Unit #1b

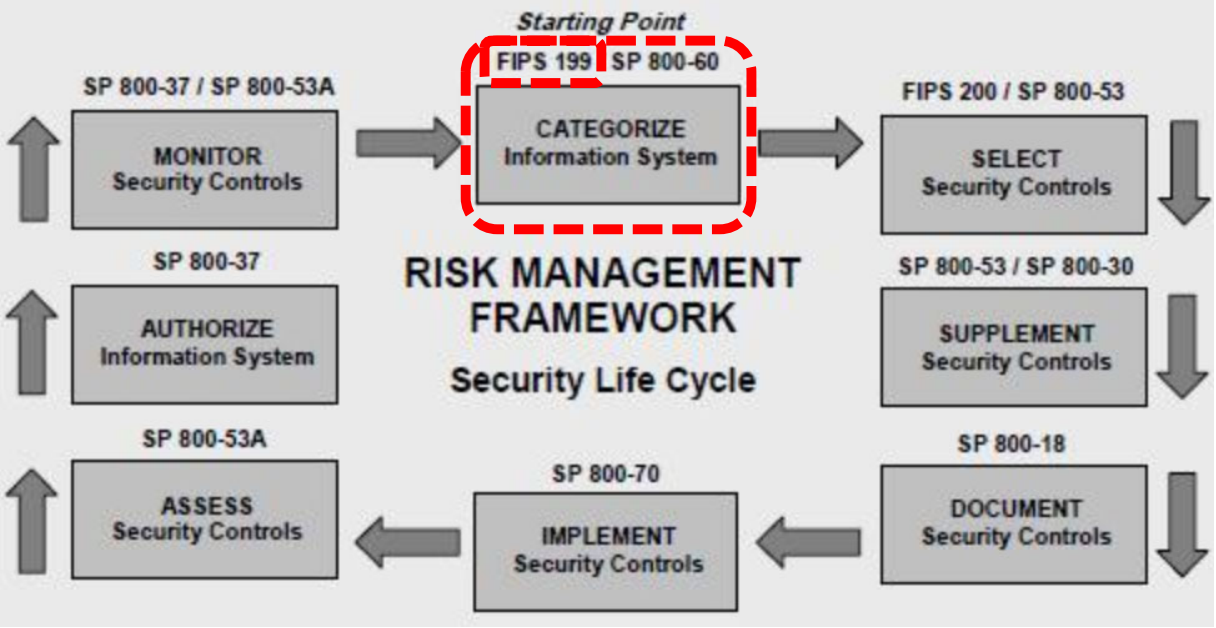
MIS5214

Planning and Policy

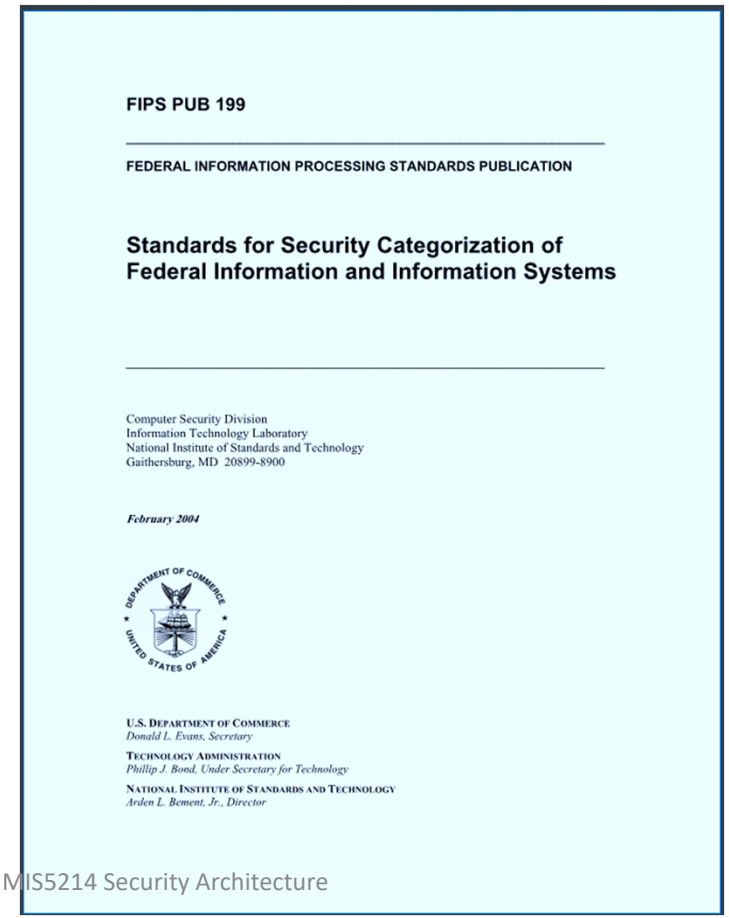
Agenda

- Risk Management Framework and IS Security Categorization
- Mapping Information Types to Security Categorizations
- *Exercise: How to assess and information security policy?*
- *Exercise – Determine Information and Information System Types and provisional security categorization*
- Security Control Baselines – review
  - Minimum Security Controls and Security Control Baselines
  - Security Control Families
- Planning Controls

Risk Management Framework



Risk Assessment based on security objectives and impact ratings for information and information system



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

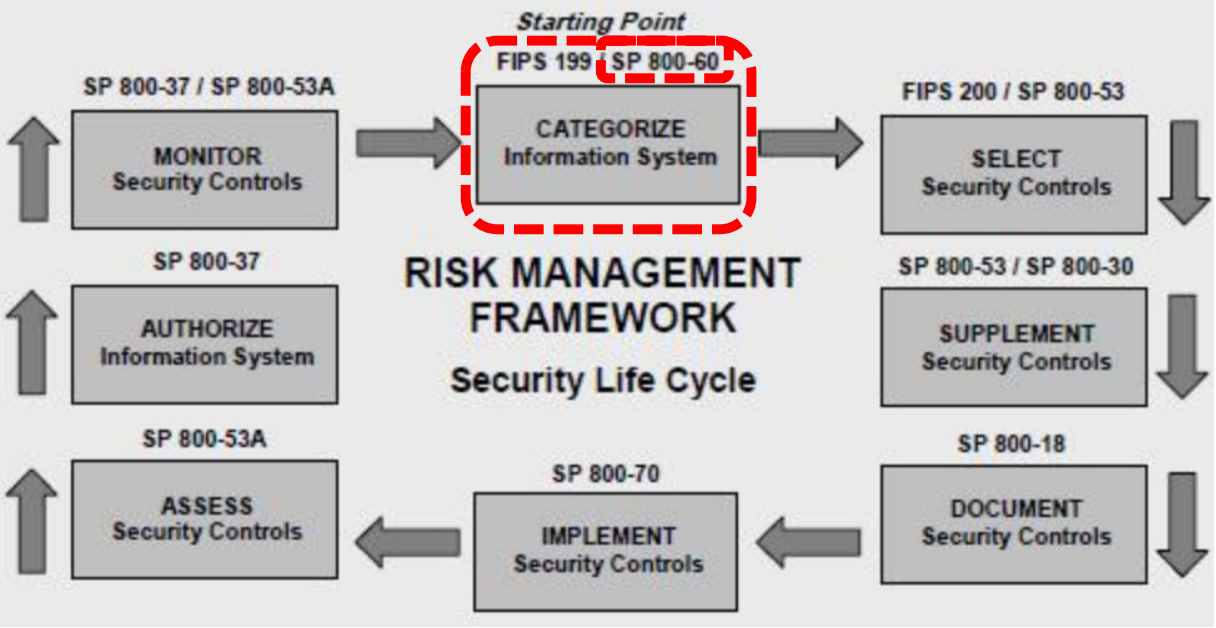
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

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.

Risk Management Framework



Mapping IS Types to Security Categories

1. Administrative and Financial Systems

Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Financial Systems (e.g., Payroll, Budgeting)	Moderate	High	Moderate	**Moderate-High**
Human Resources Systems (e.g., Employee Records)	High	Moderate	Moderate	**Moderate-High**
E-Government Systems (e.g., Public Portals, Online Services)	Moderate	Moderate	Moderate	**Moderate**
E-Commerce Systems (e.g., Online Transactions, Payment Processing)	High	High	Moderate	**High**

2. Public and Safety-Critical Systems

Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Law Enforcement Systems (e.g., Criminal Databases, Investigation Records)	High	High	High	**High**
Public Safety Systems (e.g., Emergency Response, Fire Dispatch)	Moderate	High	High	**High**
Military Systems (e.g., Command and Control, Weapon Systems)	High	High	High	**High**

3. Healthcare and Research Systems

Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Healthcare Systems (e.g., Patient Records, EHR)	High	High	High	**High**
Research and Development Systems (e.g., Experimental Data, Prototypes)	Moderate	High	Moderate	**Moderate-High**

4. Industrial and Infrastructure Control Systems

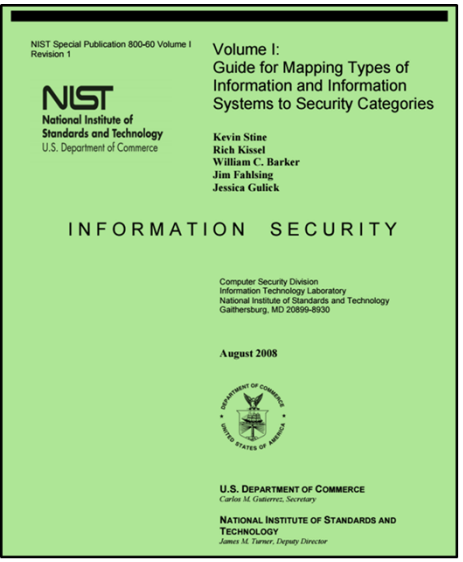
Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Industrial Control Systems (ICS) (e.g., SCADA, Power Grid Management)	Low	High	High	**High**
Telecommunication Systems (e.g., Network Infrastructure, VoIP)	Moderate	High	High	**High**

5. Education and Public-Facing Systems

Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Academic and Learning Systems (e.g., Student Records, Online Learning)	Moderate	Moderate	Low	**Moderate**
Public Websites (e.g., Informational, News Portals)	Low	Moderate	Moderate	**Moderate**

6. Cloud and Digital Service Systems

Information System Type	Confidentiality Impact	Integrity Impact	Availability Impact	Overall Security Category
Cloud Service Systems (e.g., Government Cloud, SaaS Services)	High	High	High	**High**



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

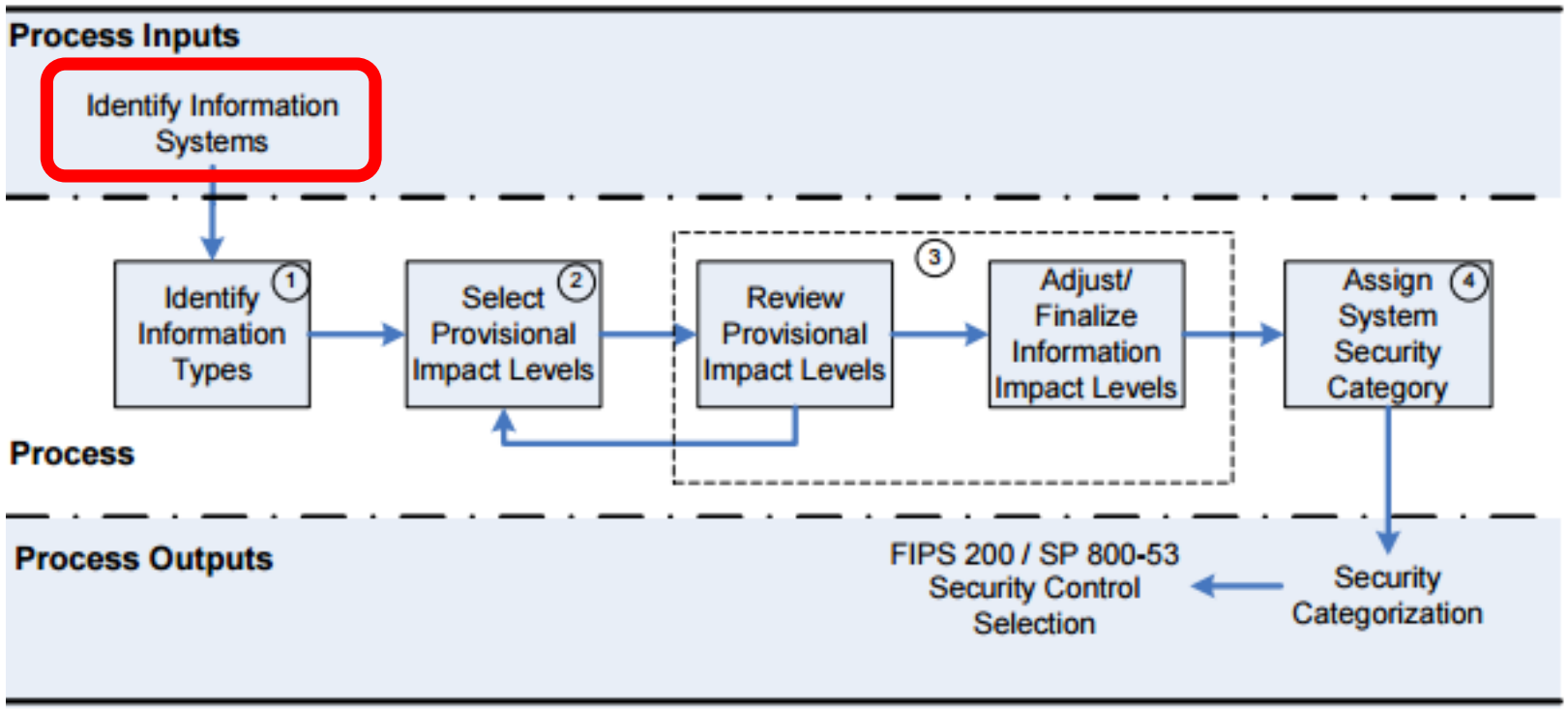
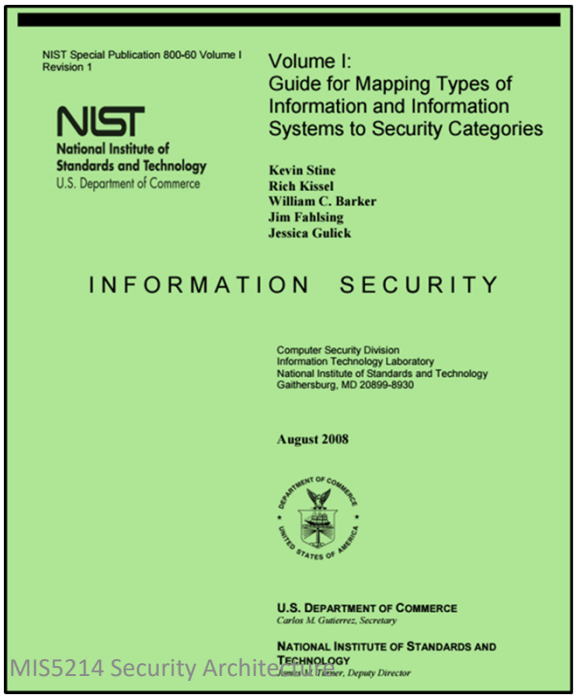


Figure 2: SP 800-60 Security Categorization Process Execution

2 Broad types of Information and Information Systems

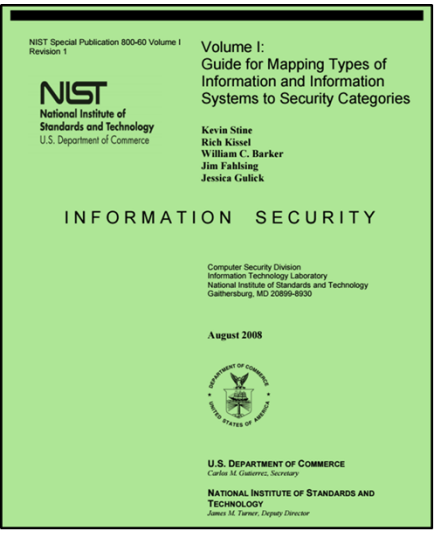
1. **Mission-based Information & Information Systems**

2. Management and Support Information & Information Systems



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



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

Example Management & Support Information & Information Systems

Table 5: Services Delivery Support Functions and Information Types[15]

C.2.1 Controls and Oversight	C.2.4 Internal Risk Management & Mitigation	C.2.8 General Government
Corrective Action (Policy/Regulation)	Contingency Planning	Central Fiscal Operations
Program Evaluation	Continuity of Operations	Legislative Functions
Program Monitoring	Service Recovery	Executive Functions
C.2.2 Regulatory Development	**C.2.5 Revenue Collection**	Central Property Management
Policy & Guidance Development	Debt Collection	Central Personnel Management
Public Comment Tracking	User Fee Collection	Taxation Management
Regulatory Creation	Federal Asset Sales	Central Records & Statistics Management
Rule Publication	**C.2.6 Public Affairs**	*Income Information*
C.2.3 Planning & Budgeting	Customer Services	*Personal Identity and Authentication*
Budget Formulation	Official Information Dissemination	*Entitlement Event Information*
Capital Planning	Product Outreach	*Representative Payee Information*
Enterprise Architecture	Public Relations	*General Information*
Strategic Planning	**C.2.7 Legislative Relations**	
Budget Execution	Legislation Tracking	
Workforce Planning	Legislation Testimony	
Management Improvement	Proposal Development	
Budgeting & Performance Integration	Congressional Liaison Operations	
Tax & Fiscal Policy		

Example Resource Management Functions & Information Types

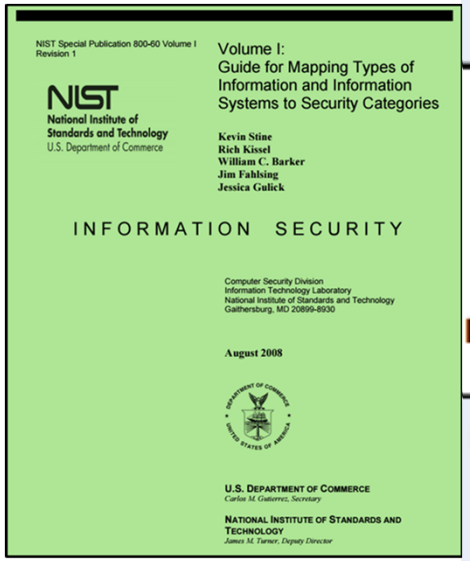
1. Administrative Management
2. Financial Management
3. Human Resources Management
4. Supply Chain Management
5. Information and Technology Management

Example Management and Support Information and Information Systems

Table 6: Government Resource Management Functions and Information Types[16]

C.3.1 Administrative Management	C.3.3 Human Resource Management	C.3.5 Information & Technology Management
Facilities, Fleet, and Equipment Management	HR Strategy	System Development
Help Desk Services	Staff Acquisition	Lifecycle/Change Management
Security Management	Organization & Position Mgmt	System Maintenance
Travel	Compensation Management	IT Infrastructure Maintenance
Workplace Policy Development & Management	Benefits Management	Information Security
C.3.2 Financial Management	Employee Performance Mgmt	Record Retention
Accounting	Employee Relations	Information Management
Funds Control	Labor Relations	System and Network Monitoring
Payments	Separation Management	Information Sharing
Collections and Receivables	Human Resources Development	
Asset and Liability Management	**C.3.4 Supply Chain Management**	
Reporting and Information	Goods Acquisition	
Cost Accounting/ Performance Measurement	Inventory Control	
	Logistics Management	
	Services Acquisition	

1. Identify Information Types



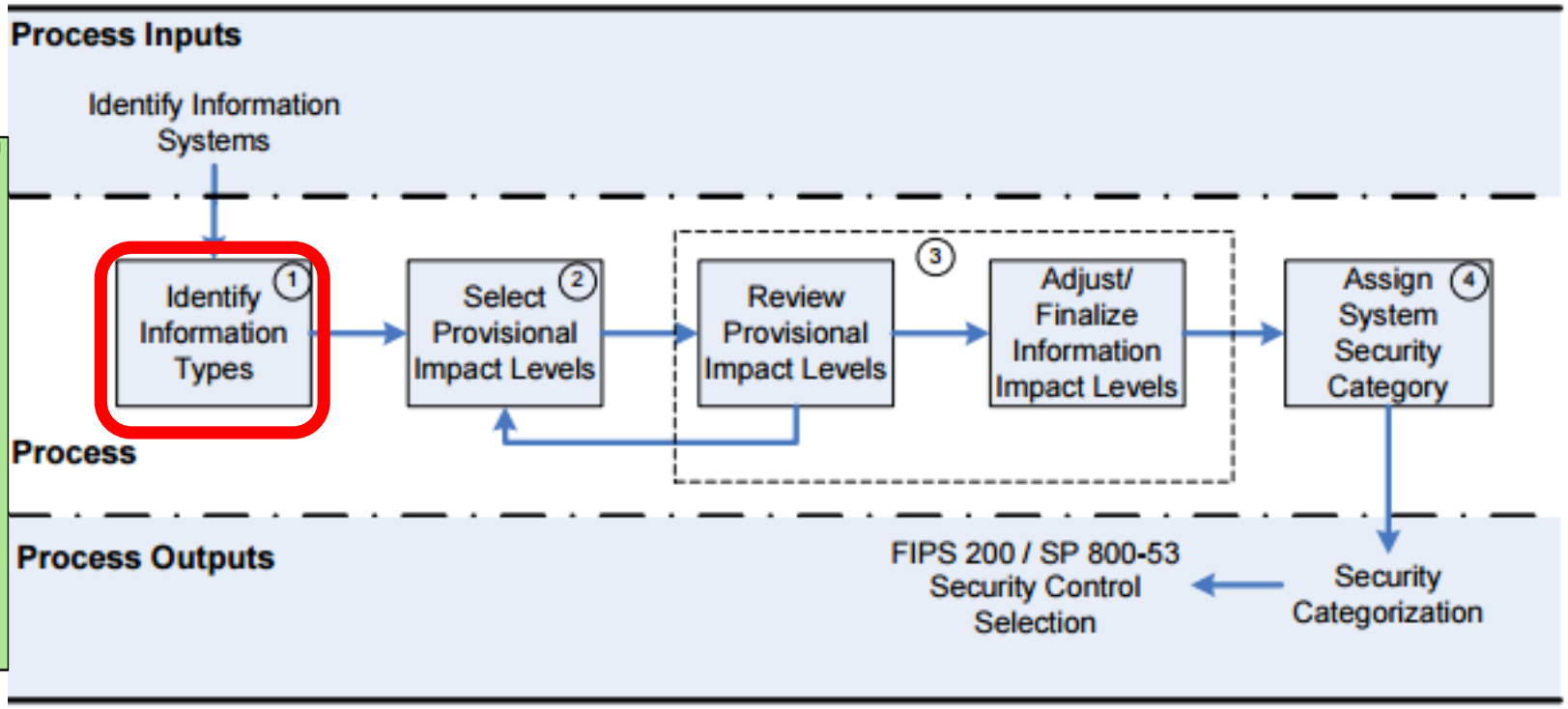


Figure 2: SP 800-60 Security Categorization Process Execution

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

Disaster Management Information Types

Table 4: Mission-Based Infor

Mission Areas and Infor

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

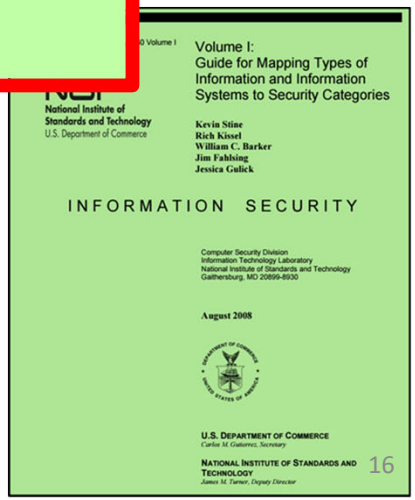
Energy Supp
Energy Cons
Energy Reso
Energy Prod
D.8 Envi
Environment
Forecastin
Environment
Pollution Pre
D.9 Ec
Business and
Intellectual
Financial Se
Industry Sect
D.10 Com
Homeowners
Community
Social Services
Postal Services
D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
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

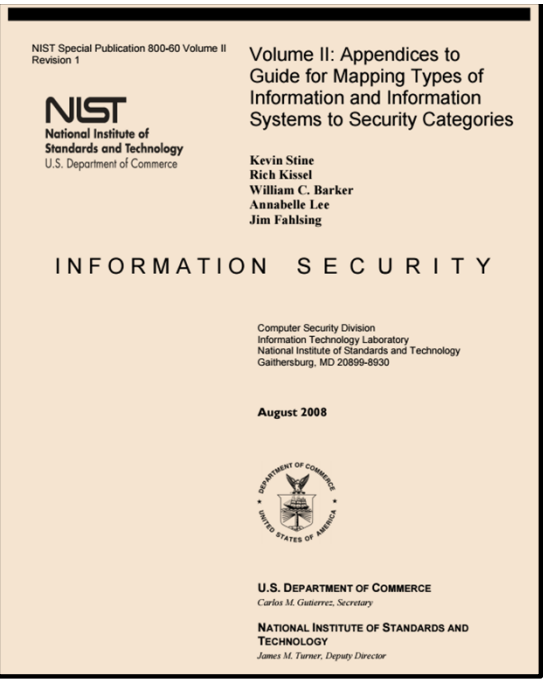
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement
D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation
D.18 Federal Correctional Activities
Criminal Incarceration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

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

Types [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





2. Select Provisional Impact Levels for the identified information system

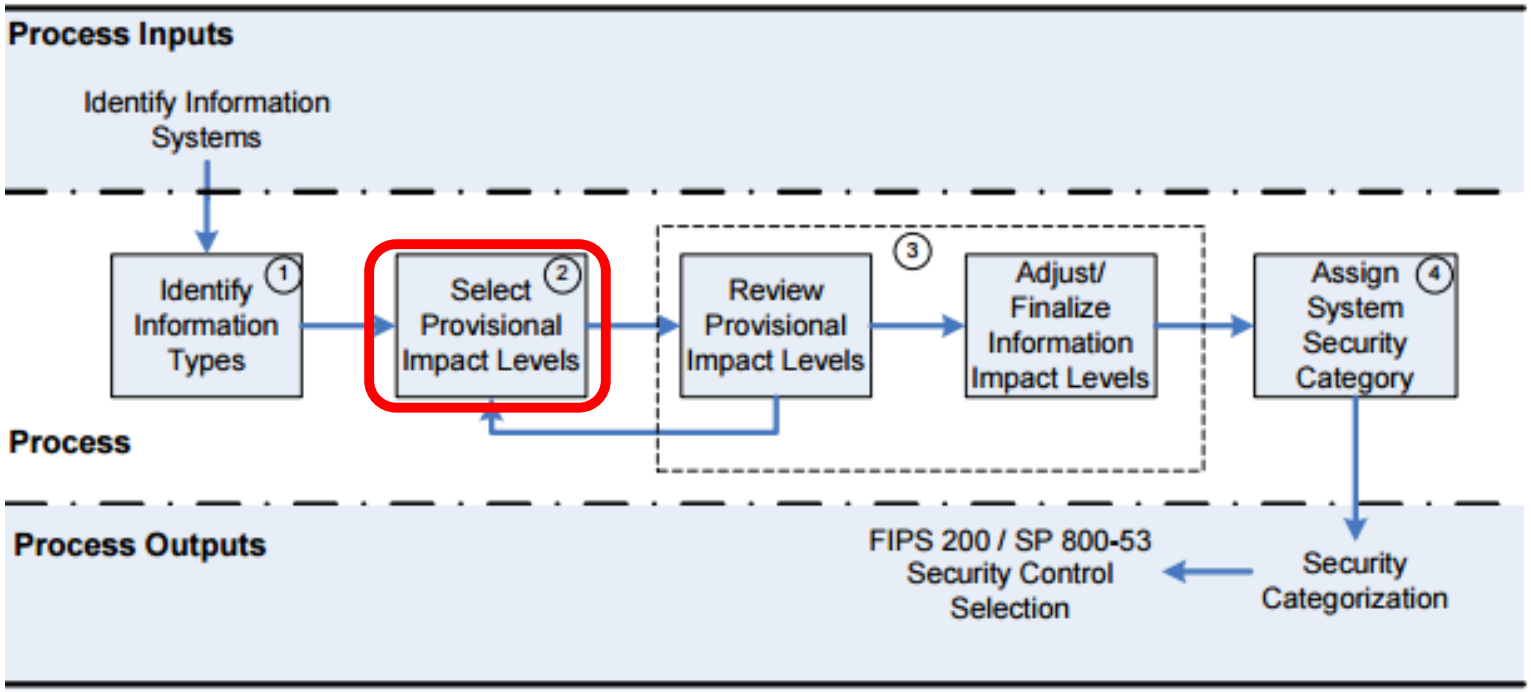
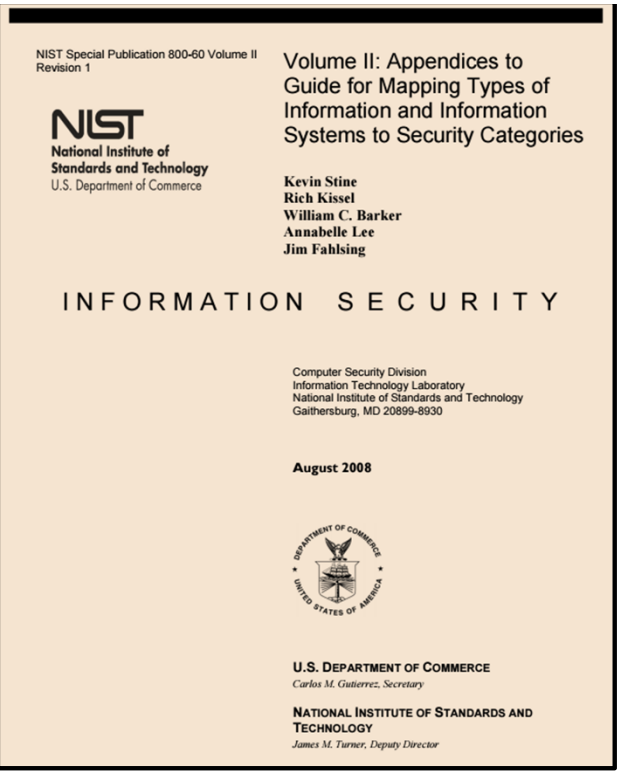


Figure 2: SP 800-60 Security Categorization Process Execution


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

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

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 107

D.2 Homeland Security 108
D.2.1 Border and Transportation Security Information Type 108
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 Type 112

D.3 Intelligence Operations 113

D.4 Disaster Management 115
D.4.1 Disaster Monitoring and Prediction Information Type 116
D.4.2 Disaster Preparedness and Planning Information Type 117
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

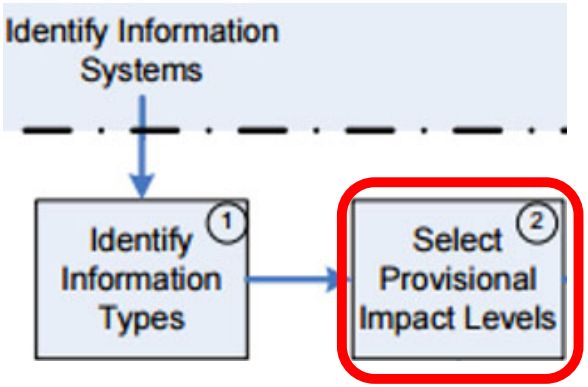
Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all physical and humanitarian disasters whether natural or man-made. Compromise of much information associated with any of the missions within the disaster management mission area may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

Can you use…

- *NIST SP 800-60 V.2 R1 to 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	?	?	?	

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:

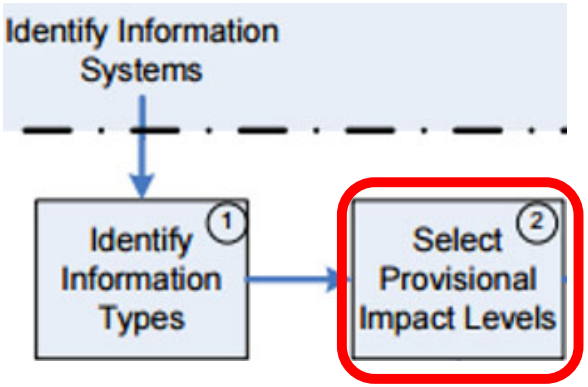
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

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)}

Question

- *Can you determine Summary Impact Levels for 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	?

Answer…

- *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	***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***

Question -

- *Can you determine Overall Impact Levels for 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:	**?**	**?**	**?**	

Answer

- *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:	Low	High	High	

Question

- *Can you determine overall Impact Level of a system of Disaster Information Systems ?*

Disaster Management Information Systems

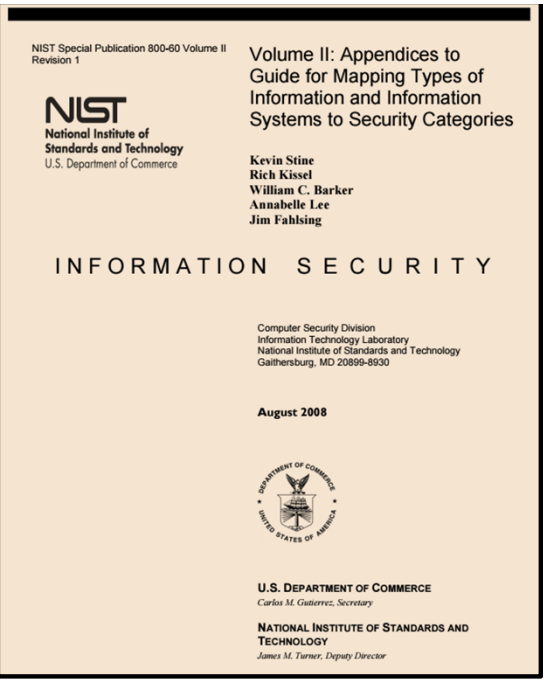
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	***High***
Disaster Preparedness and Planning	Low	Low	Low	***Low***
Disaster Repair and Restoration	Low	Low	Low	***Low***
Emergency Response Information Type	Low	High	High	***High***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

Answer

- *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***



3. Adjust Information Impact Level

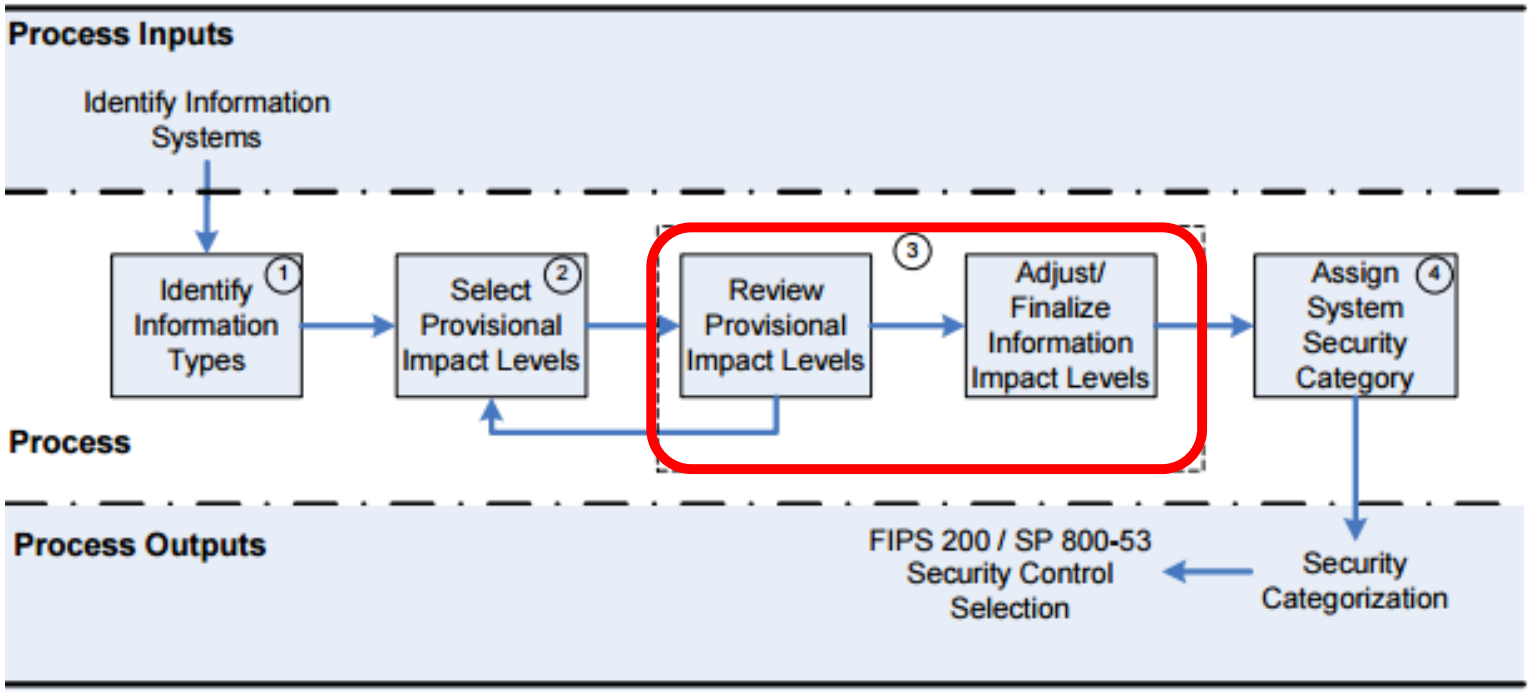


Figure 2: SP 800-60 Security Categorization Process Execution

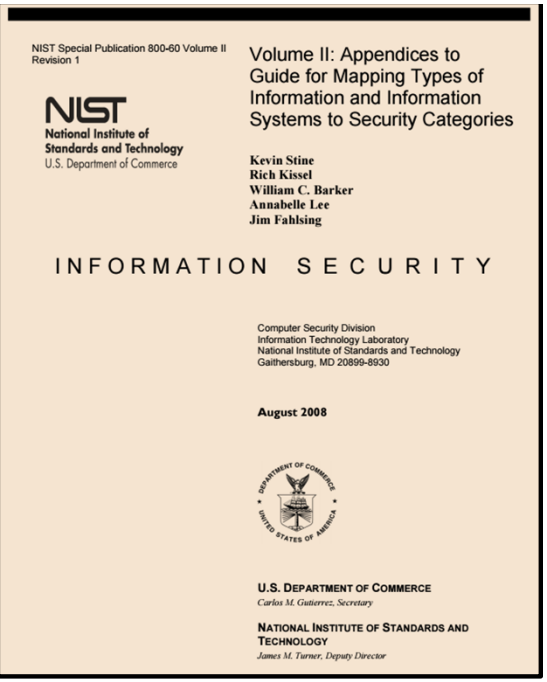
To adjust preliminary impact levels…

Use NIST SP 800 60 V2R1

- …looking at the "**Special Factors**" affecting CIA impact levels for each Disaster Management information type
- How might we adjust the impact levels ?

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***



2. Select Provisional Impact Levels for the identified information system

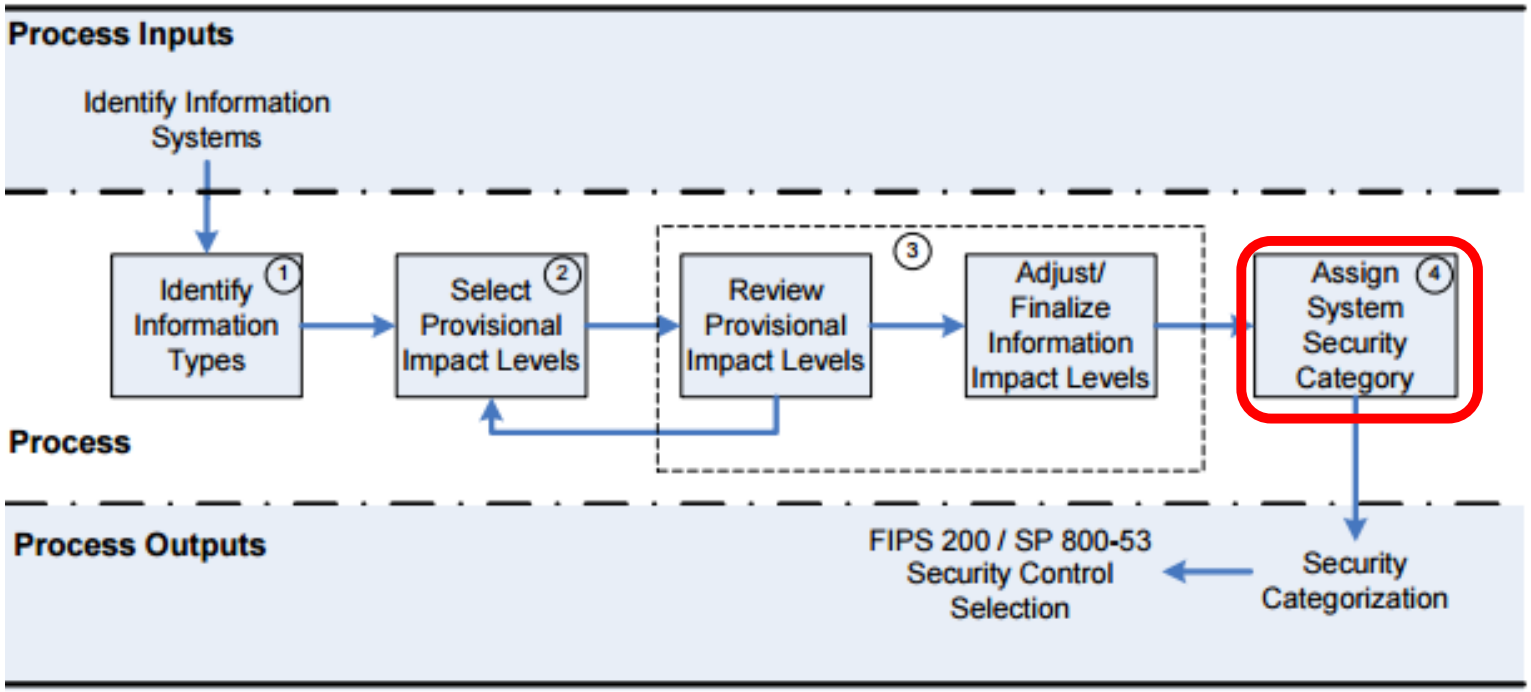
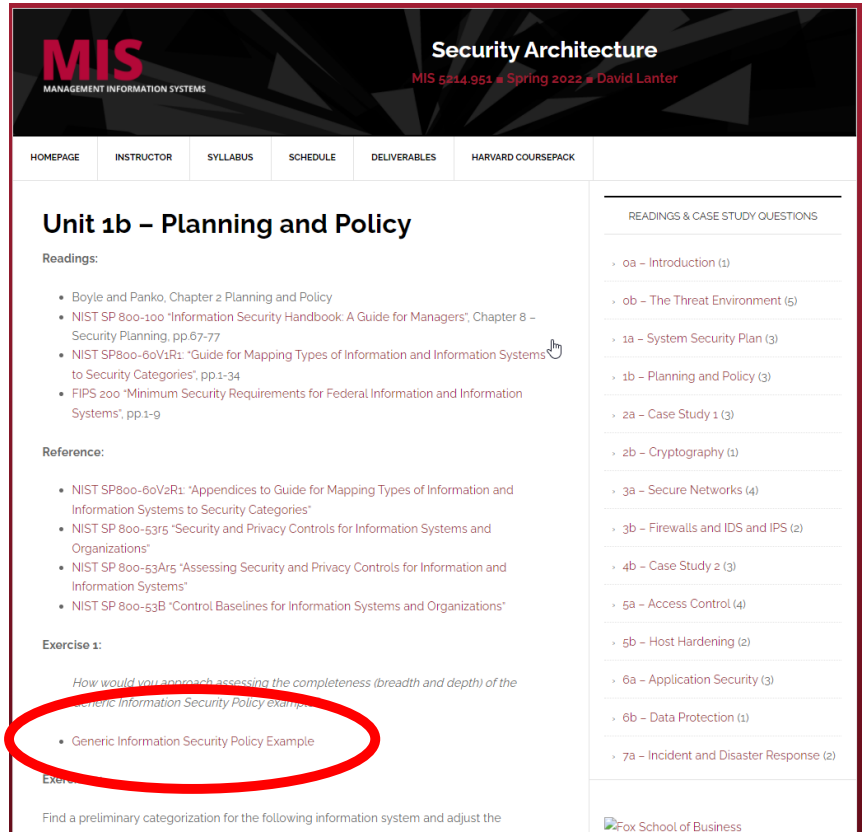


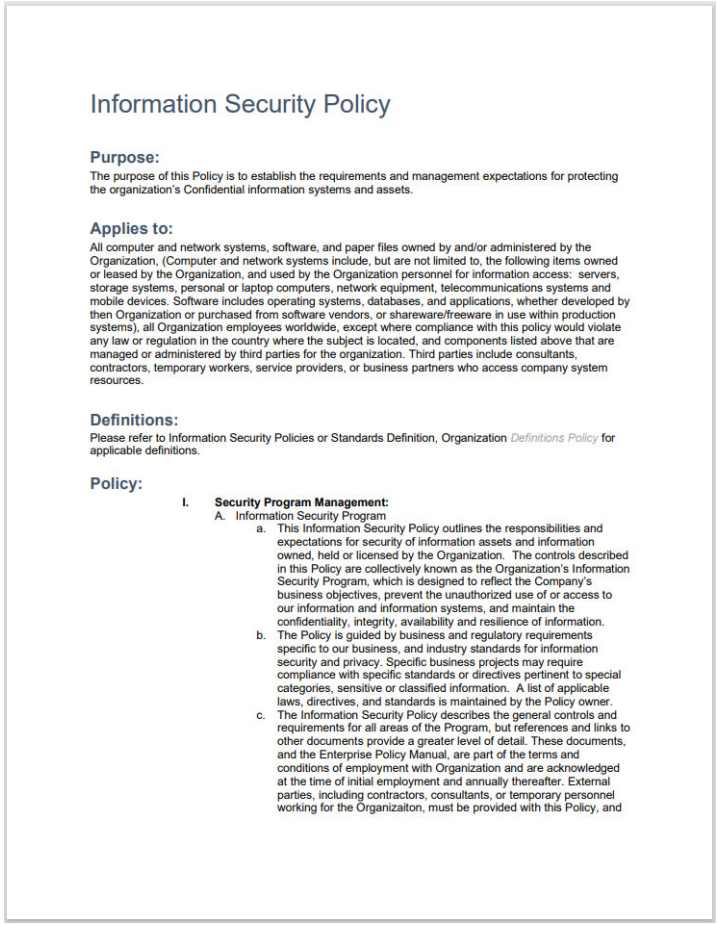
Figure 2: SP 800-60 Security Categorization Process Execution

Teams in Breakout Rooms

How would you approach assessing the completeness (breadth & depth) of the Generic Information Security Policy example, assuming it is the only such policy the firm has?

Exercise: How would you approach assessing the completeness (breadth & depth) of the [Generic Information Security Policy](#) example?





Information Security Policy

Purpose:

The purpose of this Policy is to establish the requirements and management expectations for protecting the organization's Confidential information systems and assets.

Applies to:

All computer and network systems, software, and paper files owned by and/or administered by the Organization, (Computer and network systems include, but are not limited to, the following items owned or leased by the Organization, and used by the Organization personnel for information access: servers, storage systems, personal or laptop computers, network equipment, telecommunications systems and mobile devices. Software includes operating systems, databases, and applications, whether developed by then Organization or purchased from software vendors, or shareware/freeware in use within production systems), all Organization employees worldwide, except where compliance with this policy would violate any law or regulation in the country where the subject is located, and components listed above that are managed or administered by third parties for the organization. Third parties include consultants, contractors, temporary workers, service providers, or business partners who access company system resources.

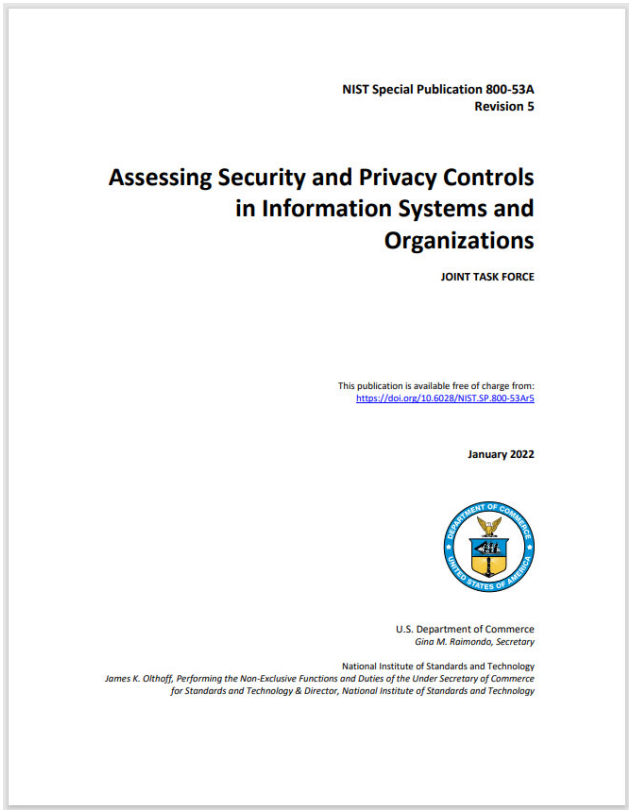
Definitions:

Please refer to Information Security Policies or Standards Definition, Organization *Definitions Policy* for applicable definitions.

Policy:

I. **Security Program Management:**
   A. Information Security Program
      a. This Information Security Policy outlines the responsibilities and expectations for security of information assets and information owned, held or licensed by the Organization. The controls described in this Policy are collectively known as the Organization's Information Security Program, which is designed to reflect the Company's business objectives, prevent the unauthorized use of or access to our information and information systems, and maintain the confidentiality, integrity, availability and resilience of information.
      b. The Policy is guided by business and regulatory requirements specific to our business, and industry standards for information security and privacy. Specific business projects may require compliance with specific standards or directives pertinent to special categories, sensitive or classified information. A list of applicable laws, directives, and standards is maintained by the Policy owner.
      c. The Information Security Policy describes the general controls and requirements for all areas of the Program, but references and links to other documents provide a greater level of detail. These documents, and the Enterprise Policy Manual, are part of the terms and conditions of employment with Organization and are acknowledged at the time of initial employment and annually thereafter. External parties, including contractors, consultants, or temporary personnel working for the Organizaiton, must be provided with this Policy, and

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 classes of NIST SP 800-18 provide a good framework for assessing completeness of Information Security Policies and controls



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

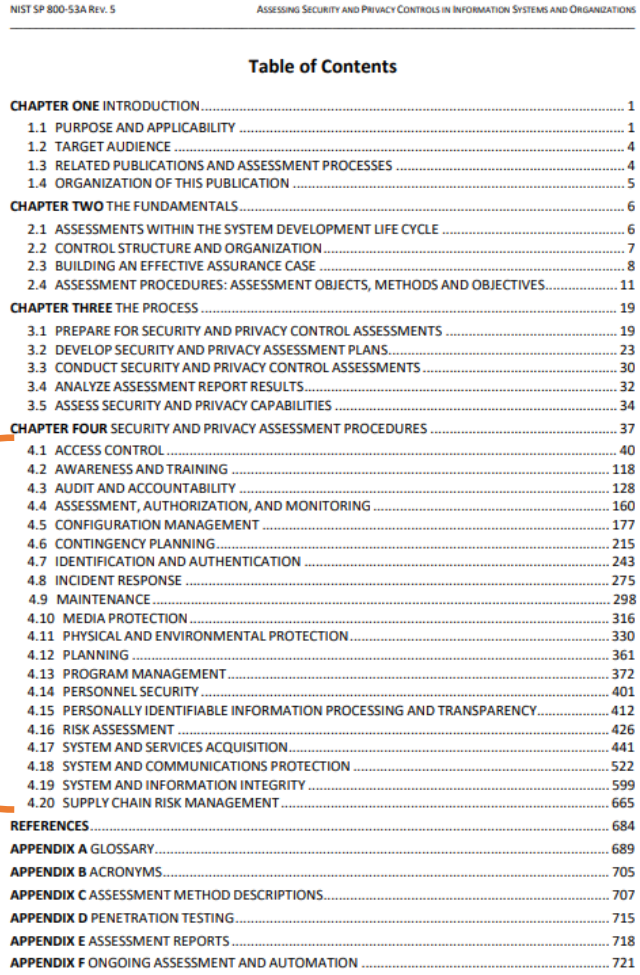
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

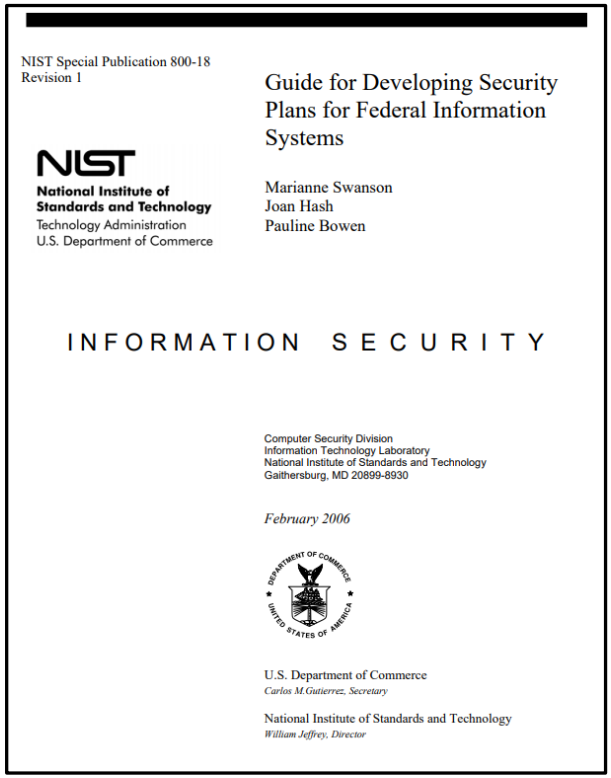


NIST SP 800-53A Rev. 5 — Assessing Security and Privacy Controls in Information Systems and Organizations

Table of Contents

CHAPTER ONE INTRODUCTION 1
1.1 PURPOSE AND APPLICABILITY 1
1.2 TARGET AUDIENCE 4
1.3 RELATED PUBLICATIONS AND ASSESSMENT PROCESSES 4
1.4 ORGANIZATION OF THIS PUBLICATION 5
CHAPTER TWO THE FUNDAMENTALS 6
2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE 6
2.2 CONTROL STRUCTURE AND ORGANIZATION 7
2.3 BUILDING AN EFFECTIVE ASSURANCE CASE 8
2.4 ASSESSMENT PROCEDURES: ASSESSMENT OBJECTS, METHODS AND OBJECTIVES 11
CHAPTER THREE THE PROCESS 19
3.1 PREPARE FOR SECURITY AND PRIVACY CONTROL ASSESSMENTS 19
3.2 DEVELOP SECURITY AND PRIVACY ASSESSMENT PLANS 23
3.3 CONDUCT SECURITY AND PRIVACY CONTROL ASSESSMENTS 30
3.4 ANALYZE ASSESSMENT REPORT RESULTS 32
3.5 ASSESS SECURITY AND PRIVACY CAPABILITIES 34
CHAPTER FOUR SECURITY AND PRIVACY ASSESSMENT PROCEDURES 37
4.1 ACCESS CONTROL 40
4.2 AWARENESS AND TRAINING 118
4.3 AUDIT AND ACCOUNTABILITY 128
4.4 ASSESSMENT, AUTHORIZATION, AND MONITORING 160
4.5 CONFIGURATION MANAGEMENT 177
4.6 CONTINGENCY PLANNING 215
4.7 IDENTIFICATION AND AUTHENTICATION 243
4.8 INCIDENT RESPONSE 275
4.9 MAINTENANCE 298
4.10 MEDIA PROTECTION 316
4.11 PHYSICAL AND ENVIRONMENTAL PROTECTION 330
4.12 PLANNING 361
4.13 PROGRAM MANAGEMENT 372
4.14 PERSONNEL SECURITY 401
4.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY 412
4.16 RISK ASSESSMENT 426
4.17 SYSTEM AND SERVICES ACQUISITION 441
4.18 SYSTEM AND COMMUNICATIONS PROTECTION 522
4.19 SYSTEM AND INFORMATION INTEGRITY 599
4.20 SUPPLY CHAIN RISK MANAGEMENT 665
REFERENCES 684
APPENDIX A GLOSSARY 689
APPENDIX B ACRONYMS 705
APPENDIX C ASSESSMENT METHOD DESCRIPTIONS 707
APPENDIX D PENETRATION TESTING 715
APPENDIX E ASSESSMENT REPORTS 718
APPENDIX F ONGOING ASSESSMENT AND AUTOMATION 721

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 classes of NIST SP 800-18 provide a good framework for assessing completeness of Information Security Policies and controls



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

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

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

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

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

Information Security Control Families of NIST SP 800-53/800-53A grouped within 3 Control Classes of NIST SP 800-18 provide a framework for assessing completeness of Information Security Policies and controls

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

Exercise

Using NIST SP 800-60, 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:

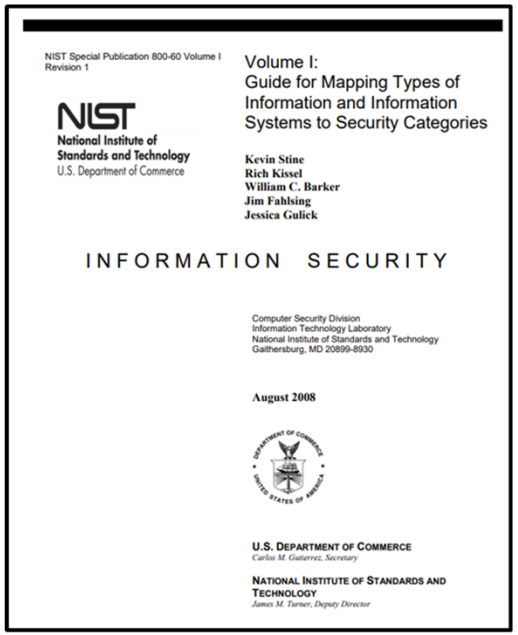
1. For clients it is a system intended to help understand sewage and storm water collection and treatment systems (i.e. pipe networks, pump stations, and treatment plants) and their capacities, overflow characteristics and controls
2. For the firm the system is intended to provide revenue through pay by clients for direct use of the service(s) of the system

Users:

1. Municipal and regional water and sewer utilities and governmental organizations and the contractors that support them will use the system to help plan capital improvement, operations, and maintenance of sewer systems (i.e. treatment plants and sewage collection networks)

Below is a preliminary categorization for the information system based on NIST SP 800-60 Vol

Business Area	Information Type ID	Information Type	Confidentiality	Integrity	Availability	Information Type Categorization	Sub-System Categorization	System Categorization
Environmental Management	D.8.3	Pollution Prevention and Control	Low	Low	Low	Low		
Public Goods Creation & Management	D.22.3	Public Resources, Facility and Infrastructure Management	Low	Low	Low	Low	***Low***	
		Tenant Data	***Low***	***Low***	***Low***	***Low***		
Information & Technology Management	C.3.5.5	Information Security	Low	Moderate	Low	Moderate		
Information & Technology Management	C.3.5.6	Record Retention	Low	Low	Low	Low	***Moderate***	***Moderate***
Information & Technology Management	C.3.5.7	Information Management	Low	Moderate	Low	Moderate		
Information & Technology Management	C.3.5.8	System and Network Monitoring	Moderate	Moderate	Low	Moderate		
		System Data	***Moderate***	***Moderate***	***Low***	***Moderate***		


NIST Special Publication 800-60 Volume I
Revision 1

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

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

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

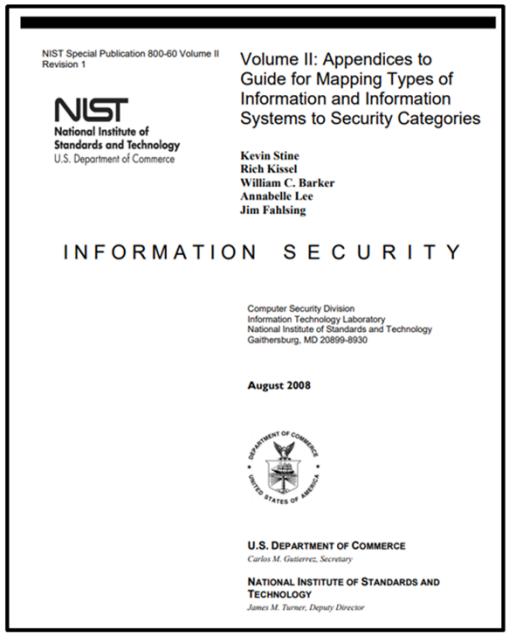
INFORMATION SECURITY

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

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

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

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

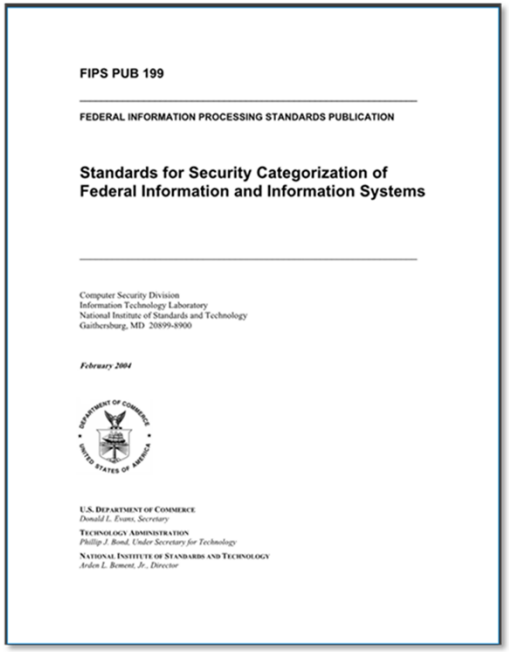
INFORMATION SECURITY

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


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

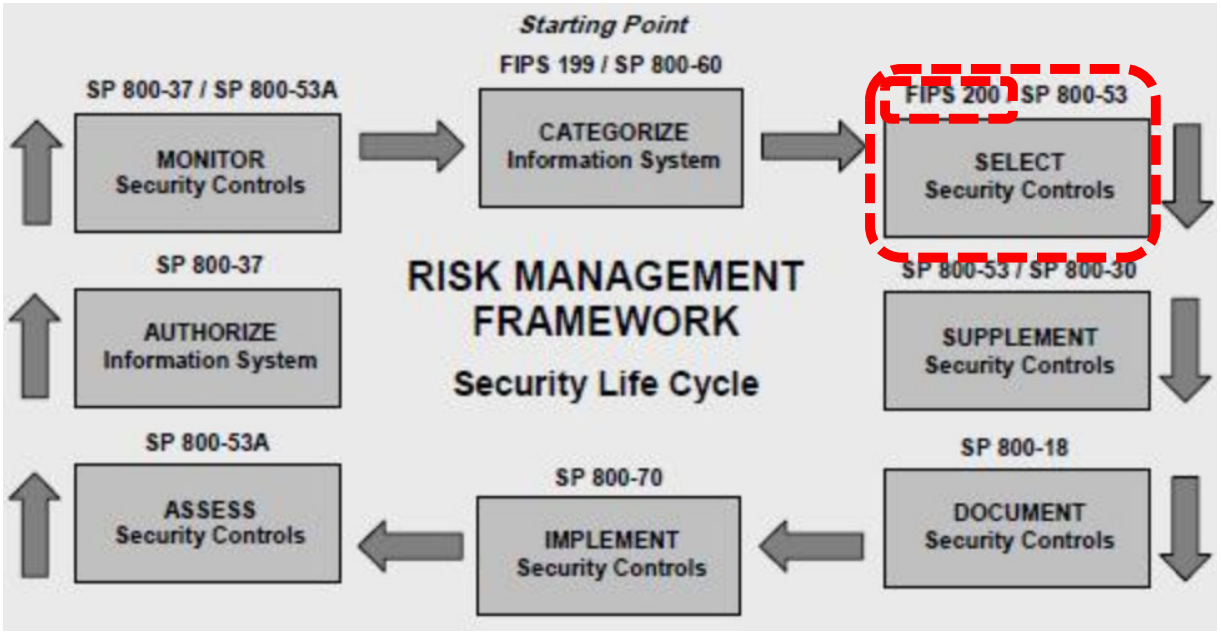
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

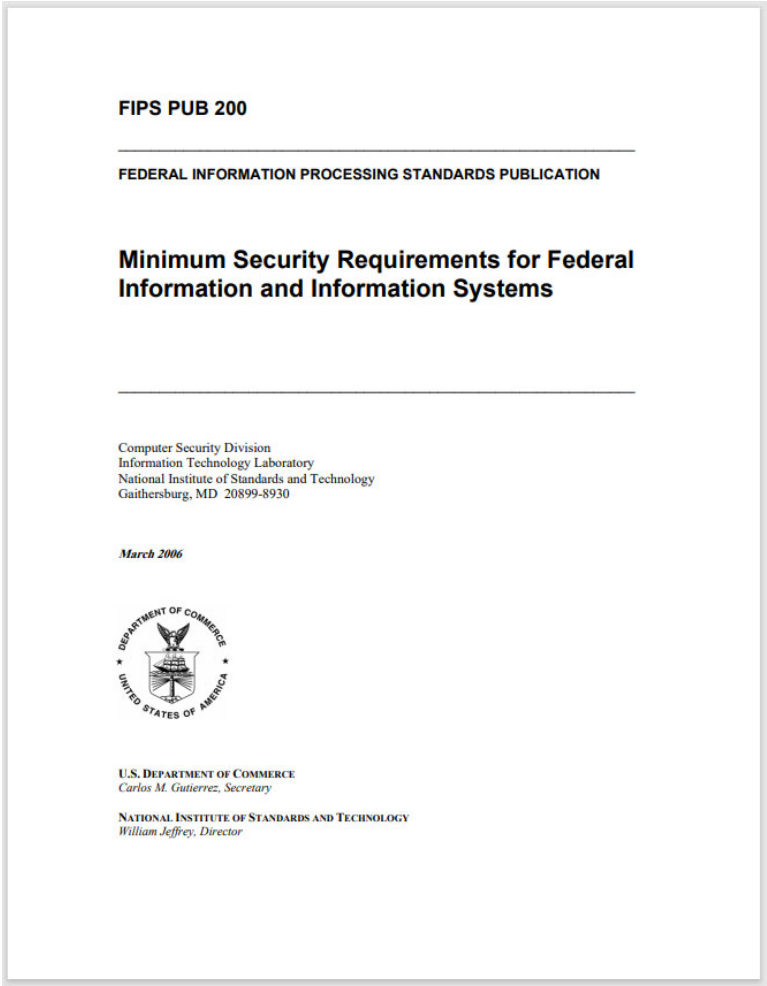
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Agenda

- ✓Risk Management Framework and IS Security Categorization
- ✓Mapping Information Types to Security Categorizations
- ✓*Team Exercise – Determine Information and Information System Types and provisional security categorization*
- Security Control Baselines – review
  - Minimum Security Controls and Security Control Baselines
  - Security Control Families
- Risk Assessment Controls
- *Team Exercise Find and assess risk assessment policy*

Risk Management Framework





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

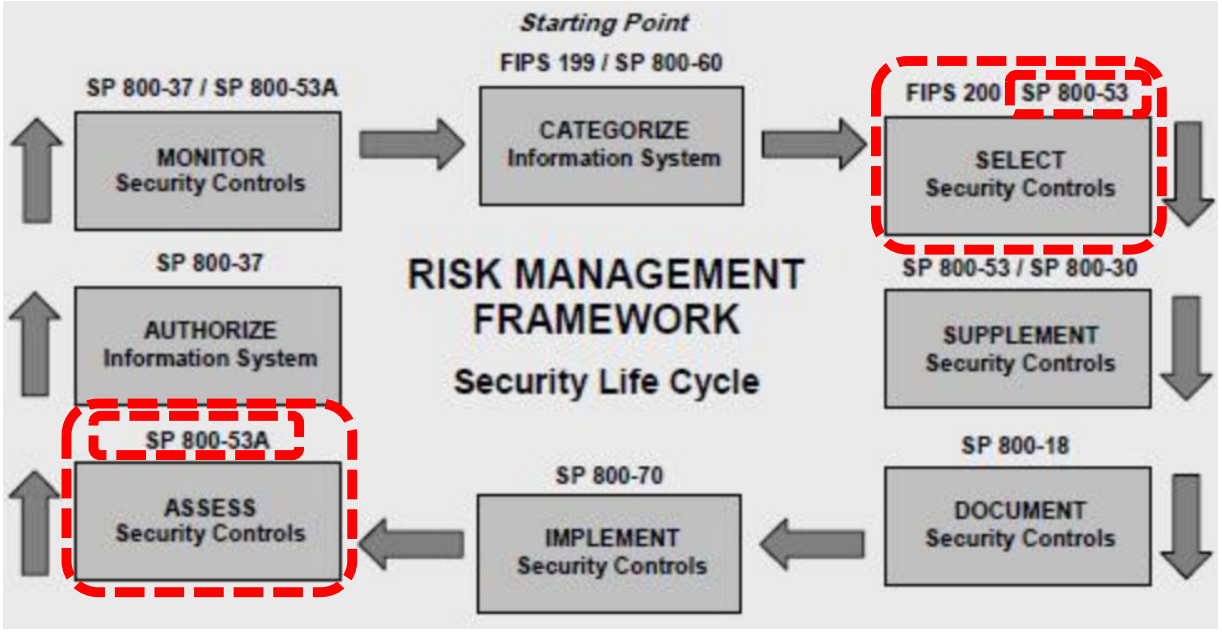
U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

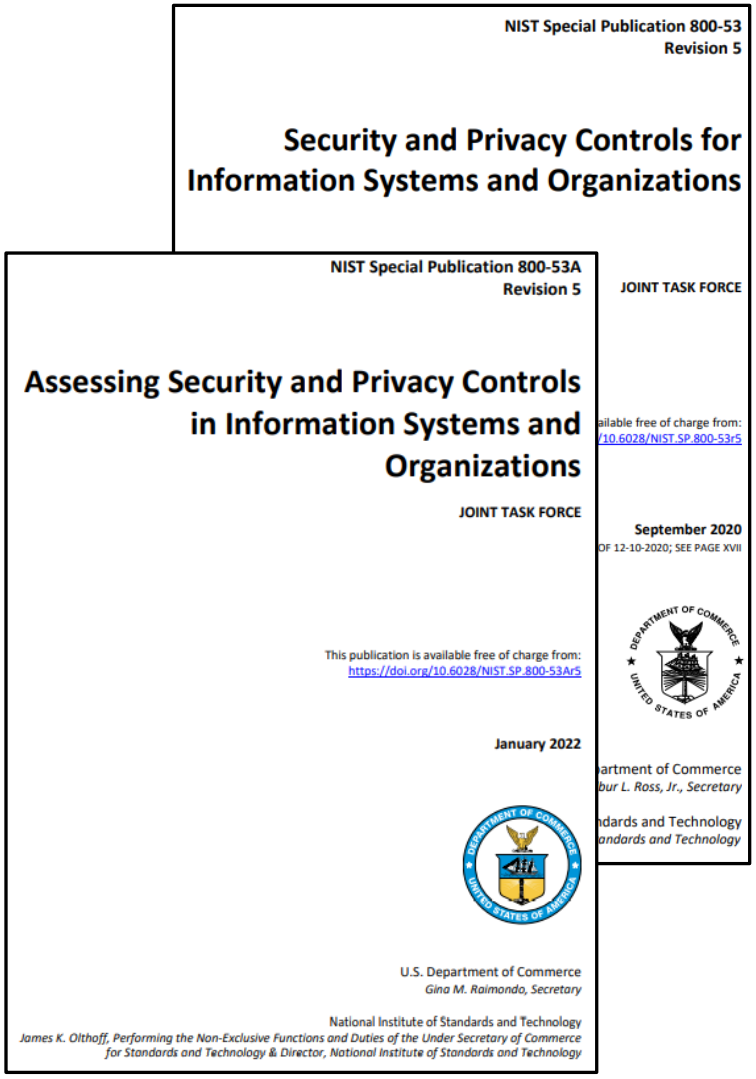
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

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)

Risk Management Framework




NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

NIST Special Publication 800-53A
Revision 5

JOINT TASK FORCE

Assessing Security and Privacy Controls in Information Systems and Organizations

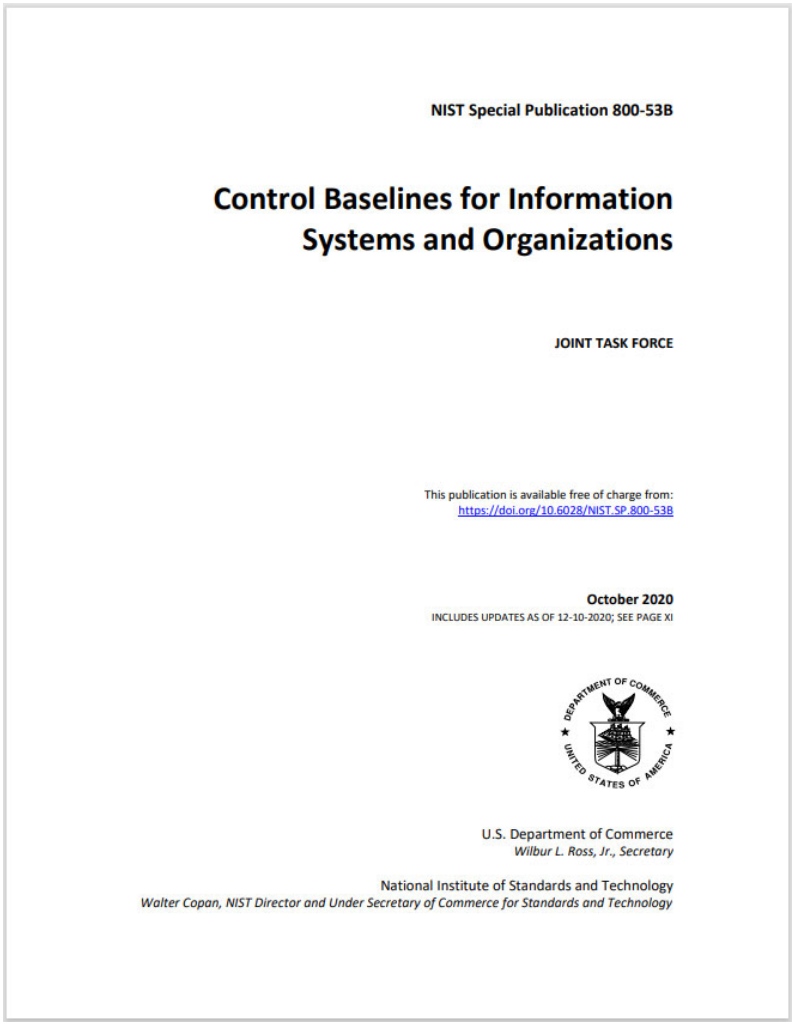
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

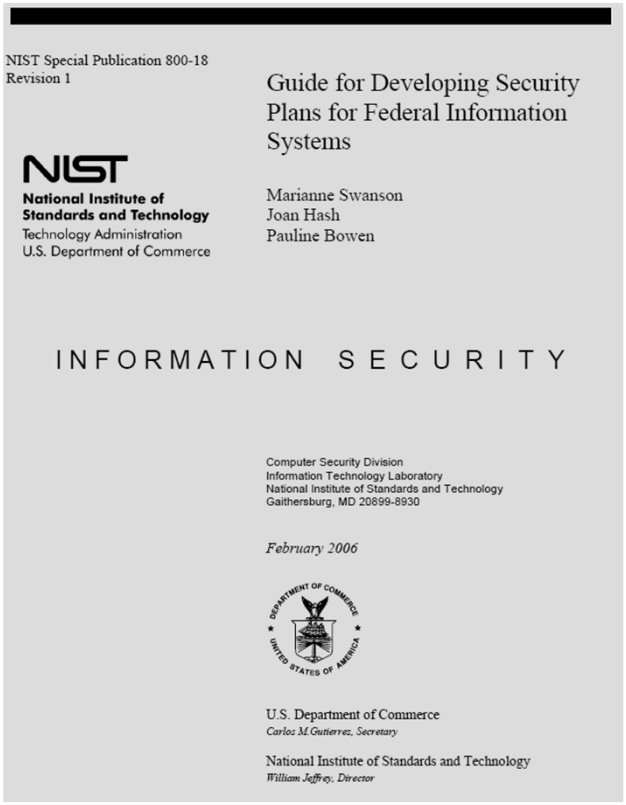
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Table of Contents

CHAPTER ONE INTRODUCTION 1
1.1 PURPOSE AND APPLICABILITY 1
1.2 TARGET AUDIENCE 2
1.3 ORGANIZATIONAL RESPONSIBILITIES 2
1.4 RELATIONSHIP TO OTHER PUBLICATIONS 3
1.5 REVISIONS AND EXTENSIONS 3
1.6 PUBLICATION ORGANIZATION 3
CHAPTER TWO THE FUNDAMENTALS 5
2.1 CONTROL BASELINES 5
2.2 SELECTING CONTROL BASELINES 6
2.3 CONTROL BASELINE ASSUMPTIONS 8
2.4 TAILORING CONTROL BASELINES 9
2.5 CAPABILITIES 14
CHAPTER THREE THE CONTROL BASELINES 15
3.1 ACCESS CONTROL FAMILY 16
3.2 AWARENESS AND TRAINING FAMILY 20
3.3 AUDIT AND ACCOUNTABILITY FAMILY 21
3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING FAMILY 23
3.5 CONFIGURATION MANAGEMENT FAMILY 24
3.6 CONTINGENCY PLANNING FAMILY 26
3.7 IDENTIFICATION AND AUTHENTICATION FAMILY 28
3.8 INCIDENT RESPONSE FAMILY 30
3.9 MAINTENANCE FAMILY 32
3.10 MEDIA PROTECTION FAMILY 33
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION FAMILY 34
3.12 PLANNING FAMILY 36
3.13 PROGRAM MANAGEMENT FAMILY 37
3.14 PERSONNEL SECURITY FAMILY 39
3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY FAMILY 40
3.16 RISK ASSESSMENT FAMILY 41
3.17 SYSTEM AND SERVICES ACQUISITION FAMILY 42
3.18 SYSTEM AND COMMUNICATIONS PROTECTION FAMILY 46
3.19 SYSTEM AND INFORMATION INTEGRITY FAMILY 51
3.20 SUPPLY CHAIN RISK MANAGEMENT FAMILY 55
REFERENCES 56
APPENDIX A GLOSSARY 59
APPENDIX B ACRONYMS 66
APPENDIX C OVERLAYS 67

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

What kind of control is Planning ?



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

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

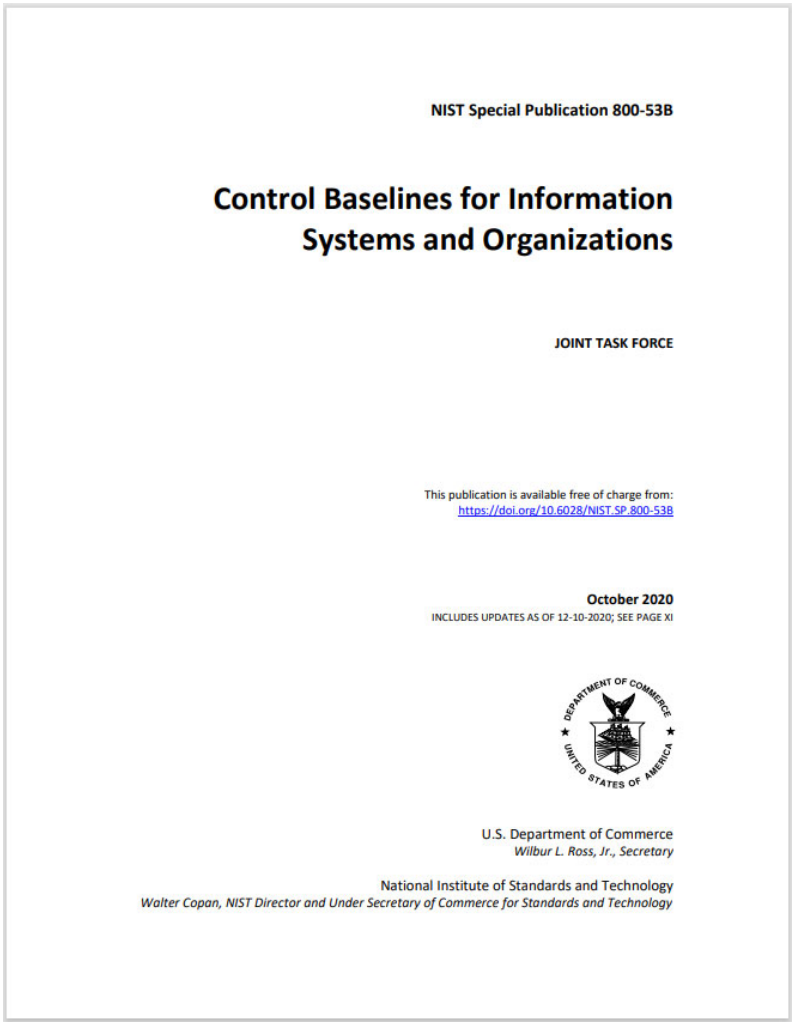
February 2006

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



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

October 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XI

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

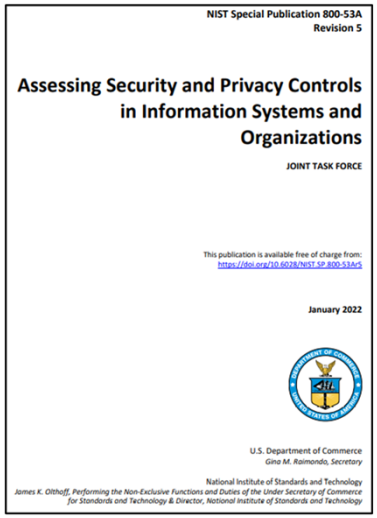
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

TABLE 3-12: PLANNING FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

PL-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-01_ODP[01]	***personnel or roles to whom the planning policy is to be disseminated is/are defined;***
	PL-01_ODP[02]	***personnel or roles to whom the planning procedures are to be disseminated is/ are defined;***
	PL-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PL-01_ODP[04]	***an official to manage the planning policy and procedures is defined;***
	PL-01_ODP[05]	***the frequency with which the current planning policy is reviewed and updated is defined;***
	PL-01_ODP[06]	***events that would require the current planning policy to be reviewed and updated are defined;***
	PL-01_ODP[07]	***the frequency with which the current planning procedures are reviewed and updated is defined;***
	PL-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	PL-01a.[01]	a planning policy is developed and documented.
	PL-01a.[02]	the planning policy is disseminated to ***<PL-01_ODP[01] personnel or roles>***;
	PL-01a.[03]	planning procedures to facilitate the implementation of the planning policy and associated planning controls are developed and documented;
	PL-01a.[04]	the planning procedures are disseminated to ***<PL-01_ODP[02] personnel or roles>***;
	PL-01a.01(a)[01]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses purpose;
	PL-01a.01(a)[02]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses scope;
	PL-01a.01(a)[03]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses roles;
	PL-01a.01(a)[04]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses responsibilities;
	PL-01a.01(a)[05]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses management commitment;
	PL-01a.01(a)[06]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses coordination among organizational entities;
	PL-01a.01(a)[07]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses compliance;
	PL-01a.01(b)	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;



NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

PL-01	POLICY AND PROCEDURES	
	PL-01b.	the ***<PL-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the planning policy and procedures;
	PL-01c.01[01]	the current planning policy is reviewed and updated ***<PL-01_ODP[05] frequency>***;
	PL-01c.01[02]	the current planning policy is reviewed and updated following ***<PL-01_ODP[06] events>***;
	PL-01c.02[01]	the current planning procedures are reviewed and updated ***<PL-01_ODP[07] frequency>***;
	PL-01c.02[02]	the current planning procedures are reviewed and updated following ***<PL-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-01-Examine	[SELECT FROM: Planning policy and procedures; system security plan; privacy plan; other relevant documents or records]
	PL-01-Interview	[SELECT FROM: Organizational personnel with planning responsibilities; organizational personnel with information security and privacy responsibilities].

ODP = Organizational-defined parameters

PL-02	SYSTEM SECURITY AND PRIVACY PLANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-02_ODP[01]	***individuals or groups with whom security and privacy-related activities affecting the system that require planning and coordination is/are assigned;***
	PL-02_ODP[02]	***personnel or roles to recieve distributed copies of the system security and privacy plans is/are assigned;***
	PL-02_ODP[03]	***frequency to review system security and privacy plans is defined;***
	PL-02a.01[01]	a security plan for the system is developed that is consistent with the organization's enterprise architecture;
	PL-02a.01[02]	a privacy plan for the system is developed that is consistent with the organization's enterprise architecture;
	PL-02a.02[01]	a security plan for the system is developed that explicitly defines the constituent system components;
	PL-02a.02[02]	a privacy plan for the system is developed that explicitly defines the constituent system components;
	PL-02a.03[01]	a security plan for the system is developed that describes the operational context of the system in terms of mission and business processes;
	PL-02a.03[02]	a privacy plan for the system is developed that describes the operational context of the system in terms of mission and business processes;
	PL-02a.04[01]	a security plan for the system is developed that identifies the individuals that fulfill system roles and responsibilities;
	PL-02a.04[02]	a privacy plan for the system is developed that identifies the individuals that fulfill system roles and responsibilities;

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

	PL-02a.05[01]	a security plan for the system is developed that identifies the information types processed, stored, and transmitted by the system;
	PL-02a.05[02]	a privacy plan for the system is developed that identifies the information types processed, stored, and transmitted by the system;
	PL-02a.06[01]	a security plan for the system is developed that provides the security categorization of the system, including supporting rationale;
	PL-02a.06[02]	a privacy plan for the system is developed that provides the security categorization of the system, including supporting rationale;
	PL-02a.07[01]	a security plan for the system is developed that describes any specific threats to the system that are of concern to the organization;
	PL-02a.07[02]	a privacy plan for the system is developed that describes any specific threats to the system that are of concern to the organization;
	PL-02a.08[01]	a security plan for the system is developed that provides the results of a privacy risk assessment for systems processing personally identifiable information;
	PL-02a.08[02]	a privacy plan for the system is developed that provides the results of a privacy risk assessment for systems processing personally identifiable information;
	PL-02a.09[01]	a security plan for the system is developed that describes the operational environment for the system and any dependencies on or connections to other systems or system components;
	PL-02a.09[02]	a privacy plan for the system is developed that describes the operational environment for the system and any dependencies on or connections to other systems or system components;
	PL-02a.10[01]	a security plan for the system is developed that provides an overview of the security requirements for the system;
	PL-02a.10[02]	a privacy plan for the system is developed that provides an overview of the privacy requirements for the system;
	PL-02a.11[01]	a security plan for the system is developed that identifies any relevant control baselines or overlays, if applicable;
	PL-02a.11[02]	a privacy plan for the system is developed that identifies any relevant control baselines or overlays, if applicable;
	PL-02a.12[01]	a security plan for the system is developed that describes the controls in place or planned for meeting the security requirements, including rationale for any tailoring decisions;
	PL-02a.12[02]	a privacy plan for the system is developed that describes the controls in place or planned for meeting the privacy requirements, including rationale for any tailoring decisions;
	PL-02a.13[01]	a security plan for the system is developed that includes risk determinations for security architecture and design decisions;
	PL-02a.13[02]	a privacy plan for the system is developed that includes risk determinations for privacy architecture and design decisions;
	PL-02a.14[01]	a security plan for the system is developed that includes security-related activities affecting the system that require planning and coordination with ***<PL-02_ODP[01] individuals or groups>***;

PL-02	SYSTEM SECURITY AND PRIVACY PLANS	
	PL-02a.14[02]	a privacy plan for the system is developed that includes privacy-related activities affecting the system that require planning and coordination with ***<PL-02_ODP[01] individuals or groups>***;
	PL-02a.15[01]	a security plan for the system is developed that is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
	PL-02a.15[02]	a privacy plan for the system is developed that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
	PL-02b.[01]	copies of the plans are distributed to ***<PL-02_ODP[02] personnel or roles>***;
	PL-02b.[02]	subsequent changes to the plans are communicated to ***<PL-02_ODP[02] personnel or roles>***;
	PL-02c.	plans are reviewed ***<PL-02_ODP[03] frequency>***;
	PL-02d.[01]	plans are updated to address changes to the system and environment of operations;
	PL-02d.[02]	plans are updated to address problems identified during the plan implementation;
	PL-02d.[03]	plans are updated to address problems identified during control assessments;
	PL-02e.[01]	plans are protected from unauthorized disclosure;
	PL-02e.[02]	plans are protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-02-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing security and privacy plan reviews and updates; enterprise architecture documentation; system security plan; privacy plan; records of system security and privacy plan reviews and updates; security and privacy architecture and design documentation; risk assessments; risk assessment results; control assessment documentation; other relevant documents or records].
	PL-02-Interview	[SELECT FROM: Organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities].
	PL-02-Test	[SELECT FROM: Organizational processes for system security and privacy plan development, review, update, and approval; mechanisms supporting the system security and privacy plan].

PL-04	RULES OF BEHAVIOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04_ODP[01]	***frequency for reviewing and updating the rules of behavior is defined;***
	PL-04_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<PL-04_ODP[03] frequency>; when the rules are revised or updated};***
	PL-04_ODP[03]	***frequency for individuals to read and re-acknowledge the rules of behavior is defined (if selected);***
	PL-04a.[01]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are established for individuals requiring access to the system;
	PL-04a.[02]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are provided to individuals requiring access to the system;
	PL-04b.	before authorizing access to information and the system, a documented acknowledgement from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received;
	PL-04c.	rules of behavior are reviewed and updated ***<PL-04_ODP[01] frequency>***;
	PL-04d.	individuals who have acknowledged a previous version of the rules of behavior are required to read and reacknowledge ***<PL-04_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; signed acknowledgements; records for rules of behavior reviews and updates; other relevant documents or records].
	PL-04-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed and resigned rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04-Test	[SELECT FROM: Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior; mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior].

PL-04(01)	RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04(01)(a)	the rules of behavior include restrictions on the use of social media, social networking sites, and external sites/applications;
	PL-04(01)(b)	the rules of behavior include restrictions on posting organizational information on public websites;
	PL-04(01)(c)	the rules of behavior include restrictions on the use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04(01)-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; training policy; other relevant documents or records].
	PL-04(01)-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04(01)-Test	[SELECT FROM: Organizational processes for establishing rules of behavior; mechanisms supporting and/or implementing the establishment of rules of behavior].

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
	Sec -Rel Acti lans	W: rpor nto			

PL-04	RULES OF BEHAVIOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04_ODP[01]	***frequency for reviewing and updating the rules of behavior is defined;***
	PL-04_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<PL-04_ODP[03] frequency>; when the rules are revised or updated};***
	PL-04_ODP[03]	***frequency for individuals to read and re-acknowledge the rules of behavior is defined (if selected);***
	PL-04a.[01]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are established for individuals requiring access to the system;
	PL-04a.[02]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are provided to individuals requiring access to the system;
	PL-04b.	before authorizing access to information and the system, a documented acknowledgement from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received;
	PL-04c.	rules of behavior are reviewed and updated ***<PL-04_ODP[01] frequency>***;
	PL-04d.	individuals who have acknowledged a previous version of the rules of behavior are required to read and reacknowledge ***<PL-04_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; signed acknowledgements; records for rules of behavior reviews and updates; other relevant documents or records].
	PL-04-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed and resigned rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04-Test	[SELECT FROM: Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior; mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior].

PL-04(01)	RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04(01)(a)	the rules of behavior include restrictions on the use of social media, social networking sites, and external sites/applications;
	PL-04(01)(b)	the rules of behavior include restrictions on posting organizational information on public websites;
	PL-04(01)(c)	the rules of behavior include restrictions on the use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04(01)-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; training policy; other relevant documents or records].
	PL-04(01)-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04(01)-Test	[SELECT FROM: Organizational processes for establishing rules of behavior; mechanisms supporting and/or implementing the establishment of rules of behavior].

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
	Sec -Rel Acti lans	W: rpor nto			

PL-08	SECURITY AND PRIVACY ARCHITECTURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-08_ODP	***frequency for review and update to reflect changes in the enterprise architecture;***
	PL-08a.01	a security architecture for the system describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
	PL-08a.02	a privacy architecture describes the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
	PL-08a.03[01]	a security architecture for the system describes how the architecture is integrated into and supports the enterprise architecture;
	PL-08a.03[02]	a privacy architecture for the system describes how the architecture is integrated into and supports the enterprise architecture;
	PL-08a.04[01]	a security architecture for the system describes any assumptions about and dependencies on external systems and services;
	PL-08a.04[02]	a privacy architecture for the system describes any assumptions about and dependencies on external systems and services;
	PL-08b.	changes in the enterprise architecture are reviewed and updated ***<PL-08_ODP frequency>*** to reflect changes in the enterprise architecture;
	PL-08c.[01]	planned architecture changes are reflected in the security plan;
	PL-08c.[02]	planned architecture changes are reflected in the privacy plan;
	PL-08c.[03]	planned architecture changes are reflected in the Concept of Operations (CONOPS);
	PL-08c.[04]	planned architecture changes are reflected in criticality analysis;
	PL-08c.[05]	planned architecture changes are reflected in organizational procedures;
	PL-08c.[06]	planned architecture changes are reflected in procurements and acquisitions.

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

PL-08	SECURITY AND PRIVACY ARCHITECTURES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-08-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing information security and privacy architecture development; procedures addressing information security and privacy architecture reviews and updates; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; records of information security and privacy architecture reviews and updates; other relevant documents or records].
	PL-08-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities].
	PL-08-Test	[SELECT FROM: Organizational processes for developing, reviewing, and updating the information security and privacy architecture; mechanisms supporting and/or implementing the development, review, and update of the information security and privacy architecture].

PL-08(01)	SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-08(01)_ODP[01]	***controls to be allocated are defined;***
	PL-08(01)_ODP[02]	***locations and architectural layers are defined;***
	PL-08(01)(a)[01]	the security architecture for the system is designed using a defense-in-depth approach that allocates ***<PL-08(01)_ODP[01] controls>*** to ***<PL-08(01)_ODP[02] locations and architectural layers>***;
	PL-08(01)(a)[02]	the privacy architecture for the system is designed using a defense-in-depth approach that allocates ***<PL-08(01)_ODP[01] controls>*** to ***<PL-08(01)_ODP[02] locations and architectural layers>***;
	PL-08(01)(b)[01]	the security architecture for the system is designed using a defense-in-depth approach that ensures the allocated controls operate in a coordinated and mutually reinforcing manner;
	PL-08(01)(b)[02]	the privacy architecture for the system is designed using a defense-in-depth approach that ensures the allocated controls operate in a coordinated and mutually reinforcing manner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-08-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing information security and privacy architecture development; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; other relevant documents or records].
	PL-08-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities].
	PL-08-Test	[SELECT FROM: Organizational processes for designing the information security and privacy architecture; mechanisms supporting and/or implementing the design of the information security and privacy architecture].

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

PL-10	BASELINE SELECTION
	ASSESSMENT OBJECTIVE: *Determine if:*
	PL-10 a control baseline for the system is selected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	PL-10-Examine [SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing system security and privacy plan reviews and updates; system design documentation; system architecture and configuration documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; system security plan; privacy plan; other relevant documents or records].
	PL-10-Interview [SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with responsibility for organizational risk management activities].

Business Area	Information Type ID	Information Type	Confidentiality	Integrity	Availability	Information Type Categorization	Sub-System Categorization	System Categorization
Environmental Management	D.8.3	Pollution Prevention and Control	Low	Low	Low	Low	*Low*	*Moderate*
Public Goods Creation & Management	D.22.3	Public Resources, Facility and Infrastructure Management	Low	Low	Low	Low		
		Tenant Data	*Low*	*Low*	*Low*	*Low*		
Information & Technology Management	C.3.5.5	Information Security	Low	Moderate	Low	Moderate	*Moderate*	
Information & Technology Management	C.3.5.6	Record Retention	Low	Low	Low	Low		
Information & Technology Management	C.3.5.7	Information Management	Low	Moderate	Low	Moderate		
Information & Technology Management	C.3.5.8	System and Network Monitoring	Moderate	Moderate	Low	Moderate		
		System Data	*Moderate*	*Moderate*	*Low*	*Moderate*		

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

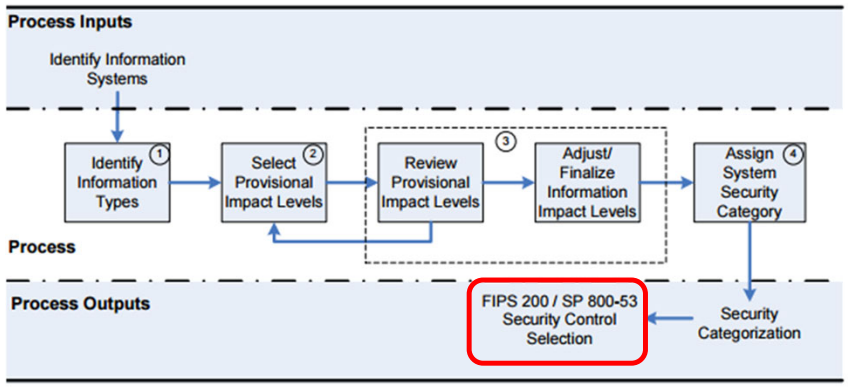


Figure 2: SP 800-60 Security Categorization Process Execution

PL-11	BASELINE TAILORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-11	the selected control baseline is tailored by applying specified tailoring actions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-11-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; system design documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; baseline tailoring rationale; system security plan; privacy plan; records of system security and privacy plan reviews and updates; other relevant documents or records].
	PL-11-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities].

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
PL-1	**Policy and Procedures**	x	x	x	x
PL-2	**System Security and Privacy Plans**	x	x	x	x
PL-2(1)	CONCEPT OF OPERATIONS	W: Incorporated into PL-7.			
PL-2(2)	FUNCTIONAL ARCHITECTURE	W: Incorporated into PL-8.			
PL-2(3)	PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	W: Incorporated into PL-2.			
PL-3	System Security Plan Update	W: Incorporated into PL-2.			
PL-4	**Rules of Behavior**	x	x	x	x
PL-4(1)	SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	x	x	x	x
PL-5	Privacy Impact Assessment	W: Incorporated into RA-8.			
PL-6	Security-Related Activity Planning	W: Incorporated into PL-2.			
PL-7	**Concept of Operations**				
PL-8	**Security and Privacy Architectures**	x		x	x
PL-8(1)	DEFENSE IN DEPTH				
PL-8(2)	SUPPLIER DIVERSITY				
PL-9	**Central Management**	x			
PL-10	**Baseline Selection**		x	x	x
PL-11	**Baseline Tailoring**		x	x	x

Agenda

- ✓Teams
- ✓Risk Management Framework and FIPS 199
- ✓Use of NIST SP 800-60 Volume 1 and Volume 2
- ✓*Exercise: How to assess and information security policy?*
- ✓*Exercise – Determine Information and Information System Types and provisional security categorization*
- ✓Security Control Baselines – review
  - Minimum Security Controls and Security Control Baselines
  - Security Control Families
- ✓Planning Controls