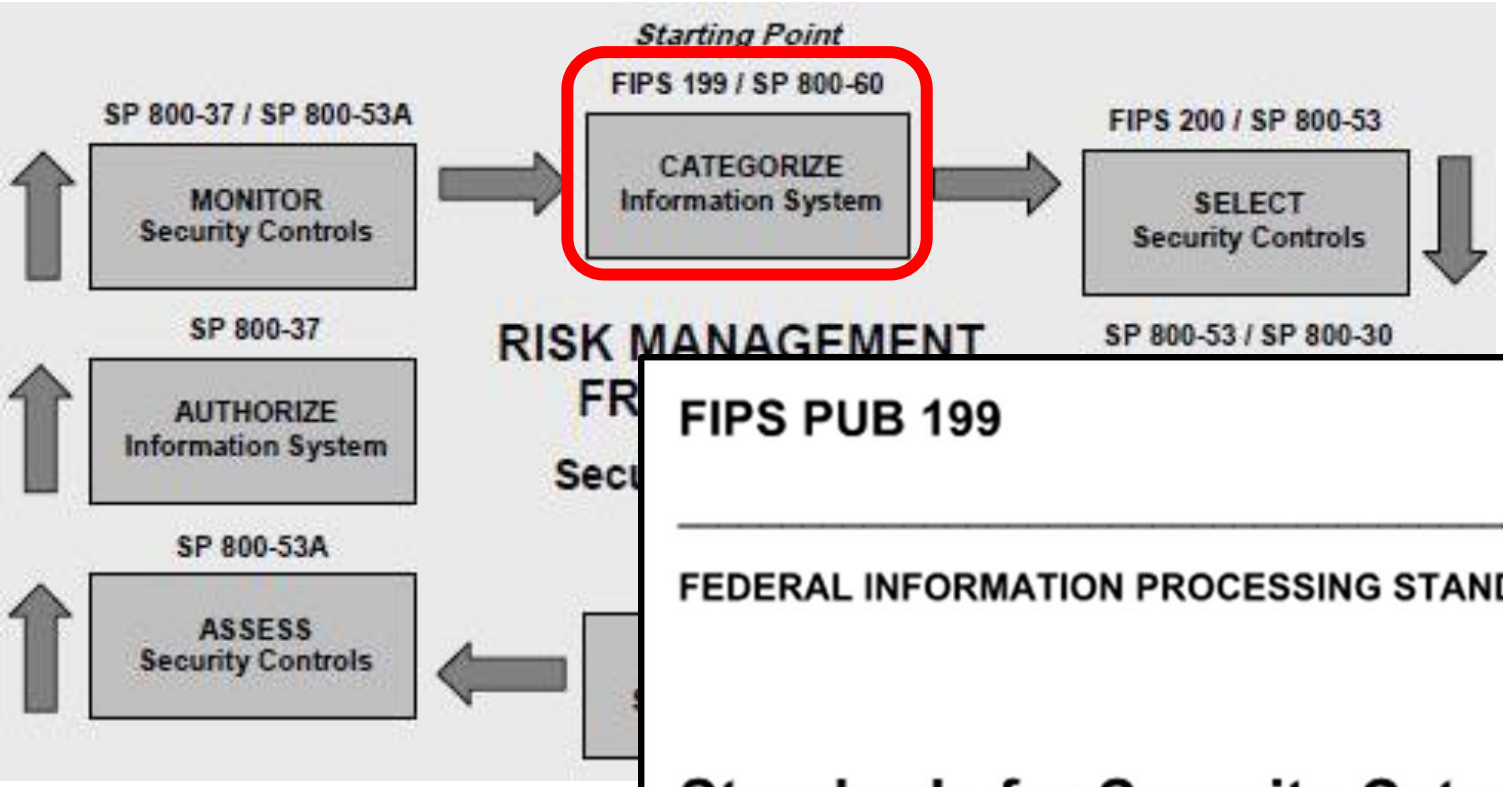


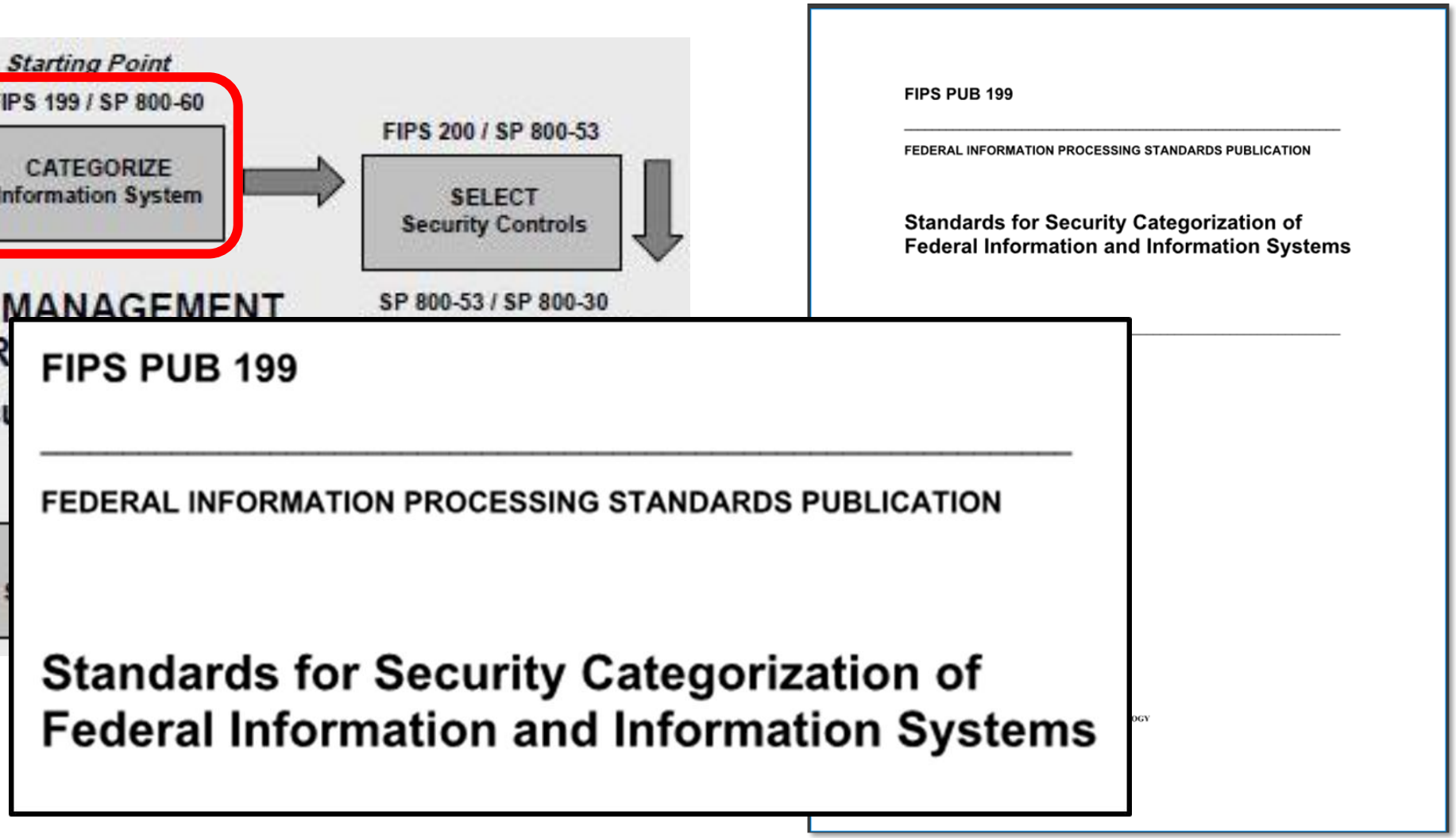


NIST's Risk Management Framework

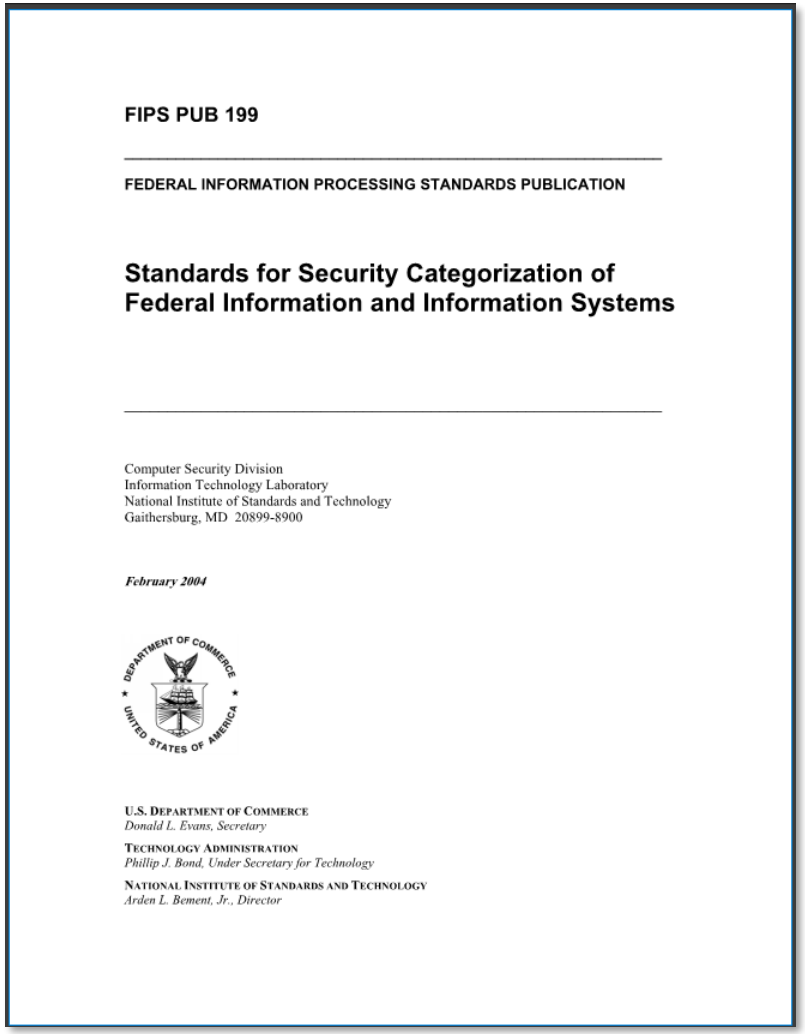


NIST Risk Management Framework





FIPS 199: Qualitative risk assessment based on security objectives



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

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

February 2004

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

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

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

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

What are the security categorizations of these datasets?

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

FIPS Pub 199 Standards for Security Categorization

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

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

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:

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

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}. = LOW rating

The resulting security category of the information system is expressed as:

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}, = MODERATE rating

What is the overall impact ratings of the datasets?

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

What is the overall Information System impact rating?

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

How would you 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

Solution:

NIST Special Publication 800-100

Information Security Handbook: A Guide for Managers

Recommendations of the National Institute of Standards and Technology

Pauline Bowen
Joan Hash
Mark Wilson

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

INFORMATION SECURITY

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

October 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

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

01527a

Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

Transformation of ordinal qualitative risk categories to interval quantitative risk measures

	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

01527a

Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

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

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

Solution

Dataset	Impact Rating	Likelihood
Communication	High	High
Electric	Moderate	Low
Traffic control	Low	Low
Water Distribution System	Moderate	Low
Sanitary Collection System	Low	Low
Storm Collection System	Low	Low
Parcel Boundary Shapefile	Low	Moderate

+

	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

= ?

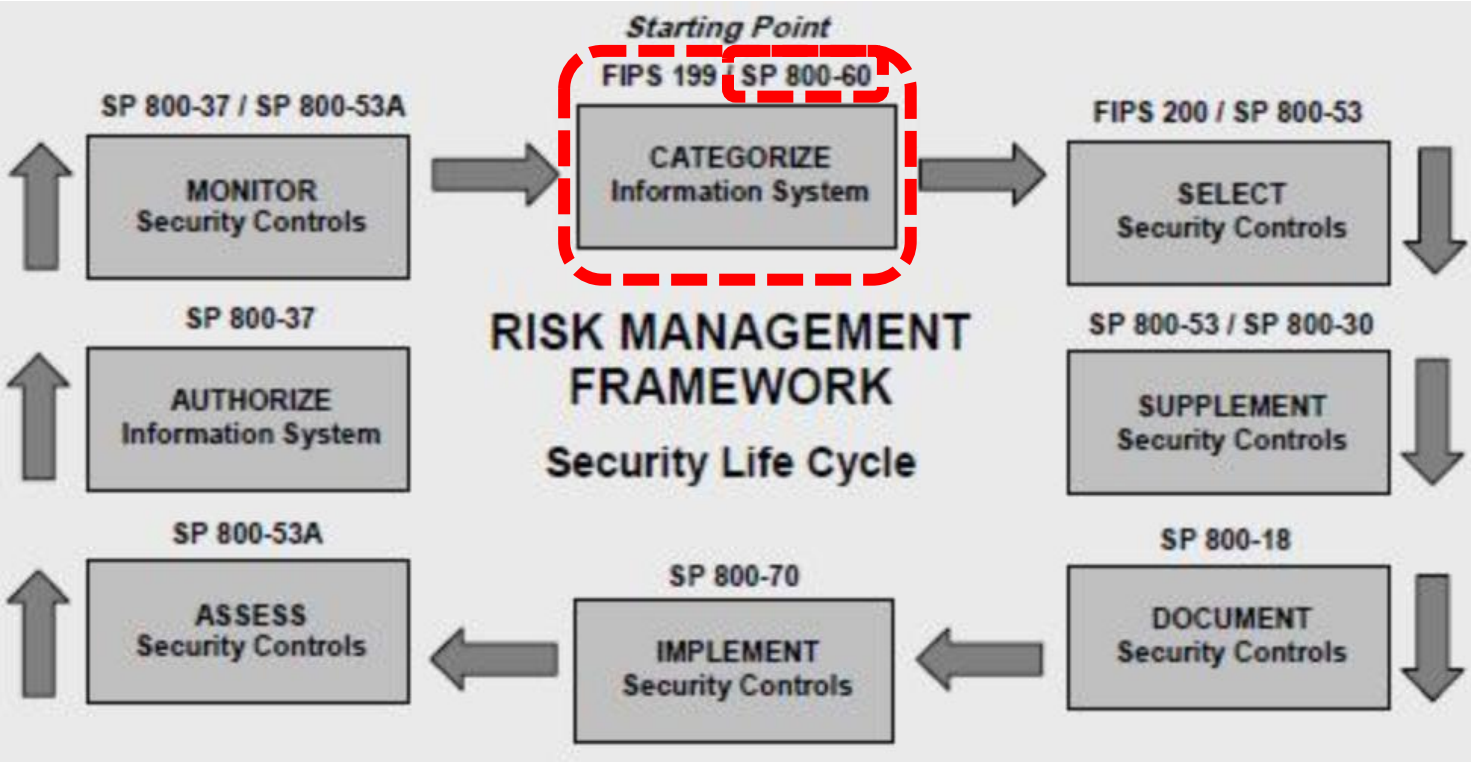
Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Traffic control	10	0.1	1
Comm_Electric Geodatabase	***High***		
			0
Water Distribution System	50	0.1	5
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1
Water_Sewer Geodatabase	**Moderate**	0.1	
			0
Parcel Boundary Shapefile	10	0.5	5

Dataset	Impact Rating	Likelihood	Risk
Communication	100	1	100
Electric	50	0.1	5
Water Distribution System	50	0.1	5
Parcel Boundary Shapefile	10	0.5	5
Traffic control	10	0.1	1
Sanitary Collection System	10	0.1	1
Storm Collection System	10	0.1	1

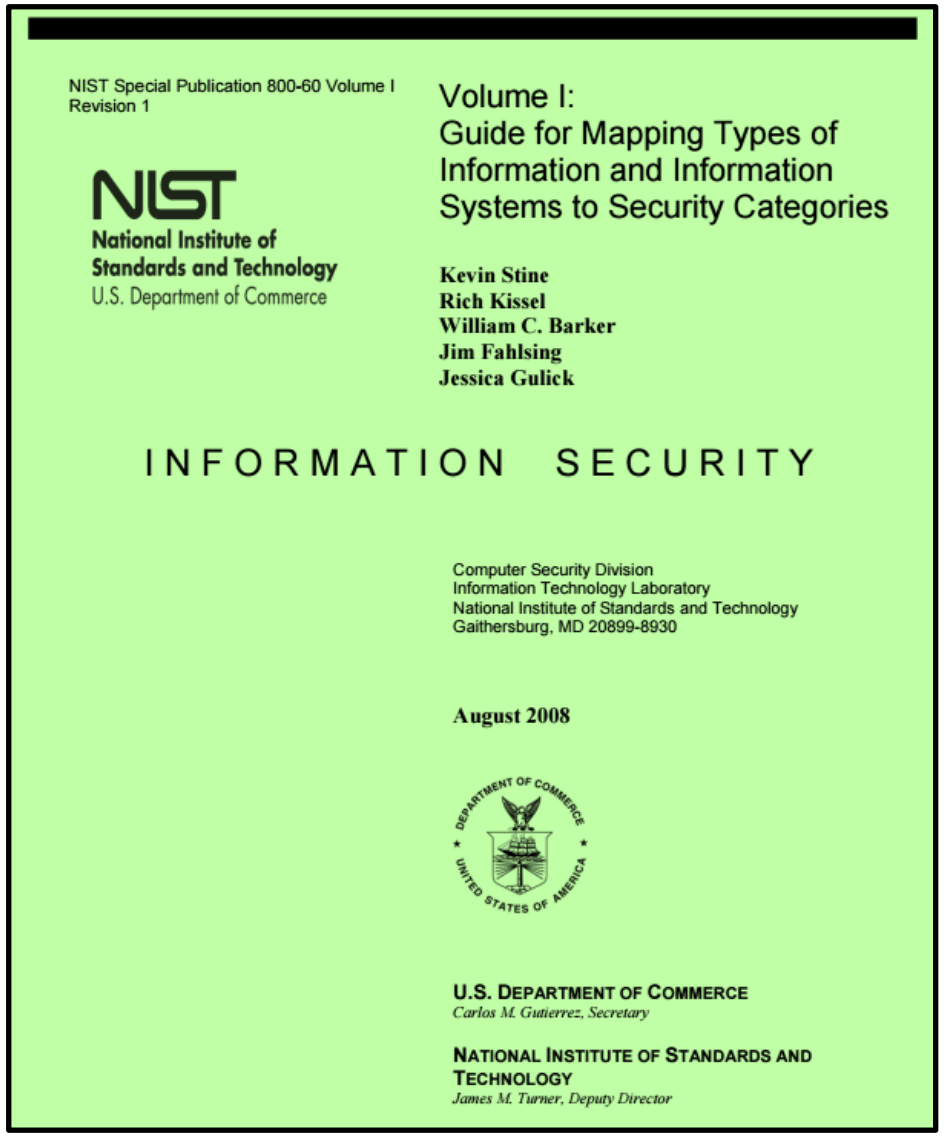
Agenda

- ✓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



NIST SP 800-60 volumes 1 and 2



NIST Special Publication 800-60 Volume I
Revision 1

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

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

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

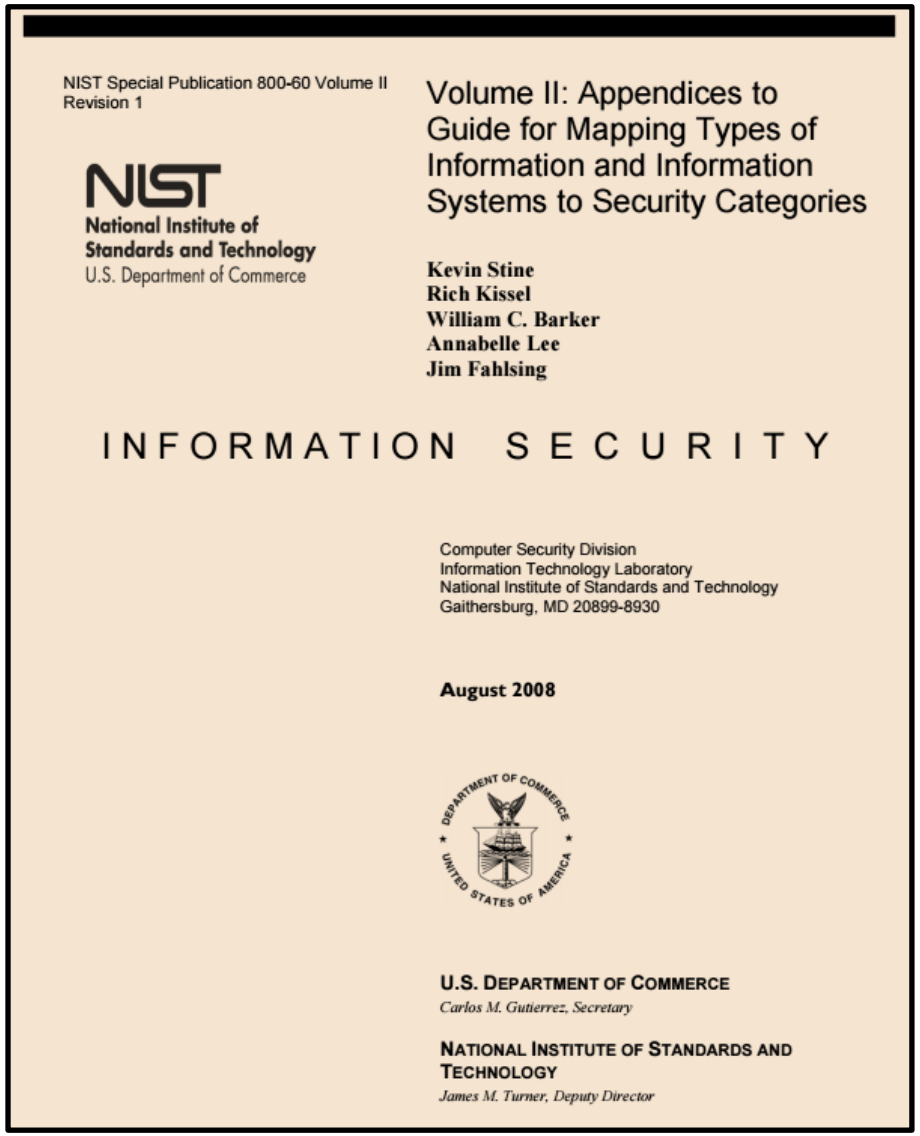
INFORMATION SECURITY

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



NIST Special Publication 800-60 Volume II
Revision 1

NIST
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

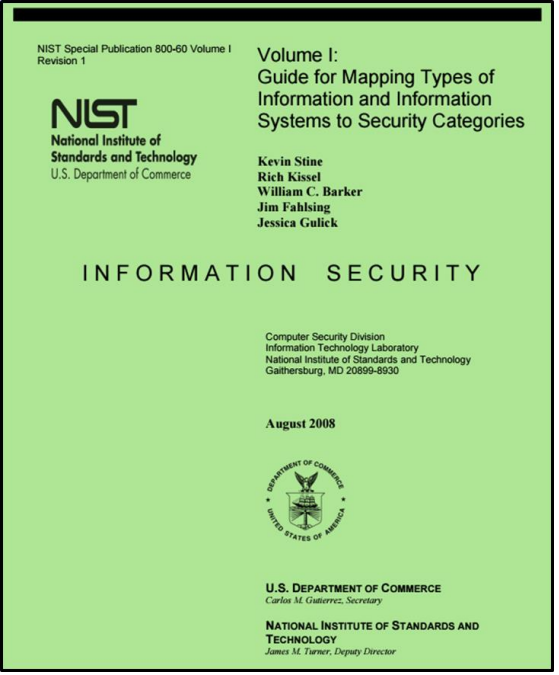
INFORMATION SECURITY

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



http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

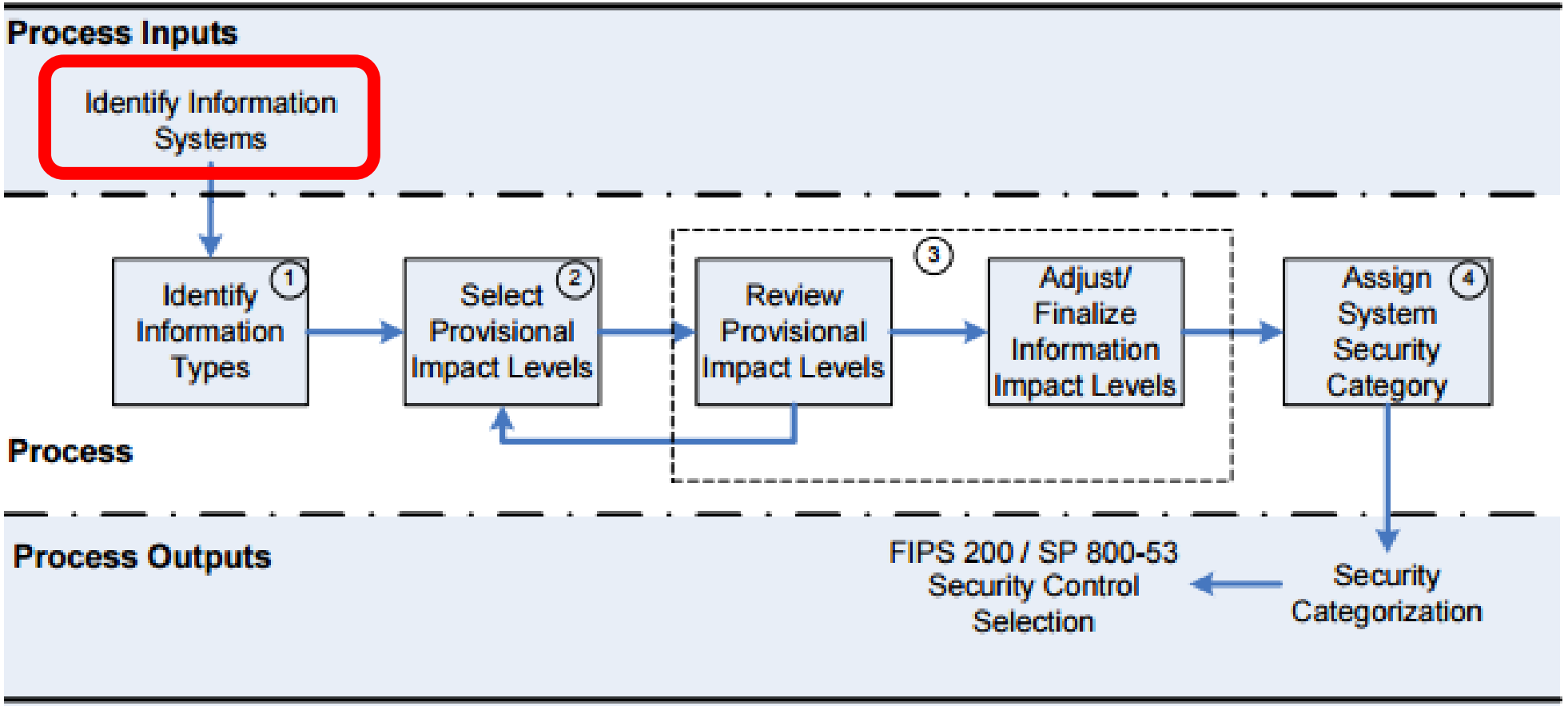
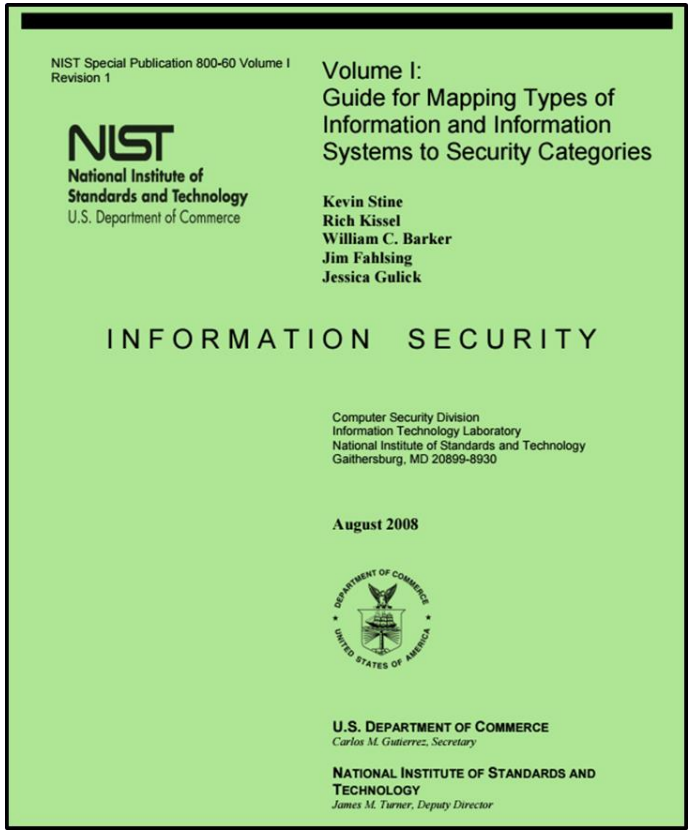


Figure 2: SP 800-60 Security Categorization Process Execution

2 Broad types of Information and Information Systems

1. **Mission-based Information & Information Systems**

2. Management and Support Information & Information Systems



NIST Special Publication 800-60 Volume I
Revision 1

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

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

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

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

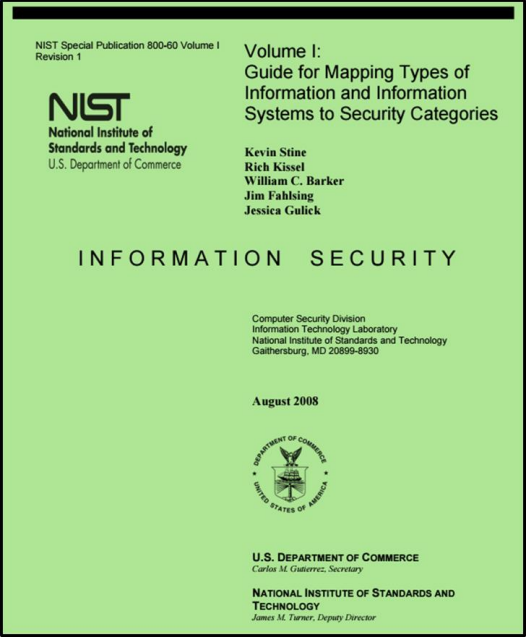
August 2008

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

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

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
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


NIST Special Publication 800-60 Volume I
Revision 1

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

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

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

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 Broad Types of Information and Information Systems

1. Mission-based Information & Information Systems

2. **Management and Support Information & Information Systems**

   i. **Services Delivery Support Functions**

   ii. **Government Resource Management Functions**

Services Delivery Support Functions and Information Types

1. Controls and Oversight
2. Regulatory Development
3. Planning and Budgeting
4. Internal Risk Management and Mitigation
5. Revenue Collection
6. Public Affairs
7. Legislative Relations
8. General Government

Government Resource Management Functions & Information Types

1. Administrative Management
2. Financial Management
3. Human Resources Management
4. Supply Chain Management
5. Information and Technology Management

Disaster Management Information Types

D.4 Disaster Management

Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

Table 4: Mission-Based Information

Mission Areas and Information

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
Intelligence Processing

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

D.5 International Affairs & 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.7 Ene
Energy Supply
Energy Conservation a
Energy Resource Man
Energy Production

D.8 Environmenta
Environmental Monito
Forecasting
Environmental Remed
Pollution Prevention a

D.9 Economic D
Business and Industry
Intellectual Property P
Financial Sector Overs
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

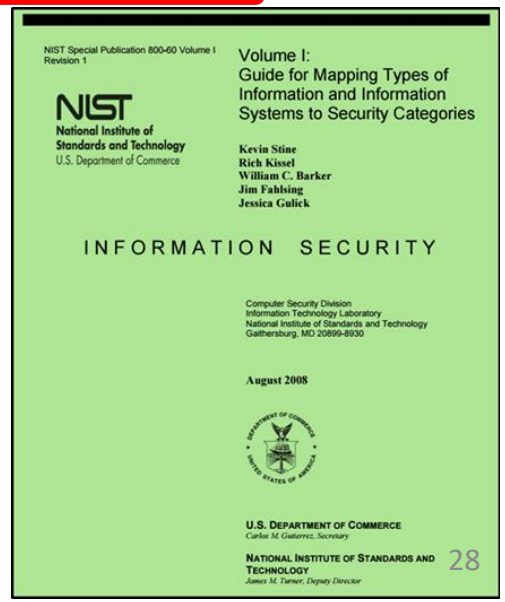
D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

Mode of Delivery]

D.24 Credit and Insurance
Direct Loans
Loan Guarantees
General Insurance

D.25 Transfers to State/ Local Governments
Formula Grants
Project/Competitive Grants
Earmarked Grants
State Loans

D.26 Direct Services for Citizens
Military Operations
Civilian Operations


NIST Special Publication 800-60 Volume I Revision 1

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

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

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

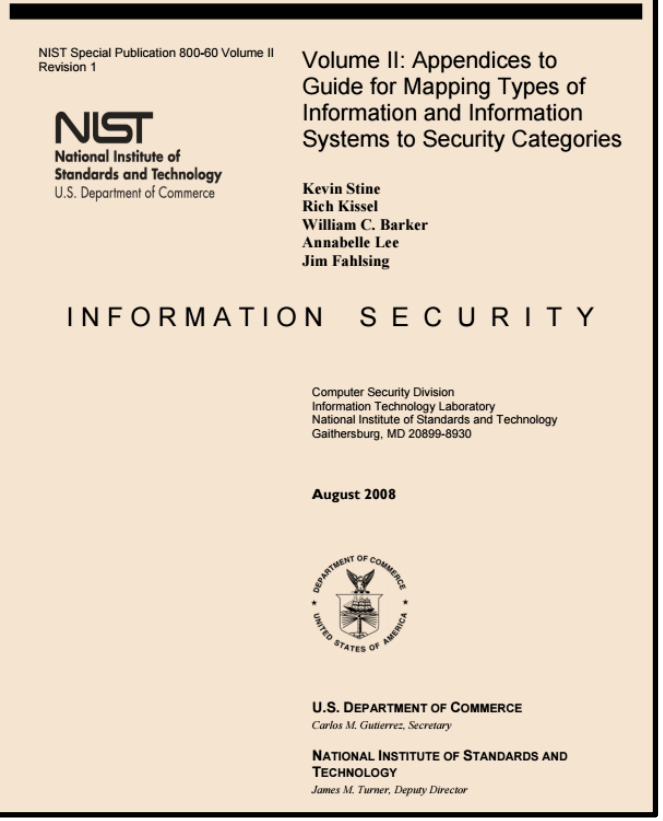
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

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


NIST Special Publication 800-60 Volume II Revision 1

NIST 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

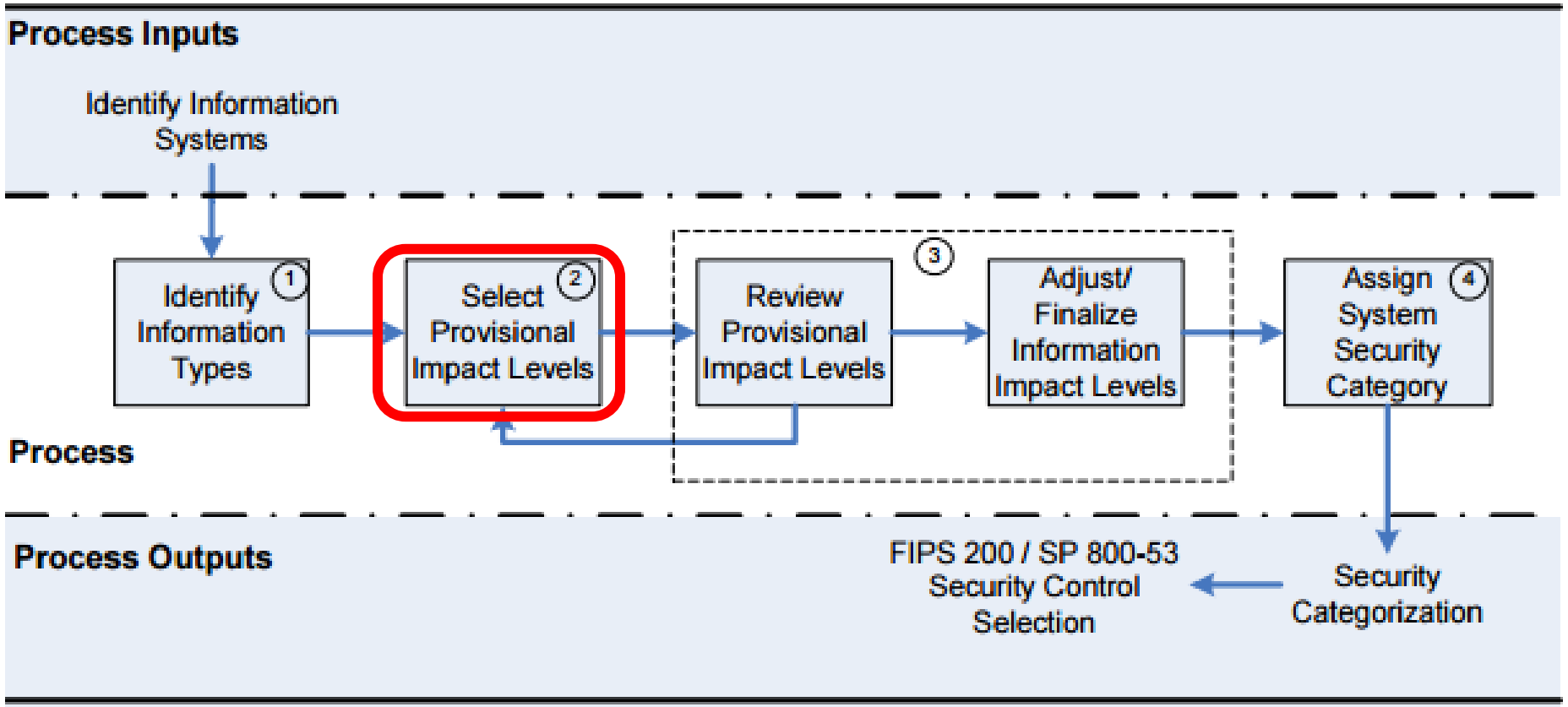
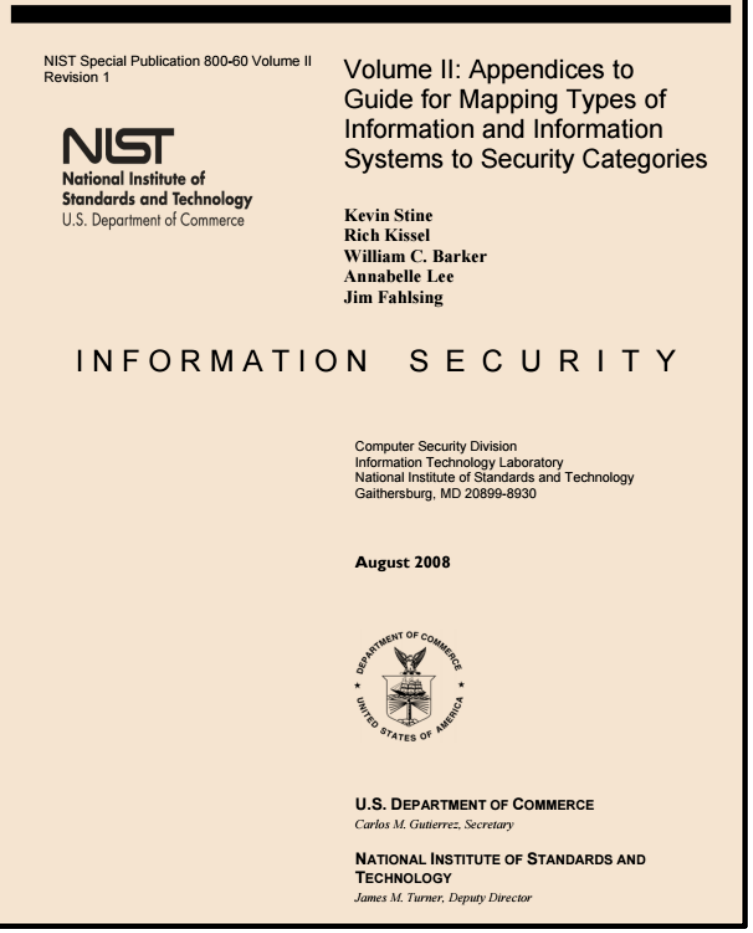


Figure 2: SP 800-60 Security Categorization Process Execution

Disaster Management Information Types



NIST Special Publication 800-60 Volume II
Revision 1

NIST
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

Disaster Management Information Impact

D.4 Disaster Management

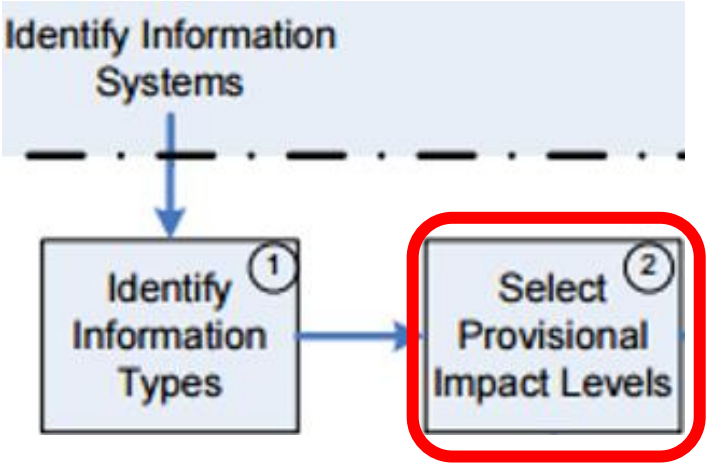
Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made. Compromise of much information associated with any of the missions within the disaster management mission area may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

Exercise

- *Using [NIST SP 800-60 V.2 R1](#) determine the Impact Levels for the Disaster Information Types*

Disaster Management Information Systems				
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	?	?	?	?
Disaster Preparedness and Planning	?	?	?	?
Disaster Repair and Restoration	?	?	?	?
Emergency Response Information Type	?	?	?	?
Information System Impact Rating:	?	?	?	?

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:

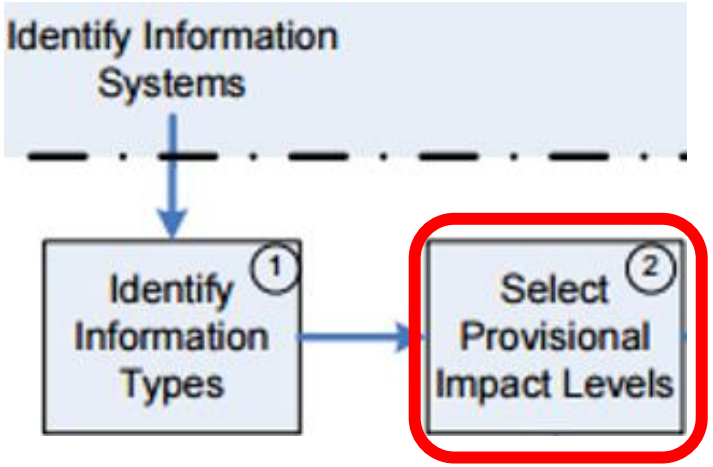
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

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*

Disaster Management Information Systems				
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	?
Disaster Preparedness and Planning	Low	Low	Low	?
Disaster Repair and Restoration	Low	Low	Low	?
Emergency Response Information Type	Low	High	High	?

Determine the Overall Impact Levels for the Disaster Information Types

Disaster Management Information 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:	**?**	**?**	**?**	

Determine the Overall Impact Level of Disaster Information System

Disaster Management Information 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	**?**

Overall Impact Level of Disaster Information Systems

Disaster Management Information 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***

Example

Find a preliminary categorization for the following information system and adjust the categorization based on your analysis – present justifications for both preliminary and adjusted categorizations

Purpose: The system has two overarching purposes:

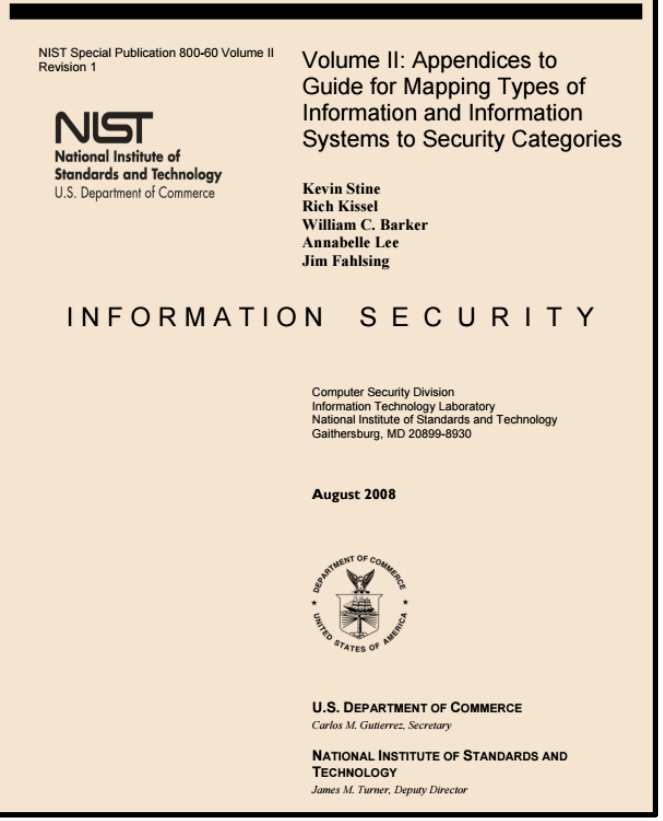
1. For clients it is a system intended to help understand sewage and storm water collection and treatment systems (i.e. pipe networks, pump stations, and treatment plants) and their capacities, overflow characteristics and controls
2. For the firm the system is intended to provide revenue through pay by clients for:
   - Direct use of the service(s) of the system
   - Help in benefiting from the service(s) of the system
   - Having the firm apply the service(s) of the system to derive beneficial information for the clients

Users:

1. Municipal and regional water and sewer utilities and governmental organizations will use the system to help plan capital improvement, operations, and maintenance of sewer systems (i.e. treatment plants and collection networks)
2. External consultants helping municipal and regional water and sewer utilities and organizations will use the system to help their clients plan capital improvement, operations, and maintenance of sewer systems
3. Internal consultants within the firm helping municipal and regional water and sewer utilities and organizations will use the system to help their client plan capital improvement, operations, and maintenance of sewer systems
4. The firm's technical information system development staff will work directly on the information system to provide, maintain, enhance and extend the services of the information system to (1), (2) and (3) above

Solution to Example

Business Area	Business Area ID	Information Type	Confidentiality	Integrity	Availability	Information Type Categorization	Sub-System Categorization	System Categorization
Environmental Management	D.8	Pollution Prevention and Control	Low	Low	Low	Low	***Low***	***Moderate***
Public Goods Creation & Management	D.22	Public Resources, Facility and Infrastructure Management	Low	Low	Low	Low		
		Tenant Data	***Low***	***Low***	***Low***	***Low***		
Information & Technology Management	C.3.5	Information Security	Low	Moderate	Low	Moderate	***Moderate***	
Information & Technology Management	C.3.5	Record Retention	Low	Low	Low	Low		
Information & Technology Management	C.3.5	Information Management	Low	Moderate	Low	Moderate		
Information & Technology Management	C.3.5	System and Network Monitoring	Moderate	Moderate	Low	Moderate		
		System Data	***Moderate***	***Moderate***	***Low***	***Moderate***		



NIST Special Publication 800-60 Volume II Revision 1

NIST 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

3. Adjust Information Impact Level

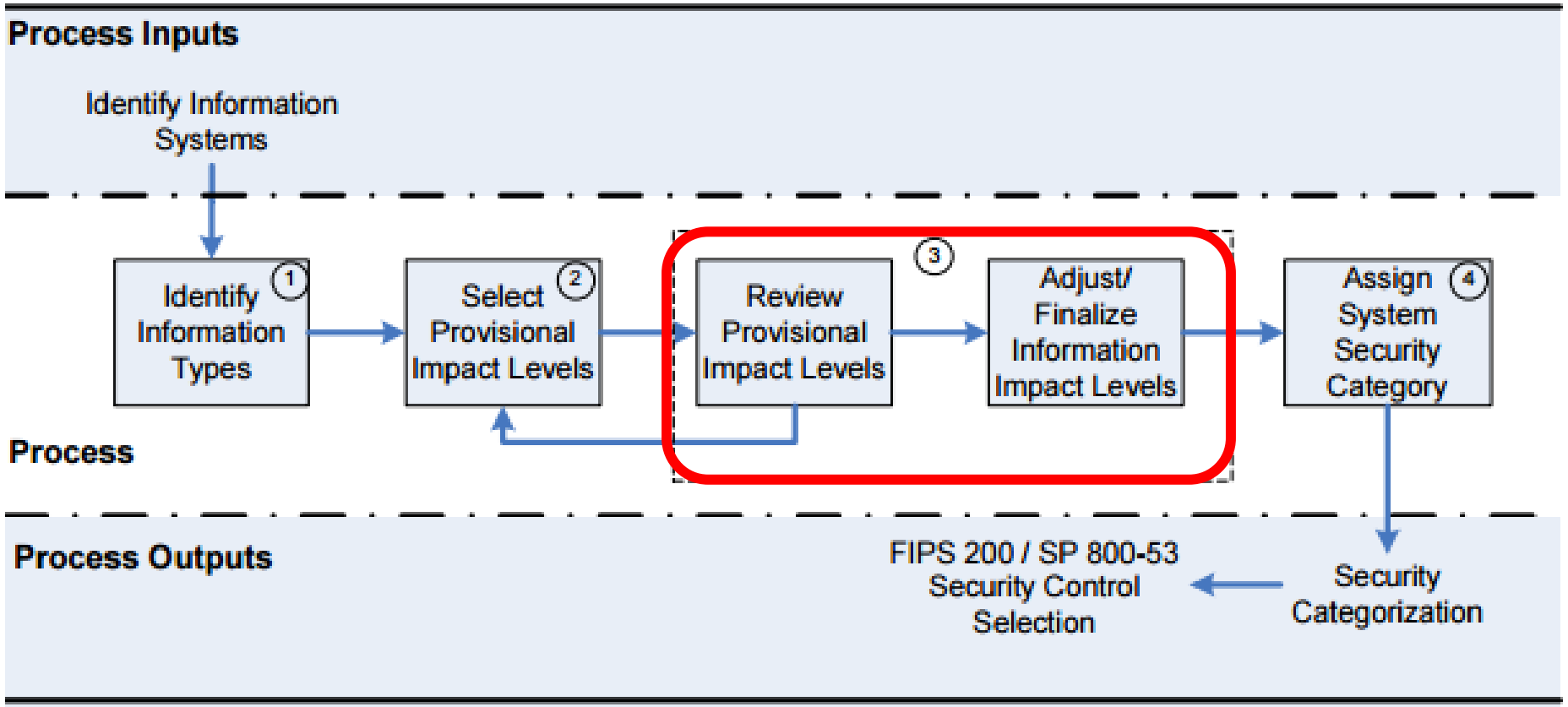


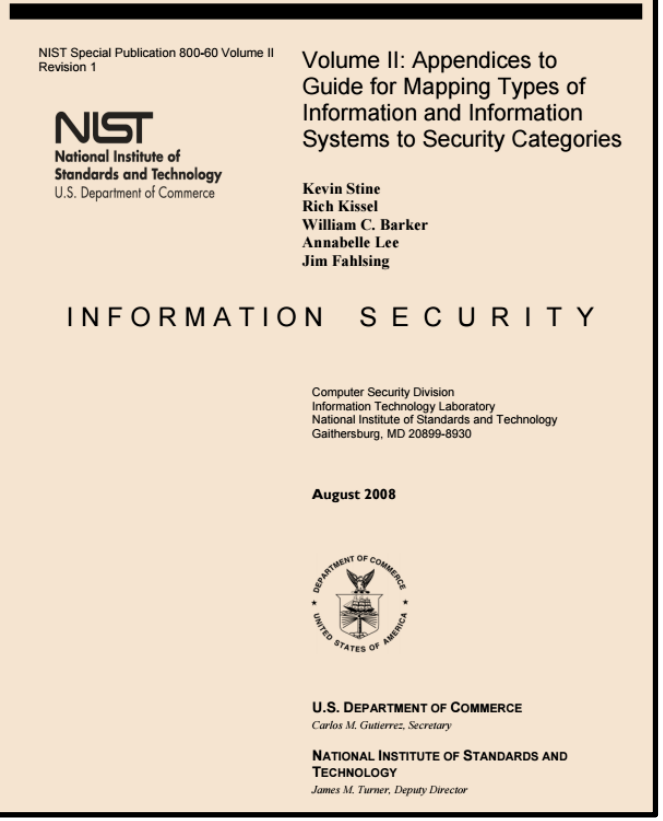
Figure 2: SP 800-60 Security Categorization Process Execution

Pragmatic adjustment of Impact Levels

Using NIST SP 800 60 V2R1

- Look at the “Special Factors” affecting CIA impact levels for each Disaster Management information type
- How would you adjust the CIA impact levels in the table ?

Disaster Management Information 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***



NIST Special Publication 800-60 Volume II Revision 1

NIST 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

2. Select Provisional Impact Levels for the identified information system

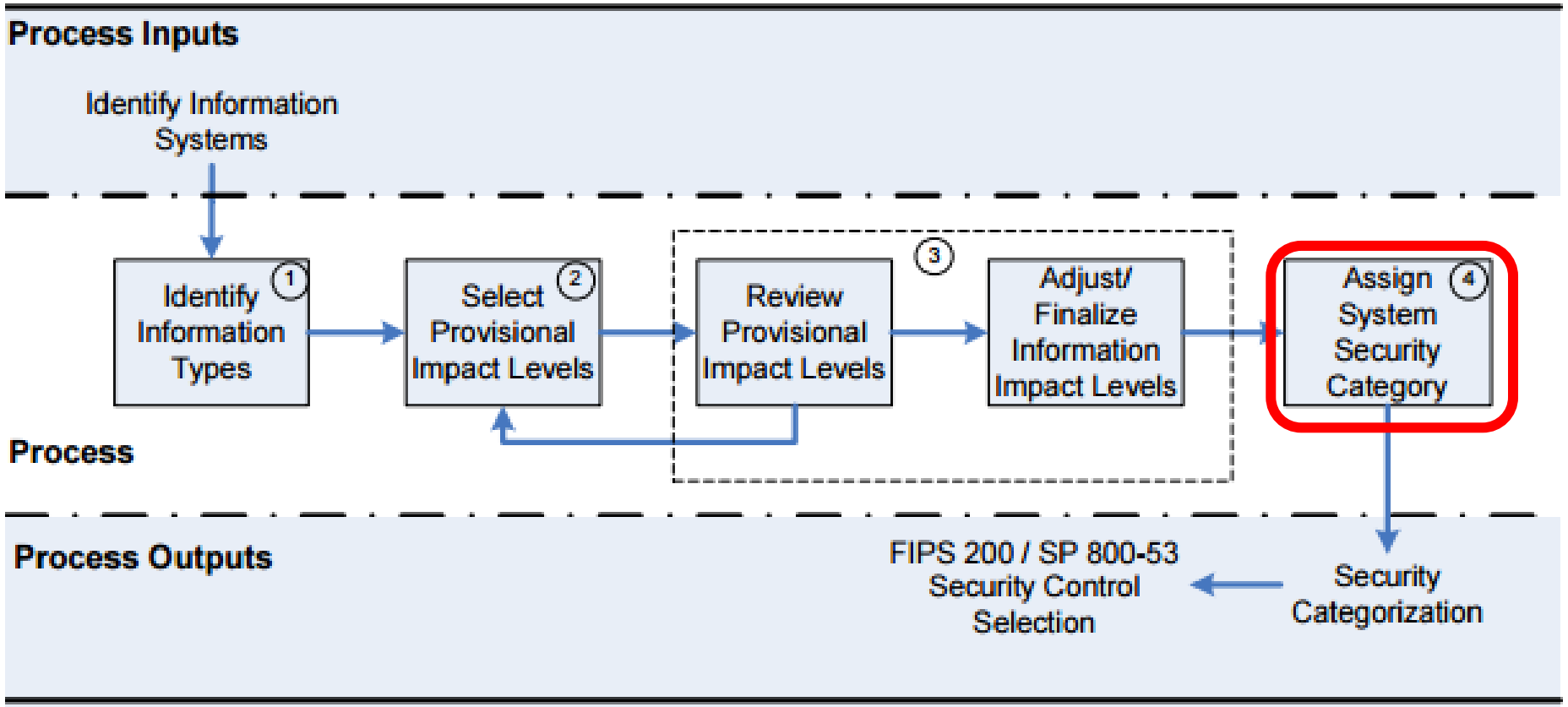


Figure 2: SP 800-60 Security Categorization Process Execution

Milestone 1 – Risk Assessment Report

Section 003

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

Full Name	Email Address	Team
Bui, Philip	tuh10905@temple.edu	1
Hartigan, Kevin P	tuh08175@temple.edu	1
Patel, Ronak H	tuj39052@temple.edu	1
Willie, Matthew R	tuh17418@temple.edu	1
Cho, Seong Beom	tug09558@temple.edu	2
Heesen, Andrew V	tuh01474@temple.edu	2
Saddic, David G	tuh09695@temple.edu	2
Dixon, Sean M	tug73584@temple.edu	3
Khalid, Zeshan H	tuh35907@temple.edu	3
Salavitabar, Sara Rose	tug98919@temple.edu	3
Duggal, Kunal	tug97695@temple.edu	4
Lee, Jin D	tug99823@temple.edu	4
Sohn, Hye-yun	tuh39295@temple.edu	4
English, Luke T	tuh14483@temple.edu	5
Lieu, Nhi	tug57349@temple.edu	5
Swink, Nicholas Ryan	tuh11380@temple.edu	5
Febles, Jordan X	tuh12737@temple.edu	6
O'Donnell, Liam Andrew	tuh04676@temple.edu	6
Tran, Kevin	tug97942@temple.edu	6
Geiger, Jack R	tug90339@temple.edu	7
Patel, Parmita N	tuh18057@temple.edu	7
Wagner, Richard Patrick	tuh05503@temple.edu	7
Sclarow, Steven	tue28808@temple.edu	7

Milestone 1 – Risk Assessment Report

Section 001

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

Full Name	Email Address	Team
Alkaysi, Sajad Ameen	tuh02908@temple.edu	1
Gaither, Cole H	tuh11015@temple.edu	1
Longjohn, Benjamin	tuh28111@temple.edu	1
Yaftali, Usman	tul51458@temple.edu	1
Banford, Gina M	tug92832@temple.edu	2
Gao, Karen	tuh23672@temple.edu	2
Mellon, Emily R	tug90782@temple.edu	2
Batchelder, Grace Caroline	tuj86226@temple.edu	3
Gindele, Emily Rose	tug96353@temple.edu	3
Patel, Snehal Chandrakant	tug97535@temple.edu	3
Brechbill, Emily L	tug98796@temple.edu	4
Gonzalez, David	tuj43022@temple.edu	4
Peake, Dominick	tuh02558@temple.edu	4
Crombie, Mellisa S	tug57106@temple.edu	5
Hilkene, Matthew Robert	tul19250@temple.edu	5
Petruzzelli, Nicholas M	tuh28833@temple.edu	5
Dalessandro, Collin Thomas	tuk31058@temple.edu	6
I Dewa Gede, Parandita	tuh33787@temple.edu	6
Schmon, Andrew R	tug87712@temple.edu	6
Debrosse, Alyssa Marie	tuh12955@temple.edu	7
Jurgelewicz, Patrick	tug98658@temple.edu	7
Swiatek, Luke M	tug97552@temple.edu	7

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