MIS 5206
Protection of Information Assets
- Unit #2a -

Risk Evaluation

Agenda

- Categorizing Information for IT Risk Management
- Using Categorization to Select a Baseline of Security Controls
- Risk Evaluation
- Test taking tip
- Quiz

Cyber Security Risk Management

Terminology:

- **Risk Capacity** = "objective magnitude or amount of loss than an enterprise can tolerate without risking its continued existence"
- **Risk Appetite** "generally reflects a management decision regarding how much risk is desirable"

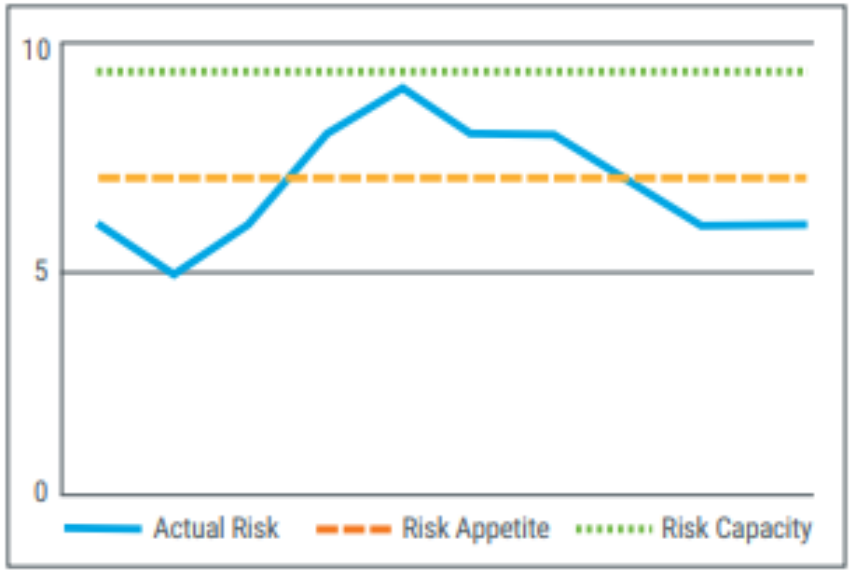


Diagram show a relatively sustainable situation

- Risk appetite is lower than risk capacity
- Actual risk exceeds risk appetite, but remains below risk capacity

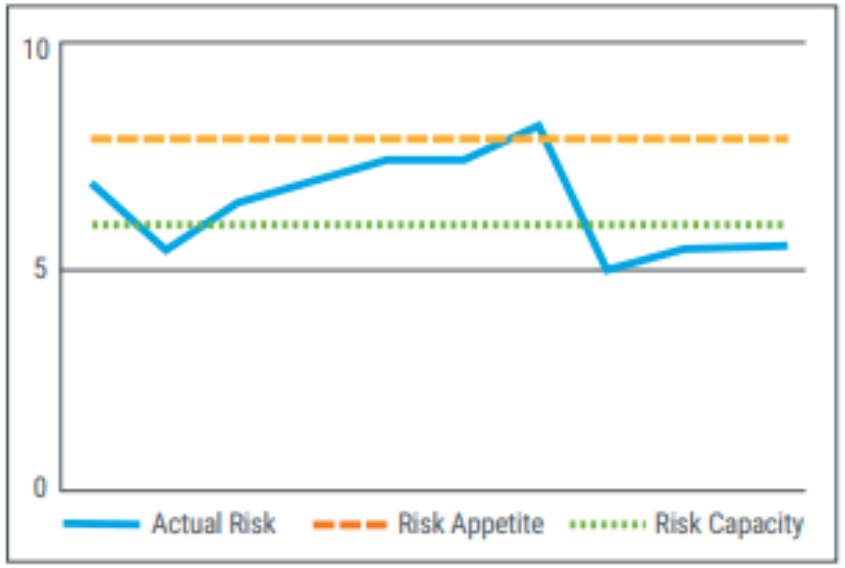


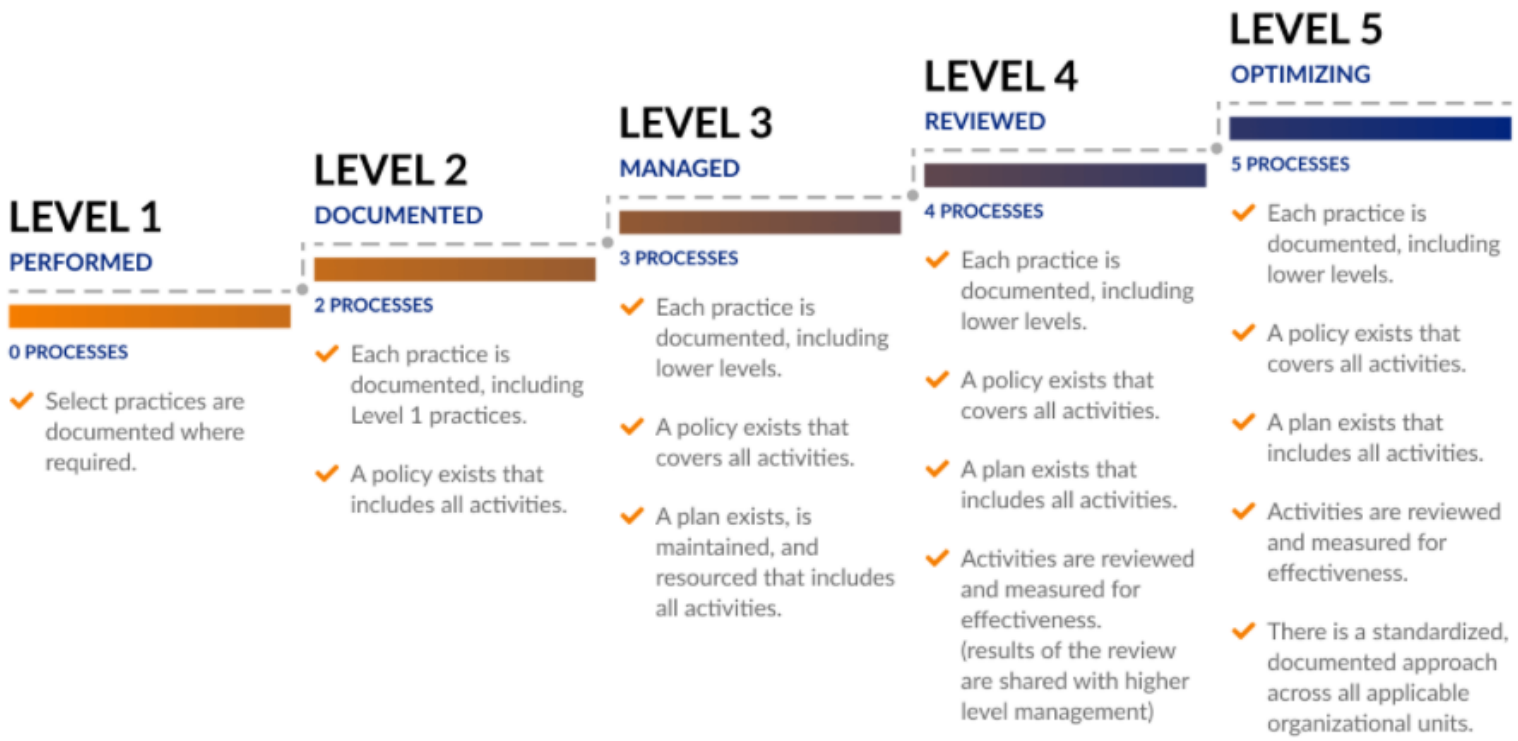
Diagram show an unsustainable situation

- Risk appetite is defined by management as a level beyond risk capacity (i.e. management is OK to accept risk and absorb loss)
- Actual risk routinely exceeds risk capacity, despite remaining below risk appetite level most of the time

NIST Cybersecurity Framework

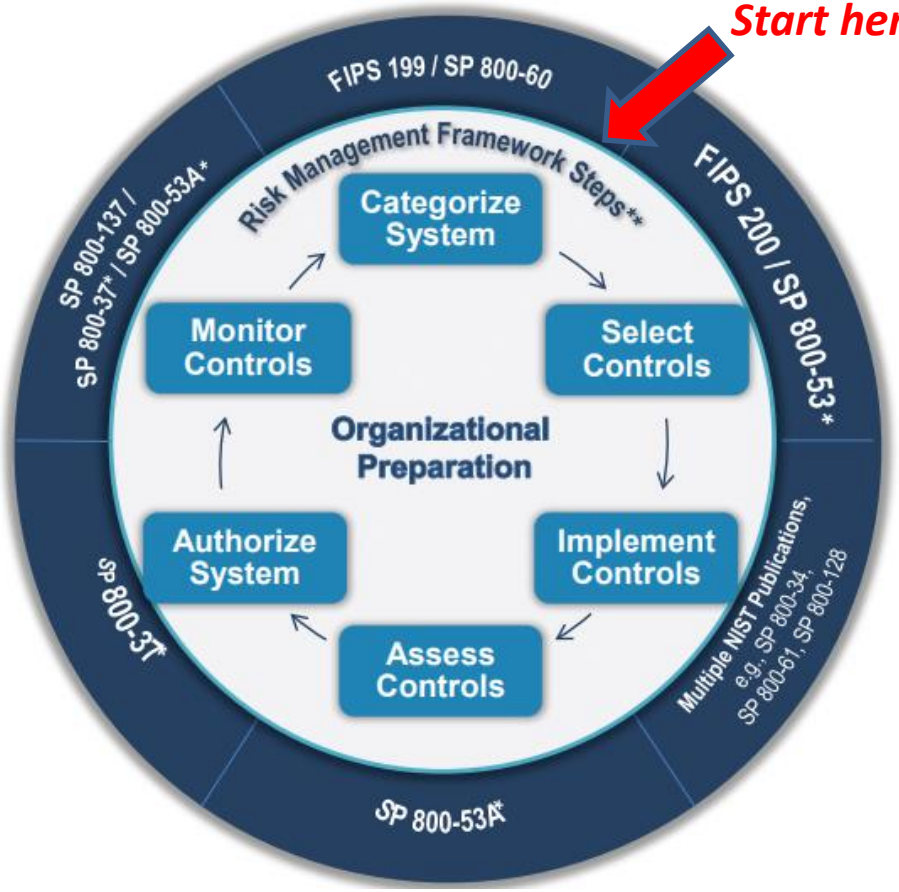
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control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

Cybersecurity Maturity Model Certification (CMMC) levels



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

Information inventory, categorization and risk evaluation is the first step in information systems security…



- A holistic and comprehensive risk management process
- Provides a framework for managing risk throughout the information system development lifecycle

Supporting Publications

Federal Information Processing Standards (FIPS)

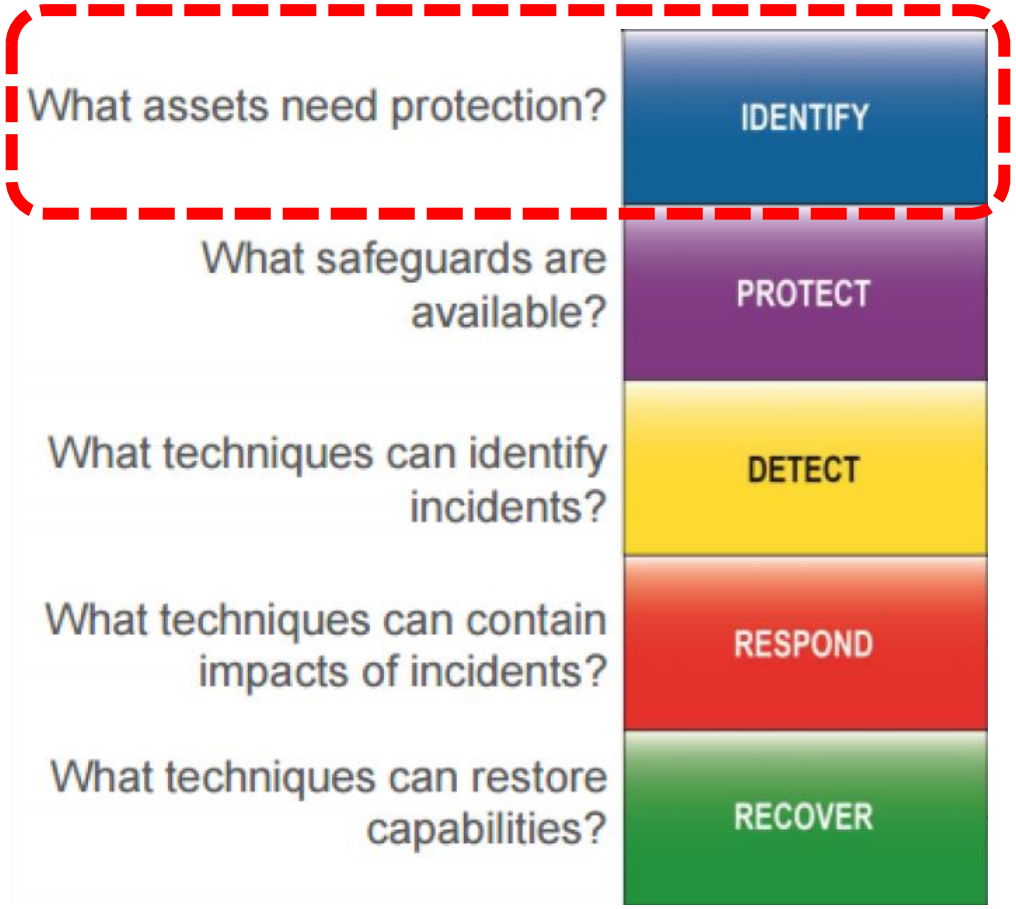
- FIPS 199 – Standards for Security Categorization
- FIPS 200 – Minimum Security Requirements

Special Publications (SPs)

- SP 800-18 – Guide for System Security Plan Development
- SP 800-30 – Guide for Conducting Risk Assessments
- SP 800-34 – Guide for Contingency Plan development
- SP 800-37 – Guide for Applying the Risk Management Framework
- SP 800-39 – Managing Information Security Risk
- SP 800-53/53A – Security Controls Catalog and Assessment Procedures
- SP 800-60 – Mapping Information Types to Security Categories
- SP 800-128 – Security-focused Configuration Management
- SP 800-137 – Information Security Continuous Monitoring
- Many others for operational and technical implementations

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

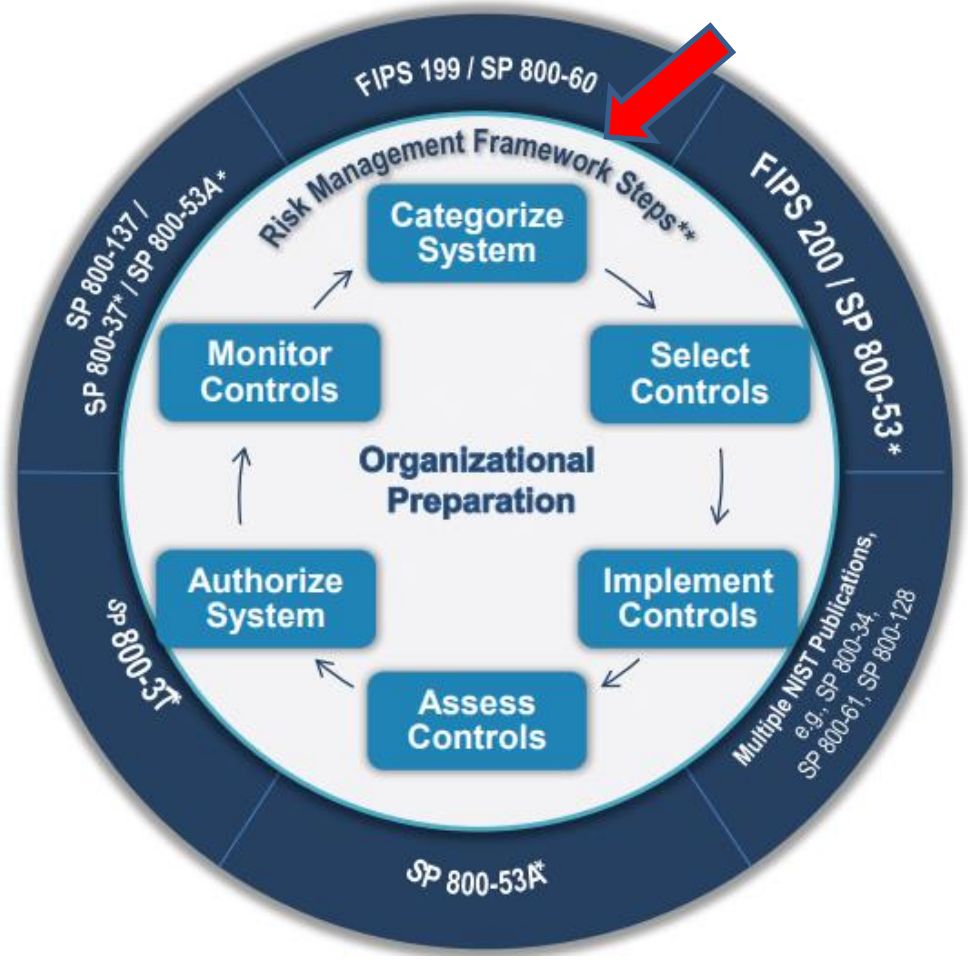
Information Categorization is part of Risk Evaluation



Why is data categorization important?

- It focuses attention on the identification and valuation of information assets
- It is the basis for access and other control policies and processes

Where information and IT asset inventory, categorization & risk evaluation fit in information systems security…

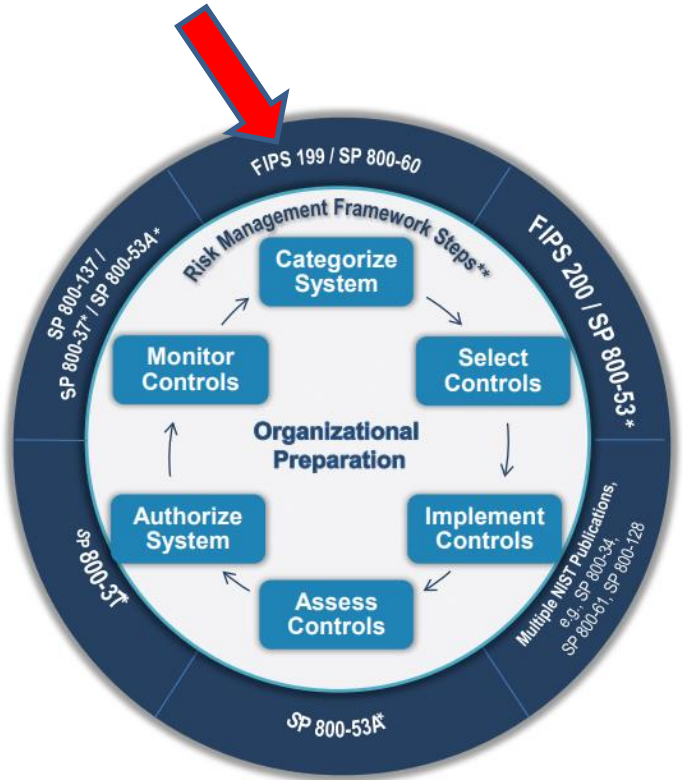


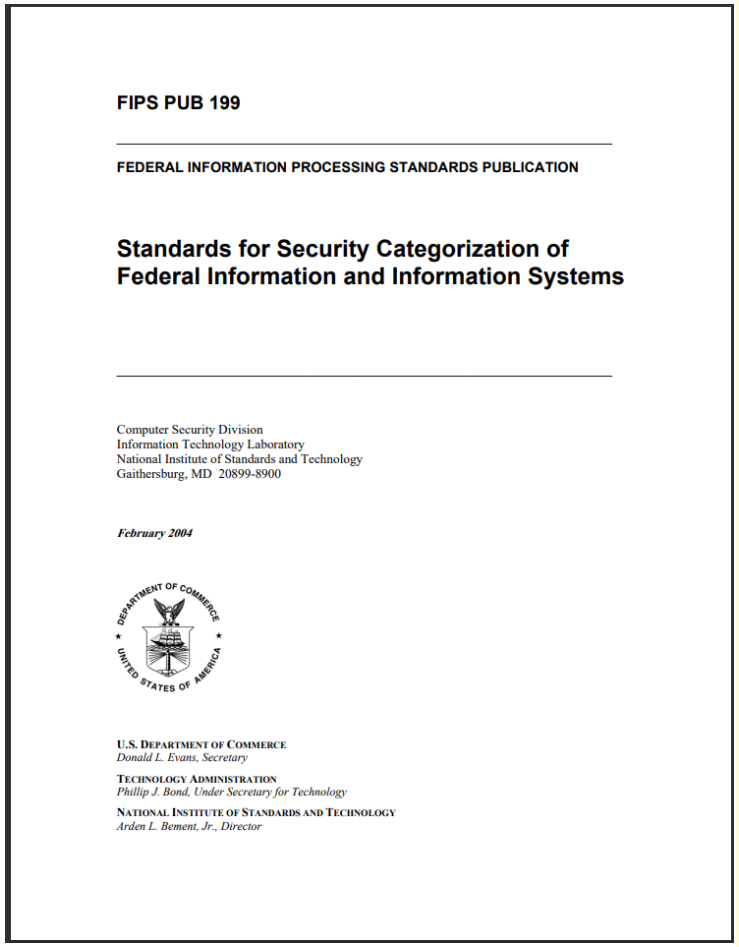
NIST Risk Management Framework

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

NIST Cybersecurity Framework

Categorizing Information and Information Systems





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

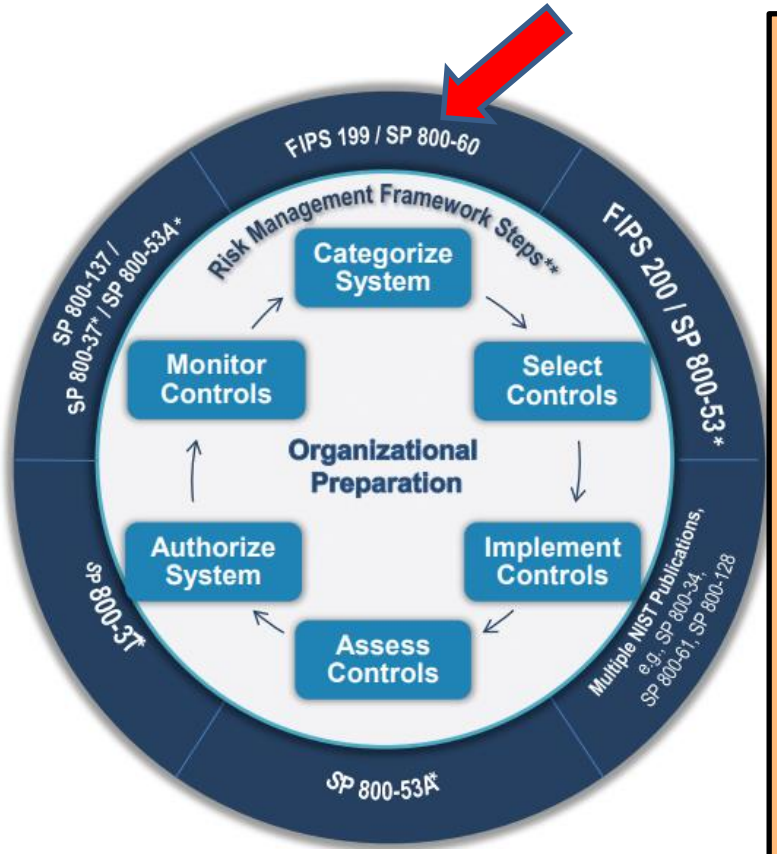
U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

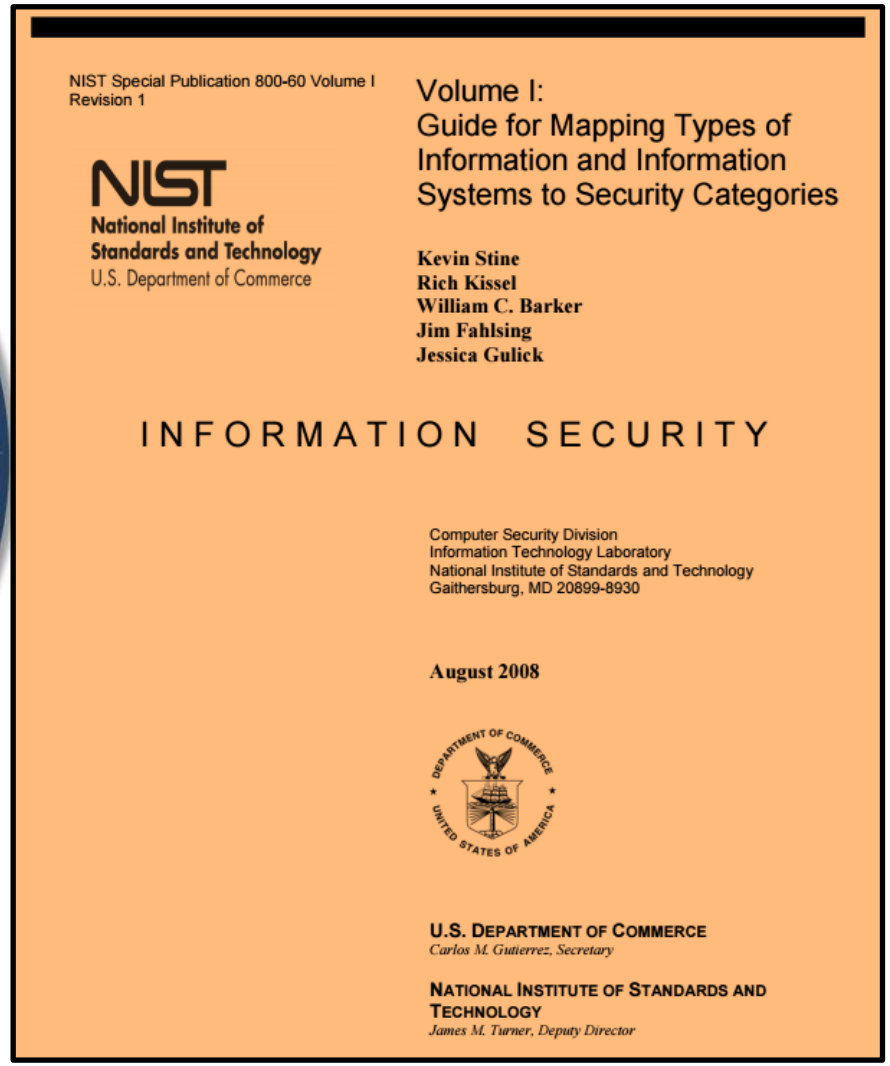
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

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.

Categorizing Information and 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

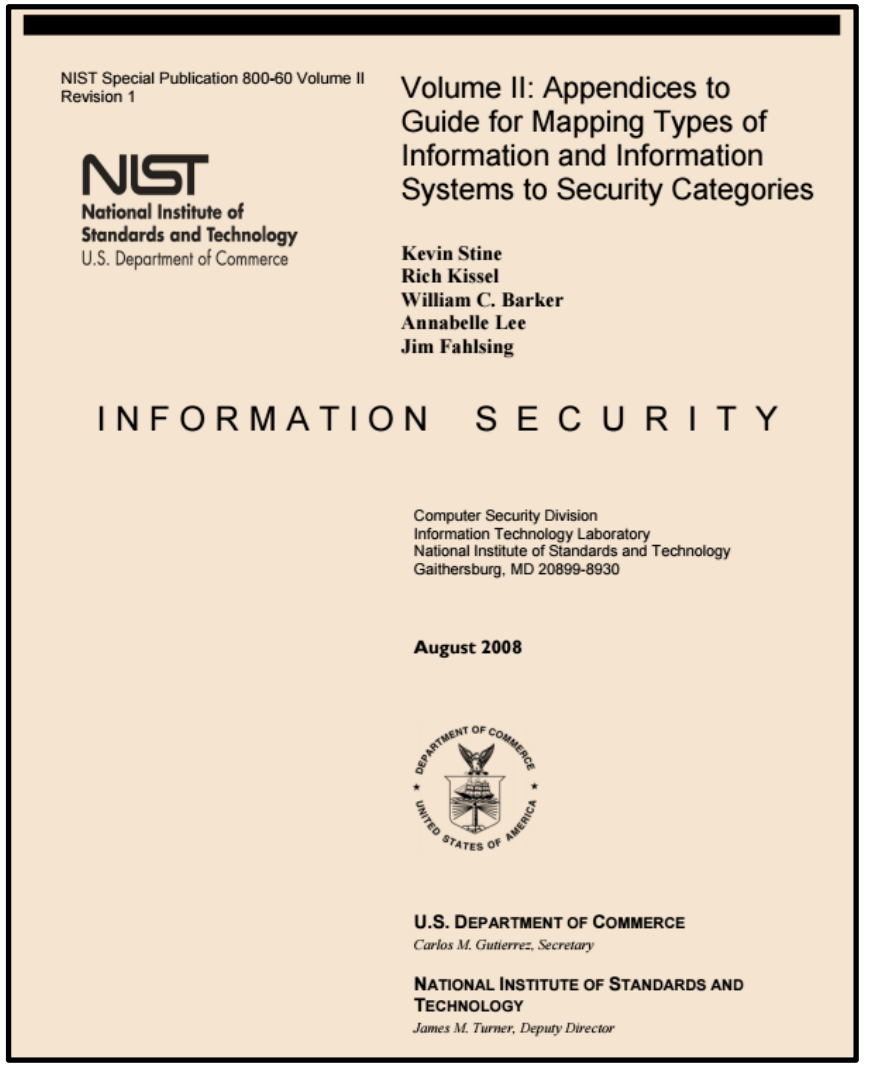
INFORMATION SECURITY

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



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

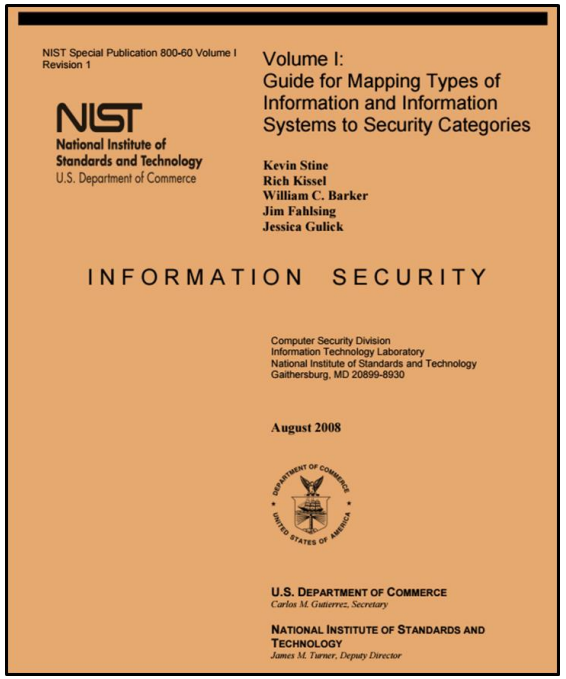
August 2008

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

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

NIST SP 800-60 provides guidance for getting started with impact categorizations of the types of data stored in wide variety of types of information systems

https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-60v1r1.pdf


NIST Special Publication 800-60 Volume I Revision 1

Volume I:
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
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

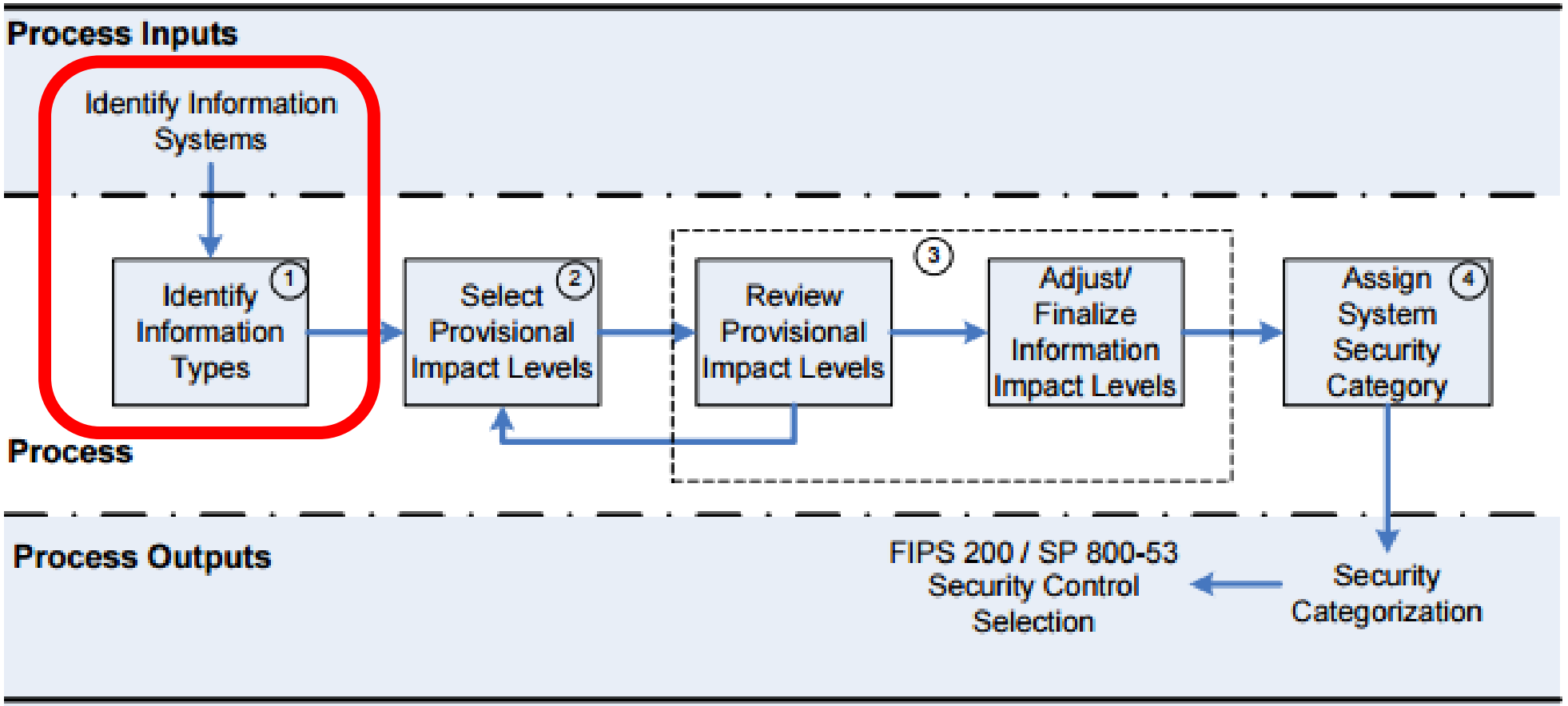


Figure 2: SP 800-60 Security Categorization Process Execution

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Mission Areas and Information Types [Services for Citizens]

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 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
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.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

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

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Services Delivery Mechanisms and Information Types [Mode of Delivery]

D.20 Knowledge Creation & Management
Research and Development
General Purpose Data and Statistics
Advising and Consulting
Knowledge Dissemination

D.21 Regulatory Compliance & Enforcement
Inspections and Auditing
Standards Setting/Reporting Guideline Development
Permits and Licensing

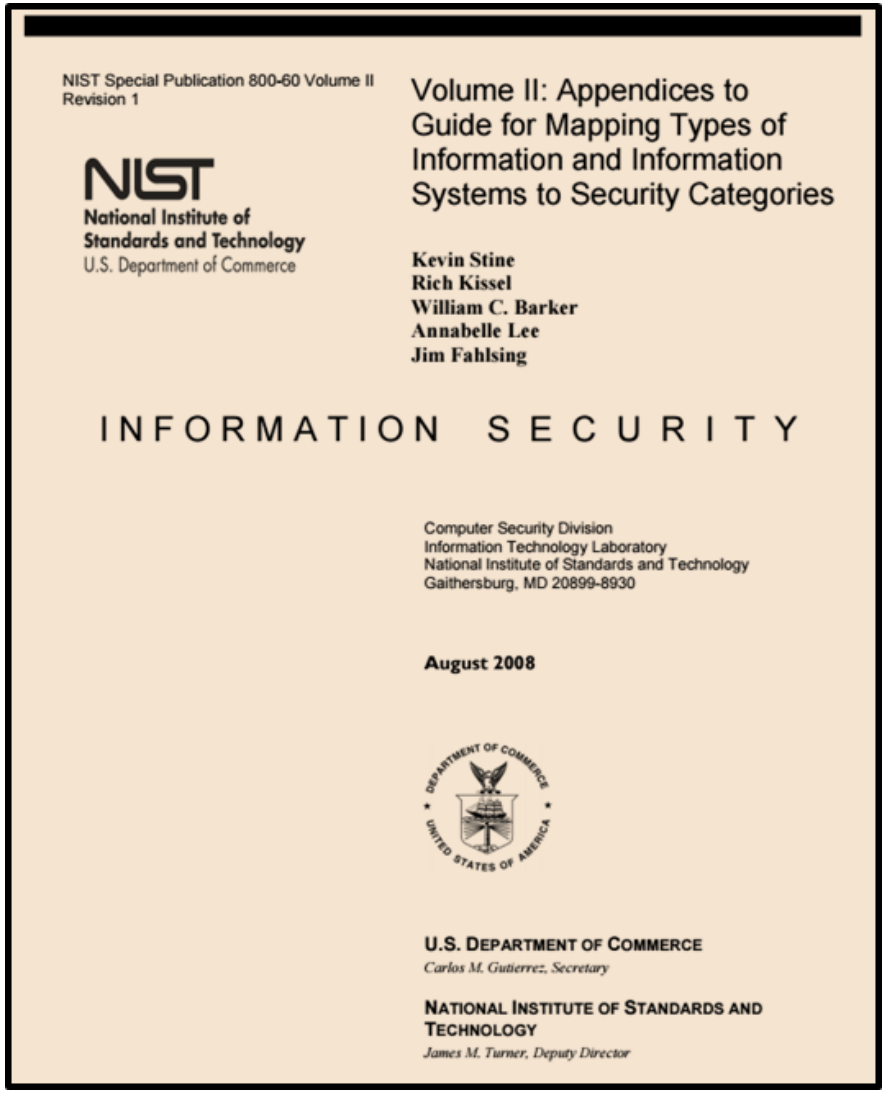
D.22 Public Goods Creation & Management
Manufacturing
Construction
Public Resources, Facility and Infrastructure Management
Information Infrastructure Management

D.23 Federal Financial Assistance
Federal Grants (Non-State)
Direct Transfers to Individuals
Subsidies
Tax Credits

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 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

	Confidentiality	Integrity	Availability
International Affairs and Commerce			
Foreign Affairs	**High**	**High**	Moderate
International Development and Humanitarian Aid	Moderate	Low	Low
Global Trade	**High**	**High**	**High**
Natural Resources			
Water Resource Management	Low	**Low**	**Low**
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	**Low**	**Low**
Energy			
Energy Supply	Low[25]	Moderate[26]	Moderate[26]
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	**Low**
Energy Production	Low	Low	**Low**
Environmental Management			
Environmental Monitoring/ Forecasting	Low	Moderate	**Low**
Environmental Remediation	**Moderate**	**Low**	**Low**
Pollution Prevention And Control	**Low**	**Low**	**Low**
Economic Development			
Business and Industry Development	Low	**Low**	**Low**
Intellectual Property Protection	Low	**Low**	**Low**
Financial Sector Oversight	Moderate	Low	**Low**
Industry Sector Income Stabilization	**Moderate**	**Low**	**Low**
Community and Social Services			
Homeownership Promotion	Low	**Low**	**Low**
Community and Regional Development	Low	**Low**	**Low**
Social Services	Low	**Low**	**Low**
Postal Services	Low	Moderate	**Moderate**
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	Low	Low
Space Operations	Low	**High**	**High**
Education			
Elementary, Secondary, and Vocational Education	**Low**	**Low**	**Low**
Higher Education	Low	Low	**Low**
Cultural & Historic Preservation	Low	Low	**Low**
Cultural & Historic Exhibition	Low	Low	**Low**
Workforce Management			

D.8.2 Environmental Remediation Information Type

Environmental remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities. The following security categorization is recommended for the environmental remediation information type:

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

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of environmental remediation information on the immediate and long-term activities of responsible agencies with respect to correcting and offsetting environmental deficiencies or imbalances. Serious adverse effects are likely to result from 1) exposure of information that is premature and not fully checked for accuracy and that can damage public confidence in an organization targeted for remedial action, 2) unauthorized disclosure of information that is proprietary to an organization, 3) unauthorized disclosure of information concerning proposed remediation that may be used by organizations opposing particular remedial actions, and 4) disclosure of an agency's tactics for enforcing remediation that will have an adverse effect on the enforcement action. The consequences of such unauthorized disclosures may have a serious adverse effect on public confidence in the agency, have a serious adverse effect on agency operations, and place the agency at a significant disadvantage.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for environmental remediation information is ***moderate***.

Integrity

The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required to detect the modification or destruction of information. The consequences of unauthorized modification or destruction of environmental remediation information may depend on the urgency with which the information is typically needed.

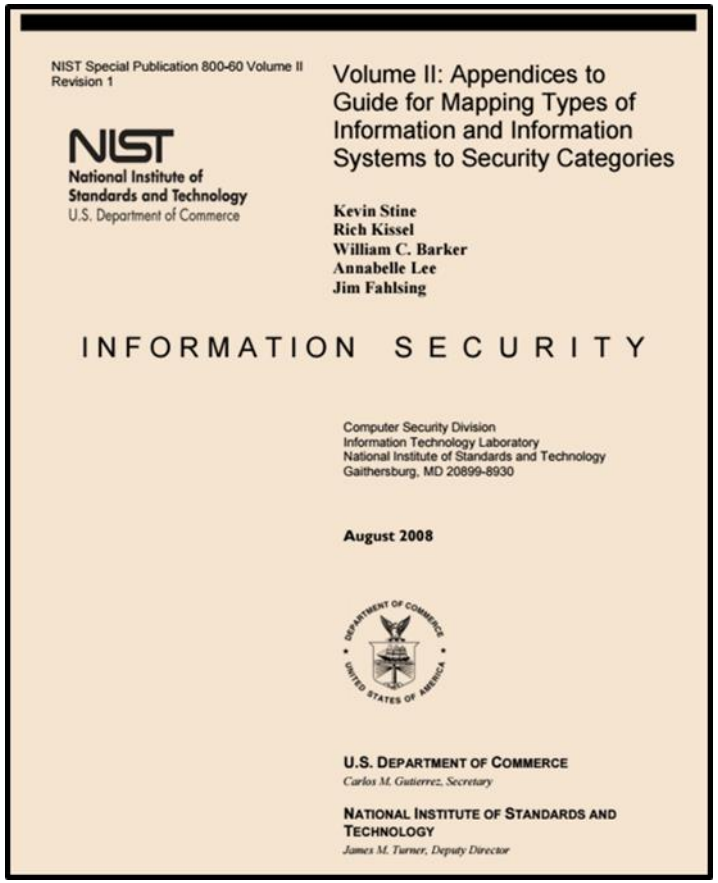
Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations, public confidence in the agency, and the agency mission.

Recommended Integrity Impact Level: The provisional integrity impact level recommended for environmental remediation information is ***low***.

Availability

The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to environmental remediation information. Except for cases of emergency bulletins necessary to correct existing threats to public safety, environmental remediation processes are usually tolerant of reasonable delays.

Recommended Availability Impact Level: The provisional availability impact level recommended for environmental remediation information is ***low***.


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

https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-60v2r1.pdf

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Mission Areas and Information Types [Services for Citizens]

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 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
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.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

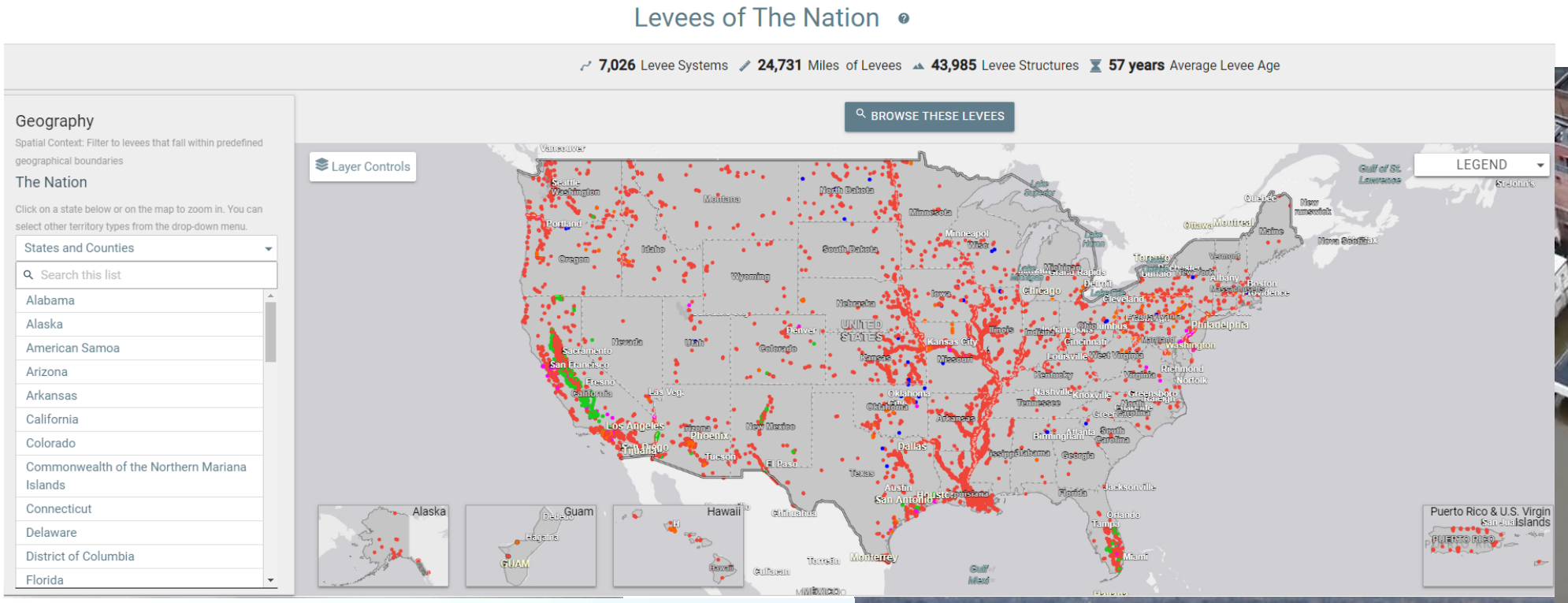
D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement

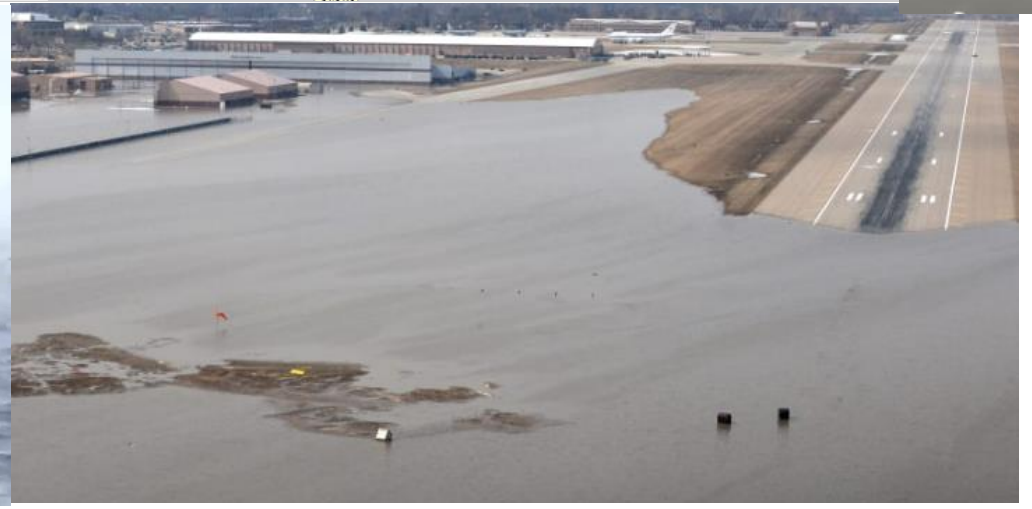
D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation

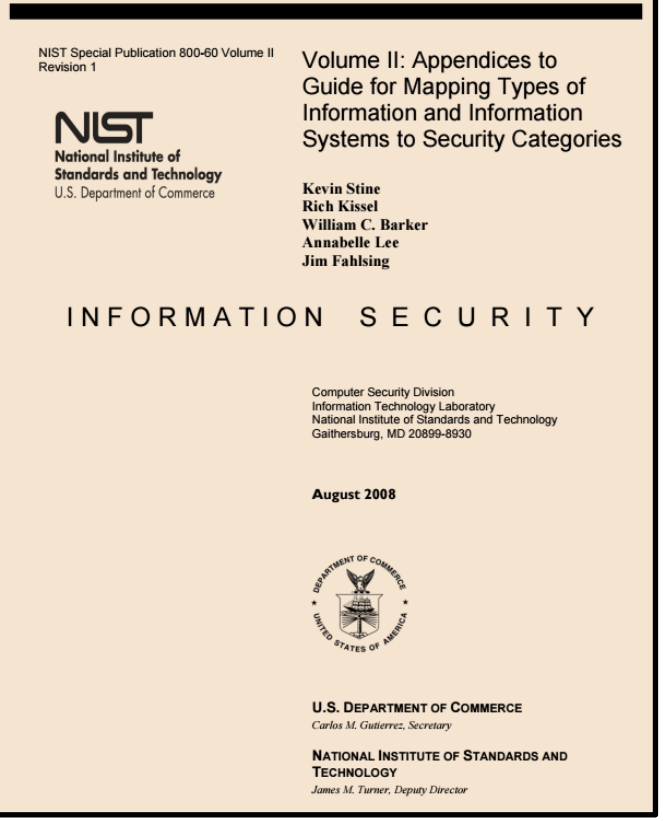
D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

Disaster Management Information System Example





[National Levee Database]



2. Select Provisional Impact Levels for the identified information system

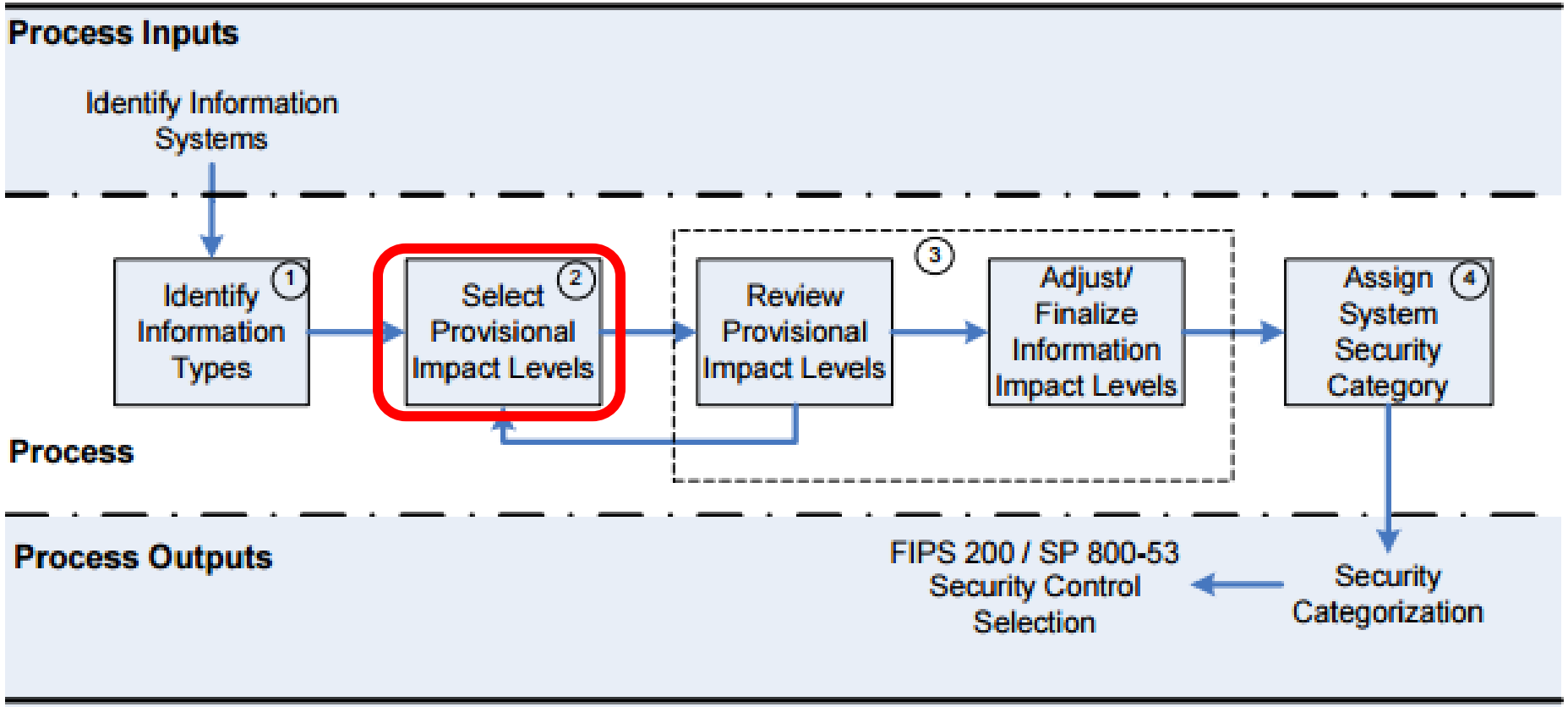
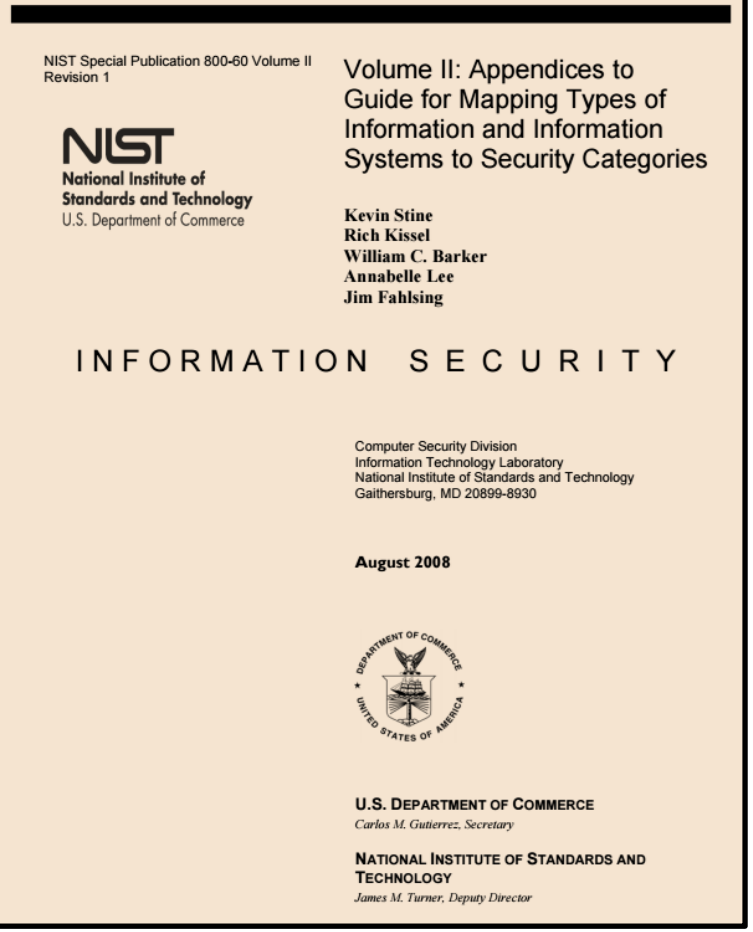


Figure 2: SP 800-60 Security Categorization Process Execution


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

Disaster Management Information

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.

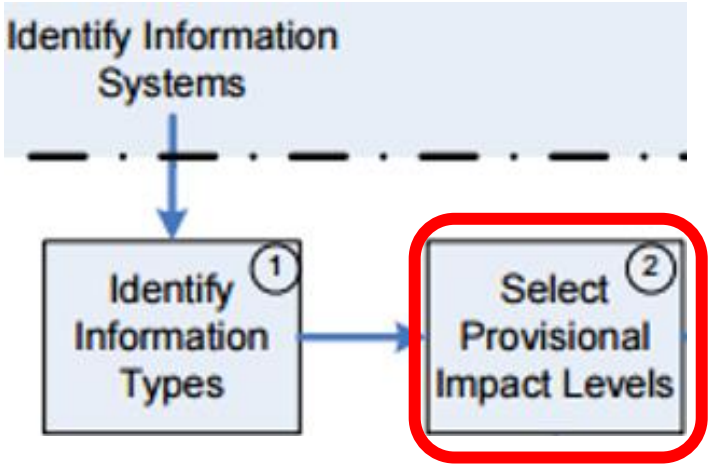
Exercise

Using NIST SP 800-60 V.2 R1 determine the security categorizations for the Disaster Information Types and an Information System containing them

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:	?	?	?	?

https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-60v2r1.pdf

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:

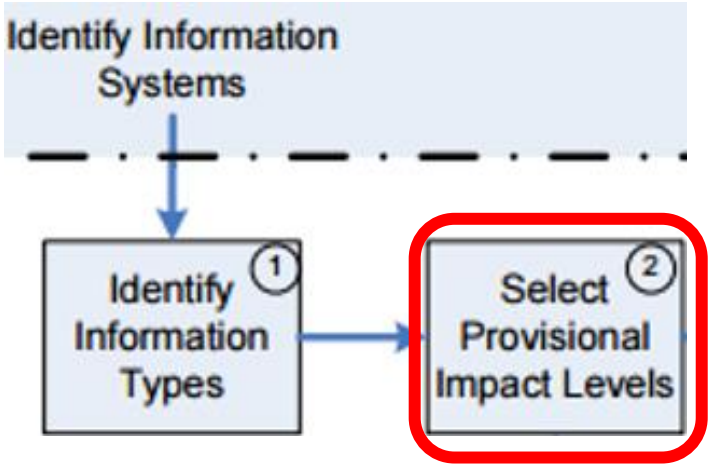
Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}

Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster monitoring and prediction information on the ability of responsible agencies to predict when and where a disaster may take place and communicate that information to affected parties. The purpose of disaster monitoring and prediction activities is generally to disseminate information. Sharing of raw information by a diverse group of analysts often improves the quality of predictive analysis.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of some disaster monitoring and prediction information may include public panic or other responses that jeopardize public safety, disaster prevention, emergency response, disaster repair, or restoration missions. For example, attempts of large populations to evacuate in an endangered area before necessary preparations are made for evacuation routes can result in a clogging of the routes and failure to evacuate large parts of the population in time to save them from a life-threatening event. Most of the disaster monitoring and prediction information is critical in terms of potential loss of human life and major property damage. The unauthorized release of this information may interfere with disaster prevention or emergency response missions. The confidentiality impact level recommended for the information cited in the example can be **moderate** or high.

Disaster Management Information Types



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:

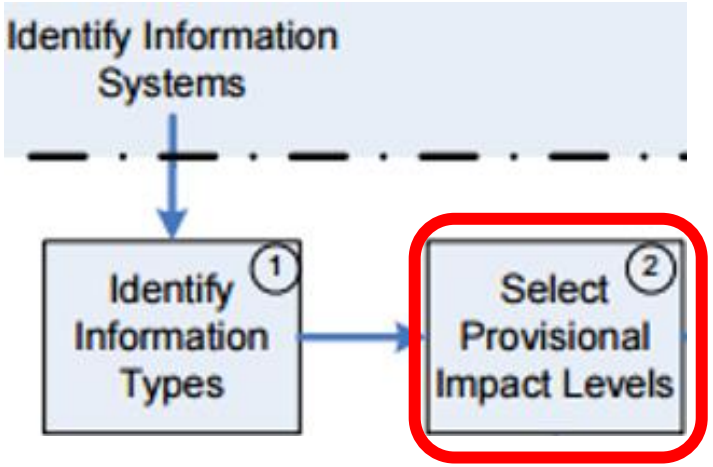
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

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)}

Determine the Security Categorizations of the 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:	**?**	**?**	**?**	

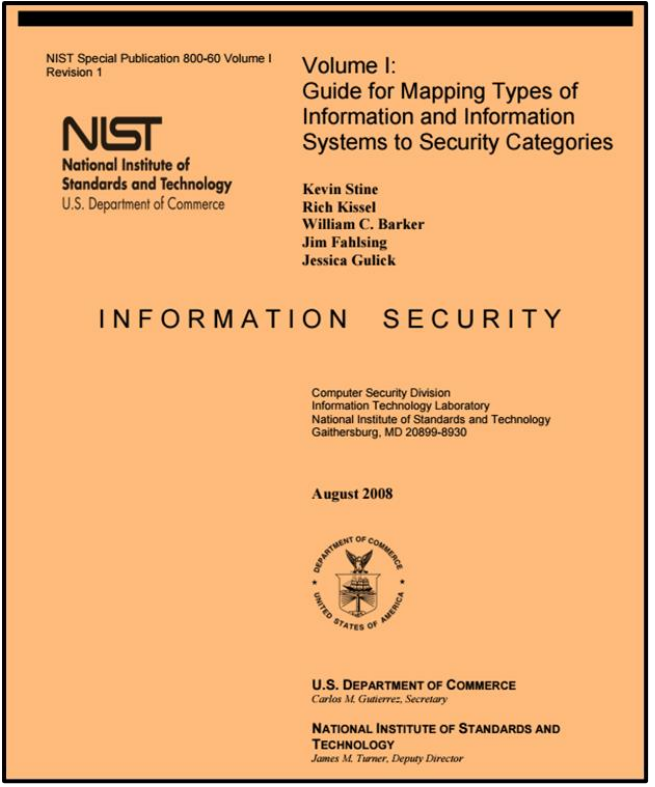
Determine the Overall Security Categorization of the Disaster Information System

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 Security Categorization of the 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	***High***



2. Once categorized, select security control baseline for the information system

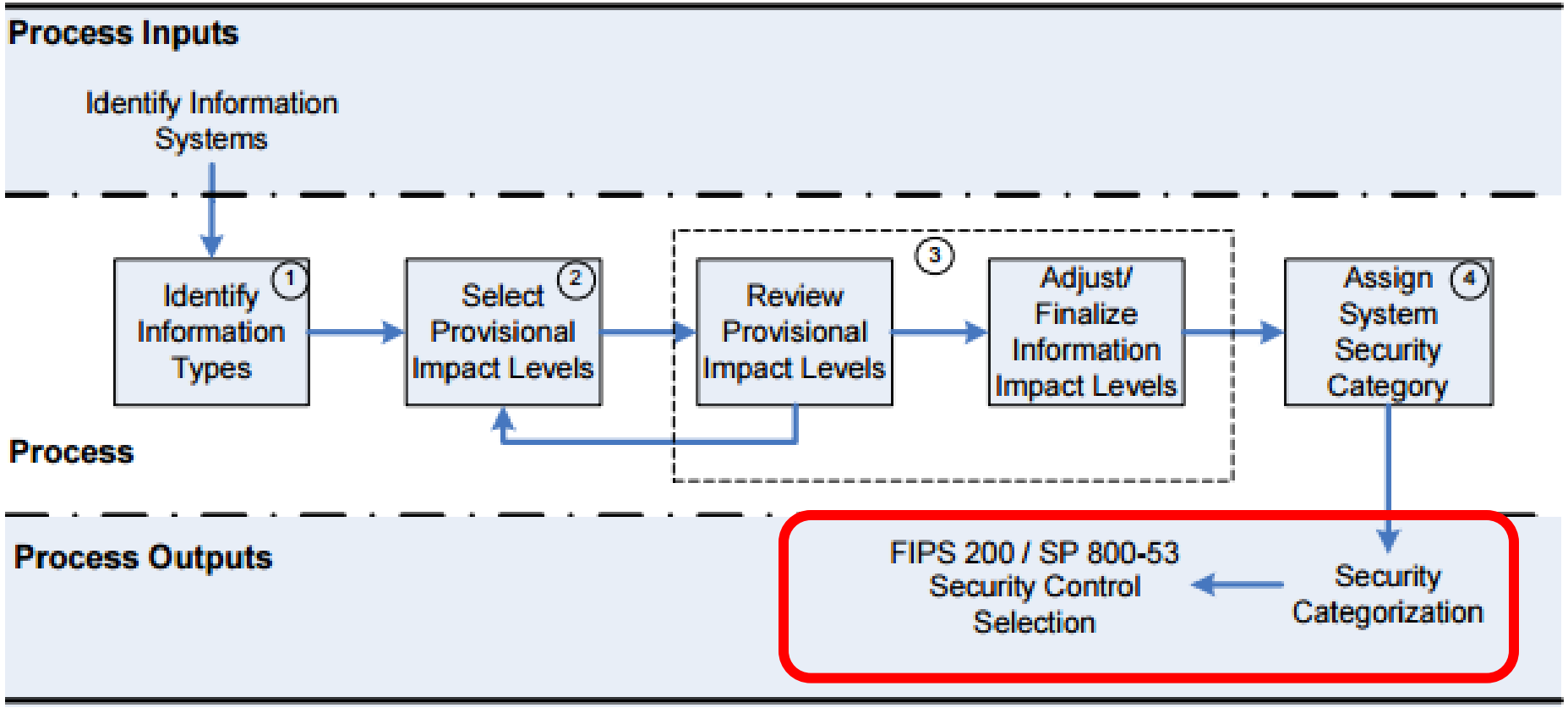
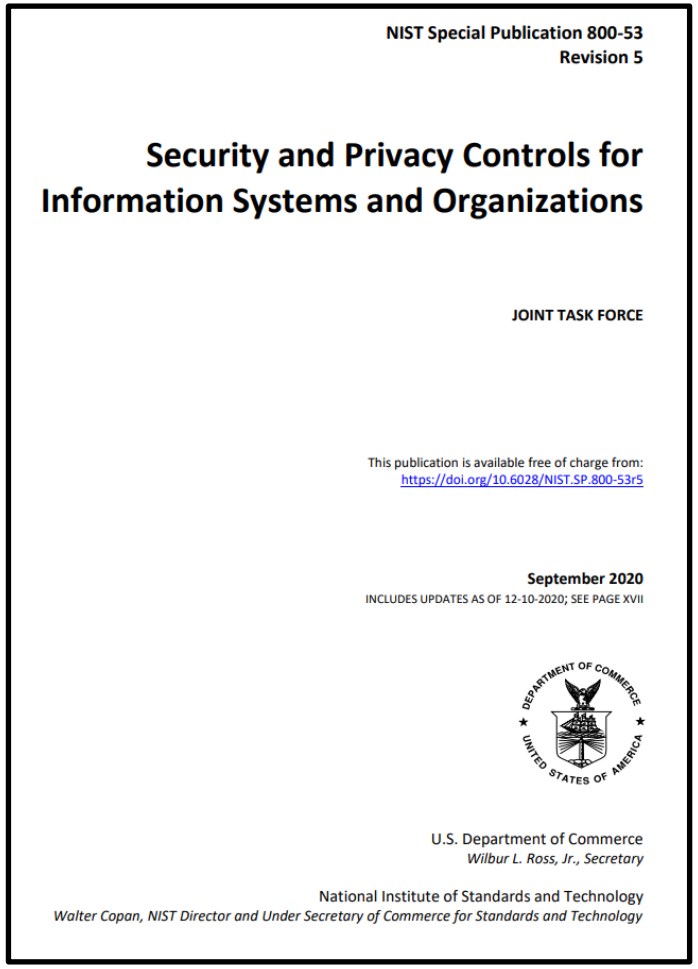


Figure 2: SP 800-60 Security Categorization Process Execution

Cybersecurity Controls are organized in “families”



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

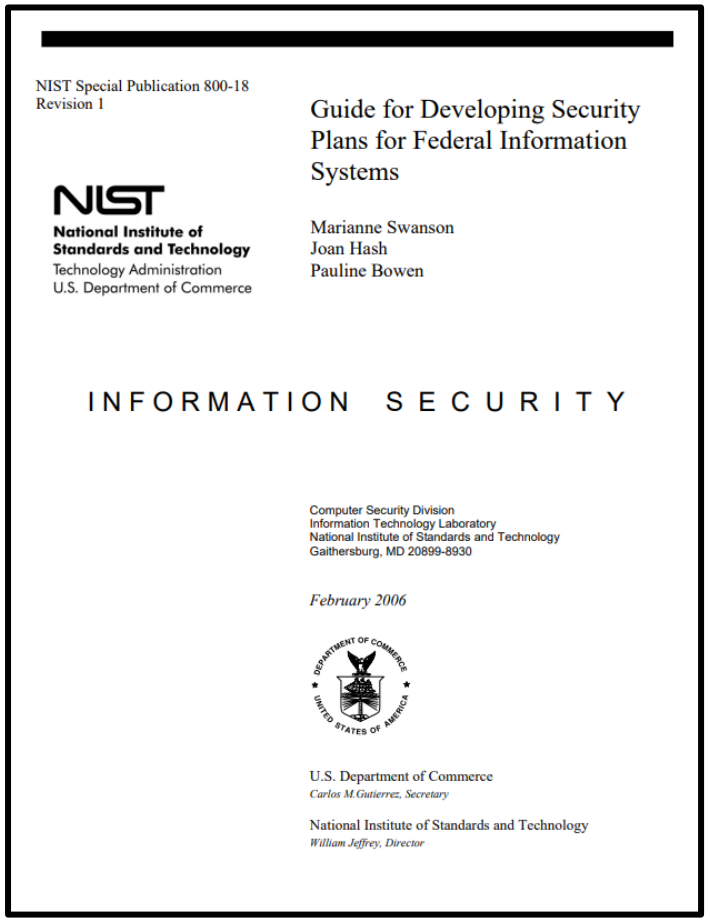
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

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

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Security control class designations help clarify controls in preparation of system security plans



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

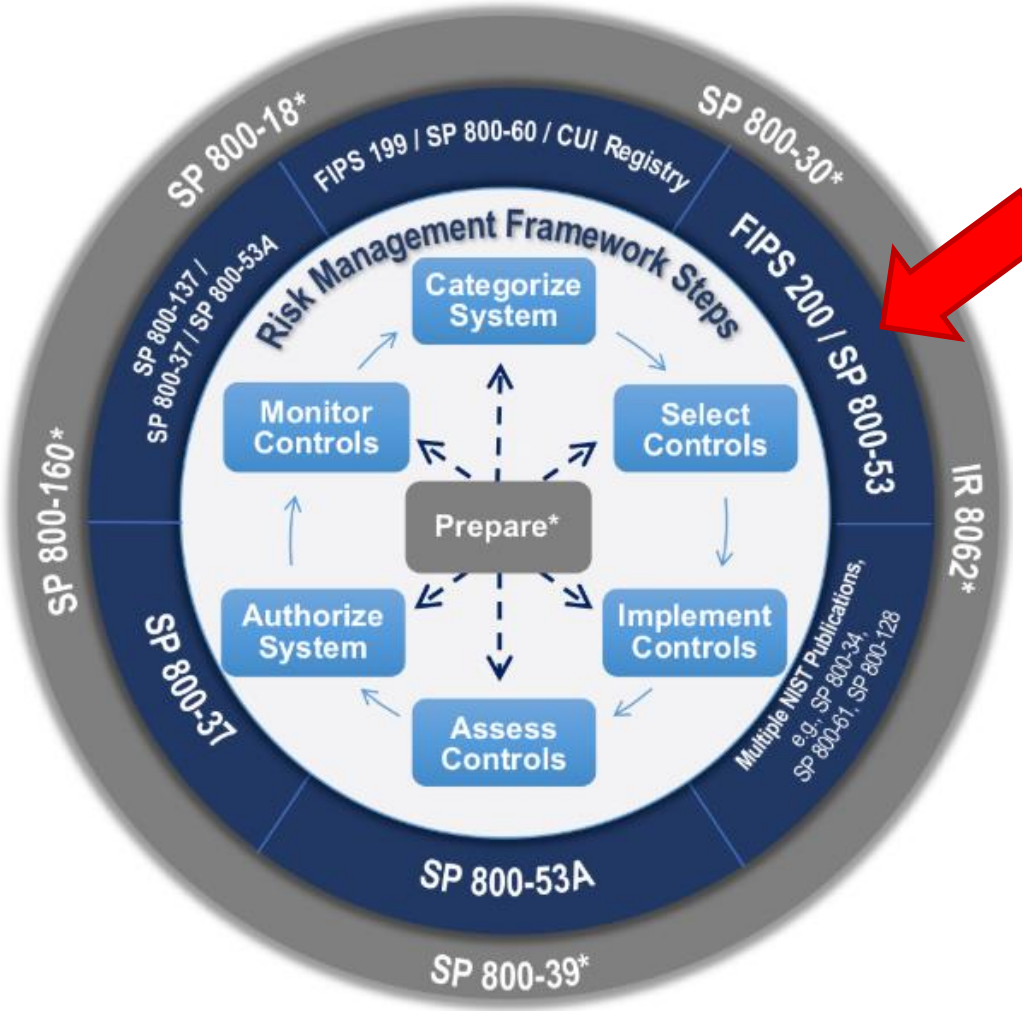
National Institute of Standards and Technology
William Jeffrey, Director

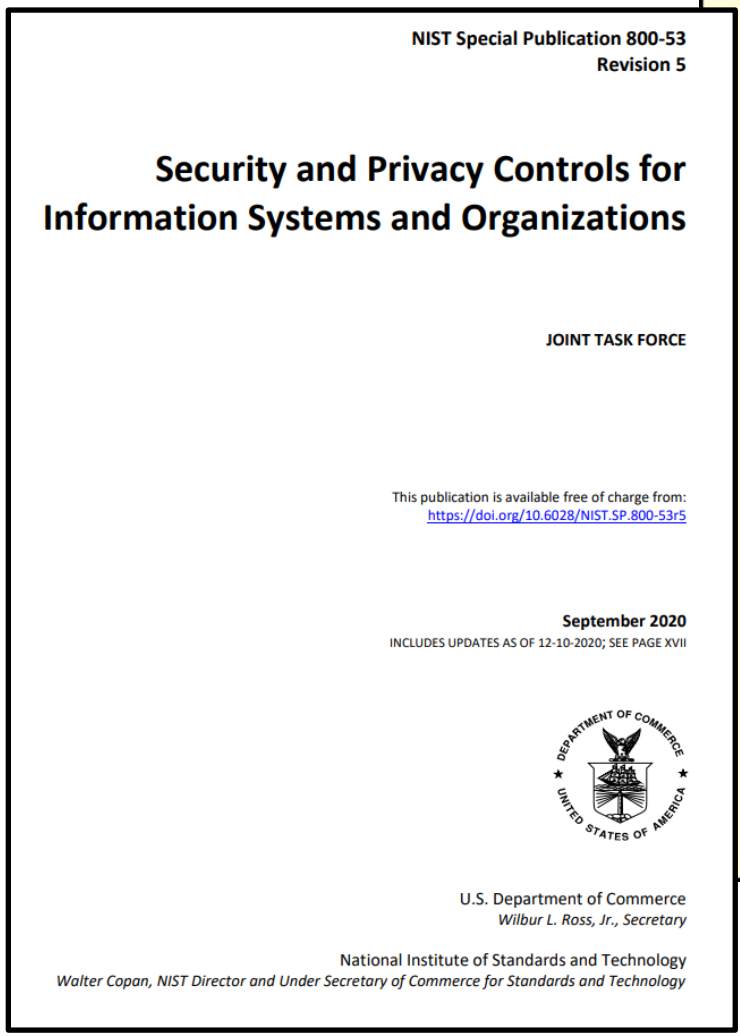
CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency 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

Management controls focus on management of the information system and management of risk for a system
Operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems) with technical expertise and/or management expertise
Technical controls focus on automated security controls that the computer system(s) executes

Selecting cybersecurity risk controls





NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

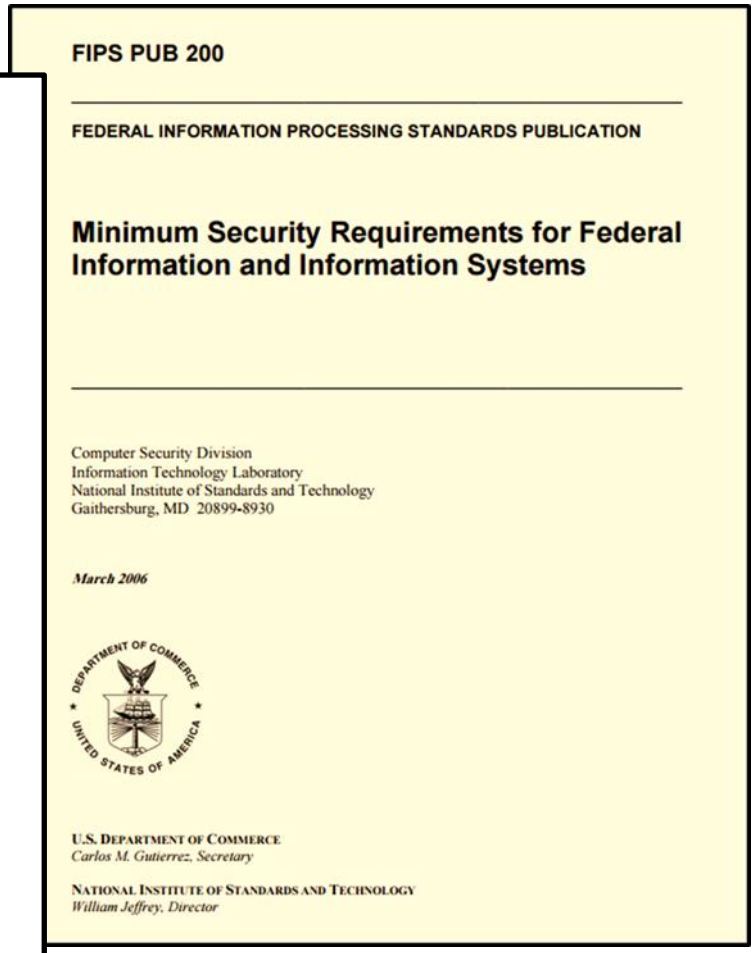
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

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



FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

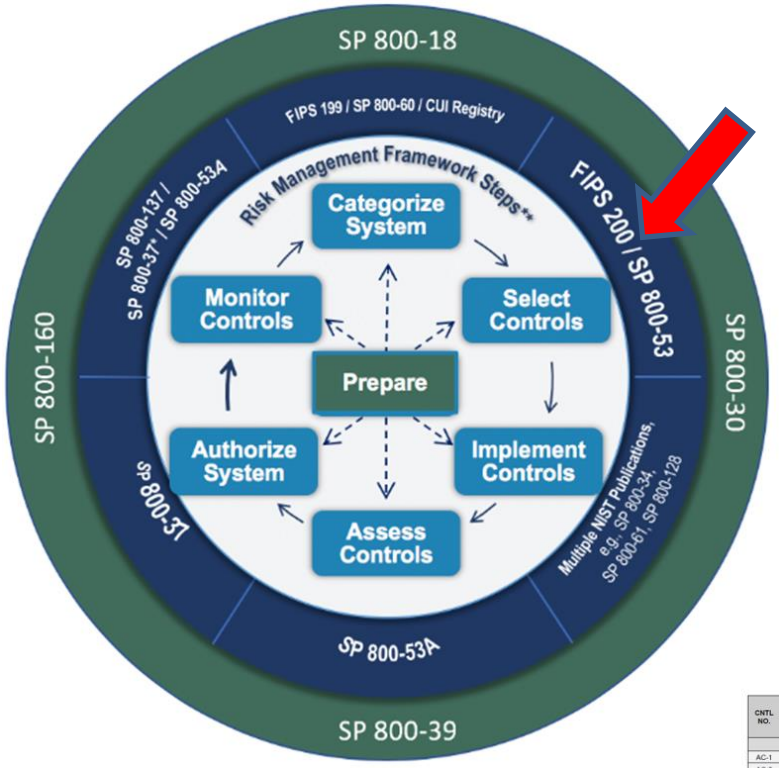
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

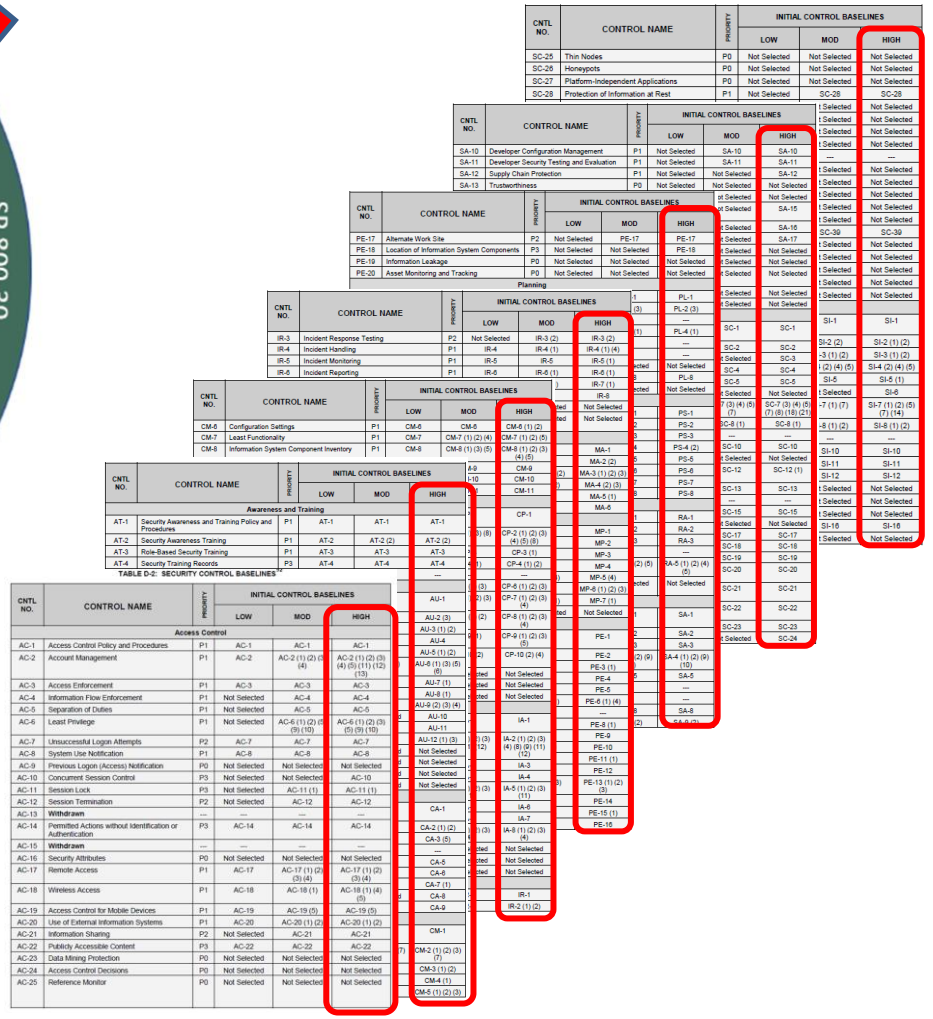
March 2006

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

FIPS 199 categorization is used to select among 3 security control baselines of security controls





CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

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

Agenda

- ✓ Categorizing Information for IT Risk Management
- ✓ Using Categorization to Select a Baseline of Security Controls
- Risk Evaluation
- Risk Management Techniques, a brief review
- Test taking tip
- Quiz

Risk Evaluation

Risk evaluation is the process of identifying risk scenarios and describing their potential business impact

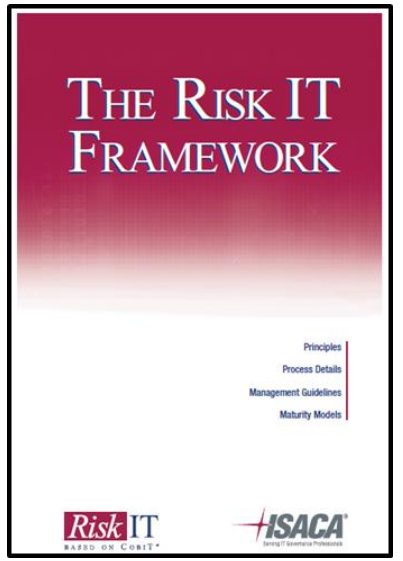
Risk Evaluation - Key Components

Collect Data	Identify relevant data to enable effective IT-related risk identification, analysis and reporting
Analyze Risk	Develop useful information to support risk decisions that take into account the business impact of risk factors
Maintain Risk Profile	Maintain and up-to-date and complete inventory of known risks and attributes as understood in the context of IT controls and business processes

Risk Evaluation - Collect Data (RE-1)

Goal: Ensure IT-related risks are identified, analyzed and presented in business terms

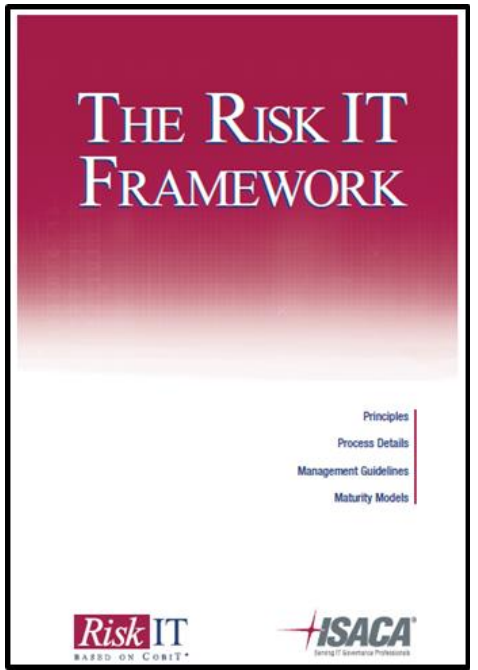
- **Metrics:**
  - # of loss events with key characteristics not captured or measured
  - Degree to which collected data support
    - Visibility and understanding of the threat landscape
      - Analyzing scenarios and reporting trends
      - Visibility and understanding of the control state



Risk Evaluation - Collect Data (RE1)

Existence of a documented risk data collection model

- # of data sources
- # of data items with identified risk factors
- Completeness of
  - Risk event data
    - Affected assets
    - Impact data
    - Threats
    - Controls
    - Measures of the effectiveness of controls
  - Historical data on risk factors

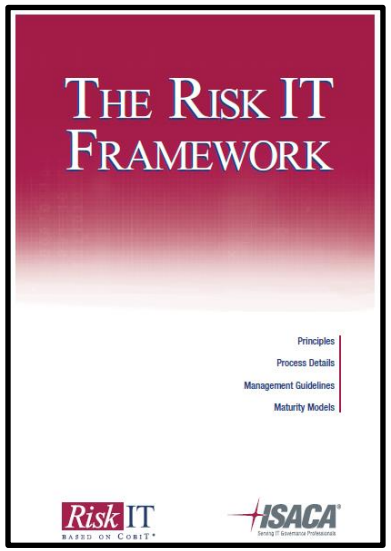


Risk Evaluation - Collect Data: Governance Roles

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE1.1 Establish and maintain a model for data collection.	I	I	A/R	C	C	C	C	C	C		C
RE1.2 Collect data on the operating environment.		I	A/R	C	I	I	C	I	I	I	C
RE1.3 Collect data on risk events.		I	A	R	C	I		C	C		I
RE1.4 Identify risk factors.			A	R	I	I	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.



Risk Evaluation - Key Components

Collect Data	Identify relevant data to enable effective IT-related risk identification, analysis and reporting
Analyze Risk	Develop useful information to support risk decisions that take into account the business impact of risk factors
Maintain Risk Profile	Maintain and up-to-date and complete inventory of known risks and attributes as understood in the context of IT controls and business processes

NYC Information Technology & Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Classification Policy

The Policy

The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope

This policy applies to all information
written, stored electronically, copie
New York general business, inform
customers.

Information Classification

All information at the City of New Yo
four levels; public, sensitive, private

- **Public**—This information mig
damage.
- **Sensitive**—This information r
inappropriate disclosure.
- **Private**—This information is f
public trust placed in the agen
- **Confidential**—This is the hig
damage to the agency's abilit
containing information whose
danger to public safety, or lea

Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Question:

How to approach categorizing and prioritizing an enterprise's data for protection?

Let’s set up an information security categorization for an example: Health Catalyst’s product line data

Determine the overall information security categorization of the different datasets

Datasets	Confidentiality	Integrity	Availability	"Overall" Impact Rating
Financial Management				
Accountable Care				
Population Health Management				
Operational and Workflow Improvement				
Patient Injury Prevention				

Remember the application of FIPS 199 to derive overall categorization of the Dean's laptop:

Asset \ Impact to	Confidentiality	Integrity	Availability	**Categorization**
Staff Salary Data	High	Low	Medium	High
Student Data	High	Low	Low	High
Fundraising Presentations	Medium	Medium	High	High
Dean's Personal Data	Low	Low	Medium	Medium

Synonyms: impact rating, security categorization, …

How can you find a way to transform the ordinal FIPS 199 impact ratings to ratio data to conduct a quantitative risk analysis?

Datasets	Impact	Likelihood	Risk
Financial Management	High	High	?
Accountable Care	High	Moderate	?
Population Health Management	Moderate	Moderate	?
Operational and Workflow Improvement	Low	Moderate	?
Patient Injury Prevention	Low	Low	?

NIST SP 800-100 Information Security Handbook: A Guide for Managers (Chapter 10, page 90)
https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-100.pdf

Analyze risk to prioritize protection

An authoritative lookup table for transforming ordinal to ratio risk data…

Threat Likelihood	Impact: Low (10)	Impact: Moderate (50)	Impact: 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)

NIST SP 800-100 Information Security Handbook: A Guide for Managers
https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-100.pdf

Analyze risk to prioritize protection

Threat Likelihood	Impact: Low (10)	Impact: Moderate (50)	Impact: 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

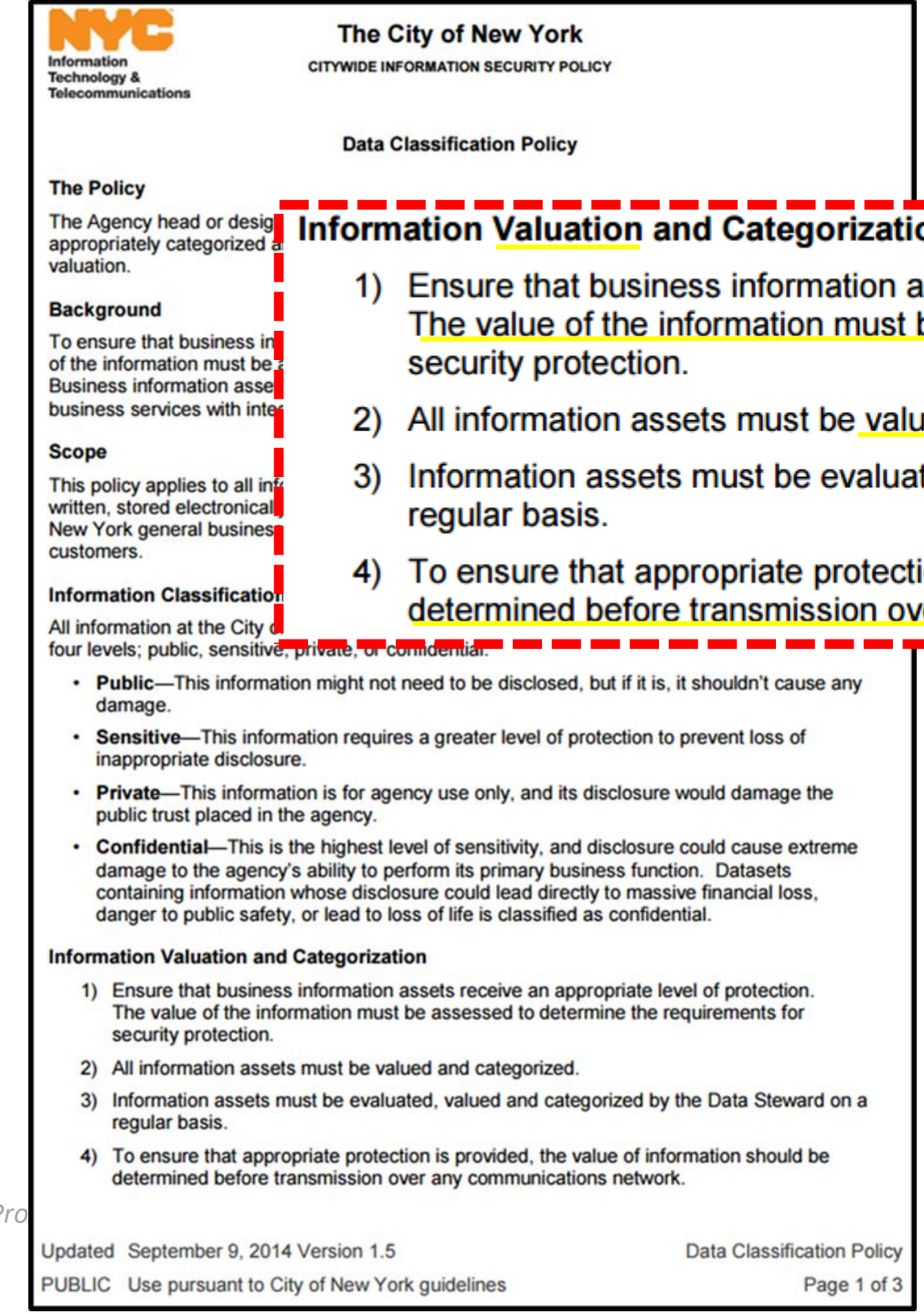
Risk Scale: High (>50 to 100) Moderate (>10 to 50) Low (1 to 10)

01527a

Transforming ordinal risk rankings to interval risk measures

Datasets	Impact	Likelihood	Risk
Financial Management	High	High	?
Accountable Care	High	Moderate	?
Population Health Management	Moderate	Moderate	?
Operational and Workflow Improvement	Low	Moderate	?
Patient Injury Prevention	Low	Low	?

Datasets	Impact	Likelihood	Risk
Financial Management	100	1.0	100
Accountable Care	100	0.5	50
Population Health Management	50	0.5	25
Operational and Workflow Improvement	10	0.5	5
Patient Injury Prevention	10	0.1	1



NYC Information Technology & Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Classification Policy

The Policy

The Agency head or desig
appropriately categorized a
valuation.

Background

To ensure that business in
of the information must be
Business information asse
business services with inte

Scope

This policy applies to all inf
written, stored electronical
New York general busines
customers.

Information Classificatio

All information at the City
four levels; public, sensitive, private, or confidential.

- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and disclosure could cause extreme damage to the agency's ability to perform its primary business function. Datasets containing information whose disclosure could lead directly to massive financial loss, danger to public safety, or lead to loss of life is classified as confidential.

Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

Updated September 9, 2014 Version 1.5 Data Classification Policy

PUBLIC Use pursuant to City of New York guidelines Page 1 of 3

Information Valuation and Categorization

1) Ensure that business information assets receive an appropriate level of protection. The value of the information must be assessed to determine the requirements for security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categorized by the Data Steward on a regular basis.
4) To ensure that appropriate protection is provided, the value of information should be determined before transmission over any communications network.

How do you assess the value of information to an organization?

Quantitative Risk Assessment

*E*xpected losses can be weighed against the costs of counter-measures and provides a basis for trading Information Security ("InfoSec") costs and benefits

- One simple assessment technique calculates the annual loss expectancy (ALE) as a product of the cost of a single event (single loss expectancy, SLE) and the annualized rate of occurrence (ARO)

$$Annual\ Loss\ Expectancy = \text{Single Loss Expectancy} \times \text{Annualized Rate of Occurrence}$$

annual rate of occurrence (ARO)= how many times is this expected to happen in one year?

- NOTE: The calculation assumes total loss of an asset. If an asset retains part of its useful value, the SLE should be adjusted by an appropriate amount.

Single loss expectancy (SLE) = Asset value X Exposure factor

Problem

How would you determine the Annual Loss Expectance (ALE) for the theft of the Dean's laptop from the Case Study 'Snowfall and a stolen laptop' ?

Annual Loss Expectancy Calculation example

Note the assumptions of:

- *5% probability of annual rate of occurrence*
- *Credit monitoring service for 1,000 individuals*

greatly influence the results…

Annual Loss Expectancy Calculation		
Credit Monitoring Service (1000 records):		$15,000
Dean's Lost Productivity (assume $300,000 salary):		
10 hours restoring data from various sources		$ 3,000
10 hours re-doing lost work		$ 3,000
Replacement Device:		$ 1,000
IT investigation:		$ 200
Single Loss Expectancy:		$22,200
Annualized Rate of Occurrence:	0.05	
Annual Loss Expectancy:		$ 1,100

Risk management decision

Decision:

- Mitigate expected loss of a dean's laptop through purchase of security countermeasures

  - Avoid
  - Accept
  - Transfer
  - ✓ **Mitigate**

Annual Loss Expectancy Calculation		
Credit Monitoring Service (1000 records):		$15,000
Dean's Lost Productivity (assume $300,000 salary):		
10 hours restoring data from various sources		$ 3,000
10 hours re-doing lost work		$ 3,000
Replacement Device:		$ 1,000
IT investigation:		$ 200
Single Loss Expectancy:		$22,200
Annualized Rate of Occurrence:	0.05	
Annual Loss Expectancy:		$ 1,110

Annual Cost of Countermeasures (per device)	
Automatic Backups:	$ 300
Managed Device Service:	$ 100
Annual Cost of Countermeasures:	$ 400

Analyze Risk

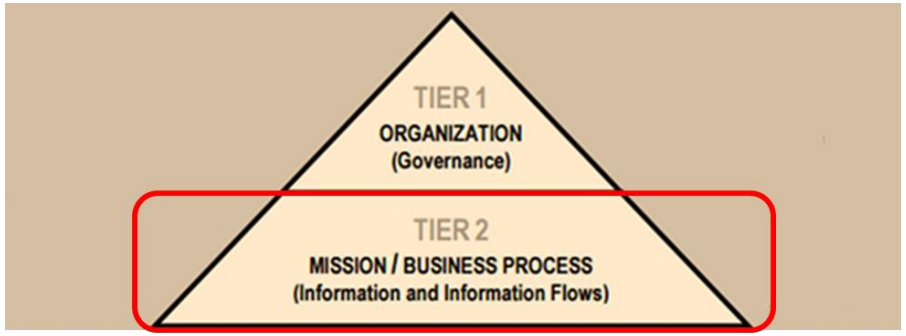
MANAGEMENT GUIDELINES—RE2

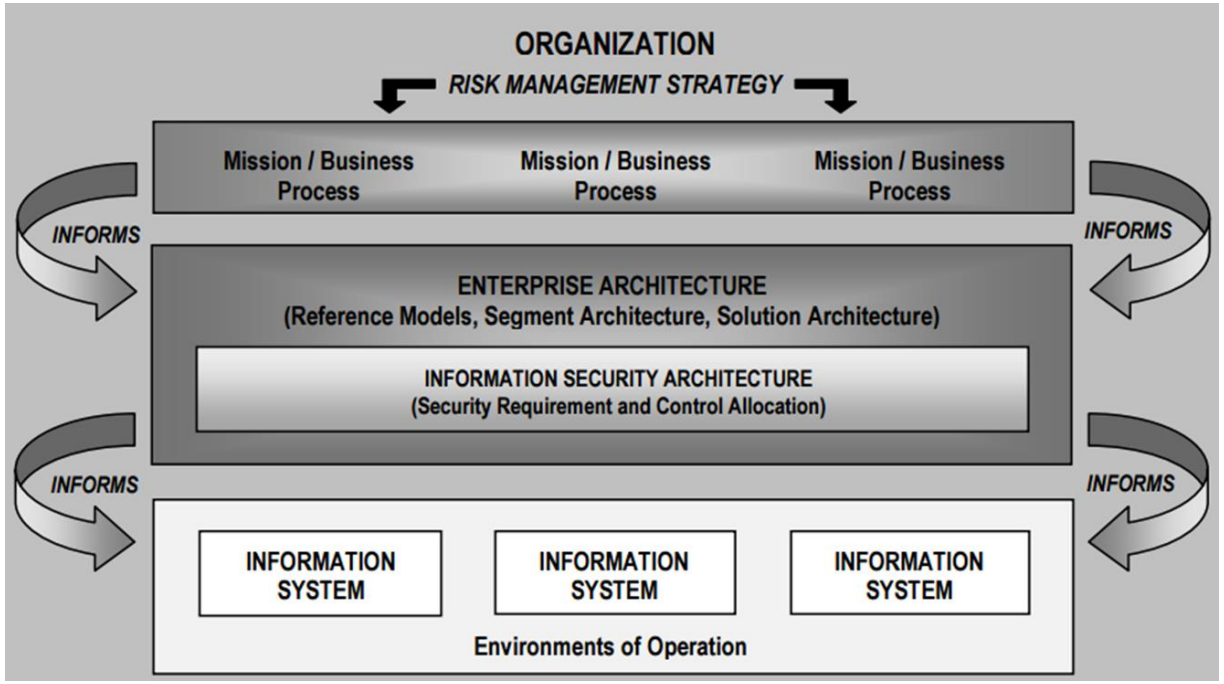
RACI Chart **Roles**

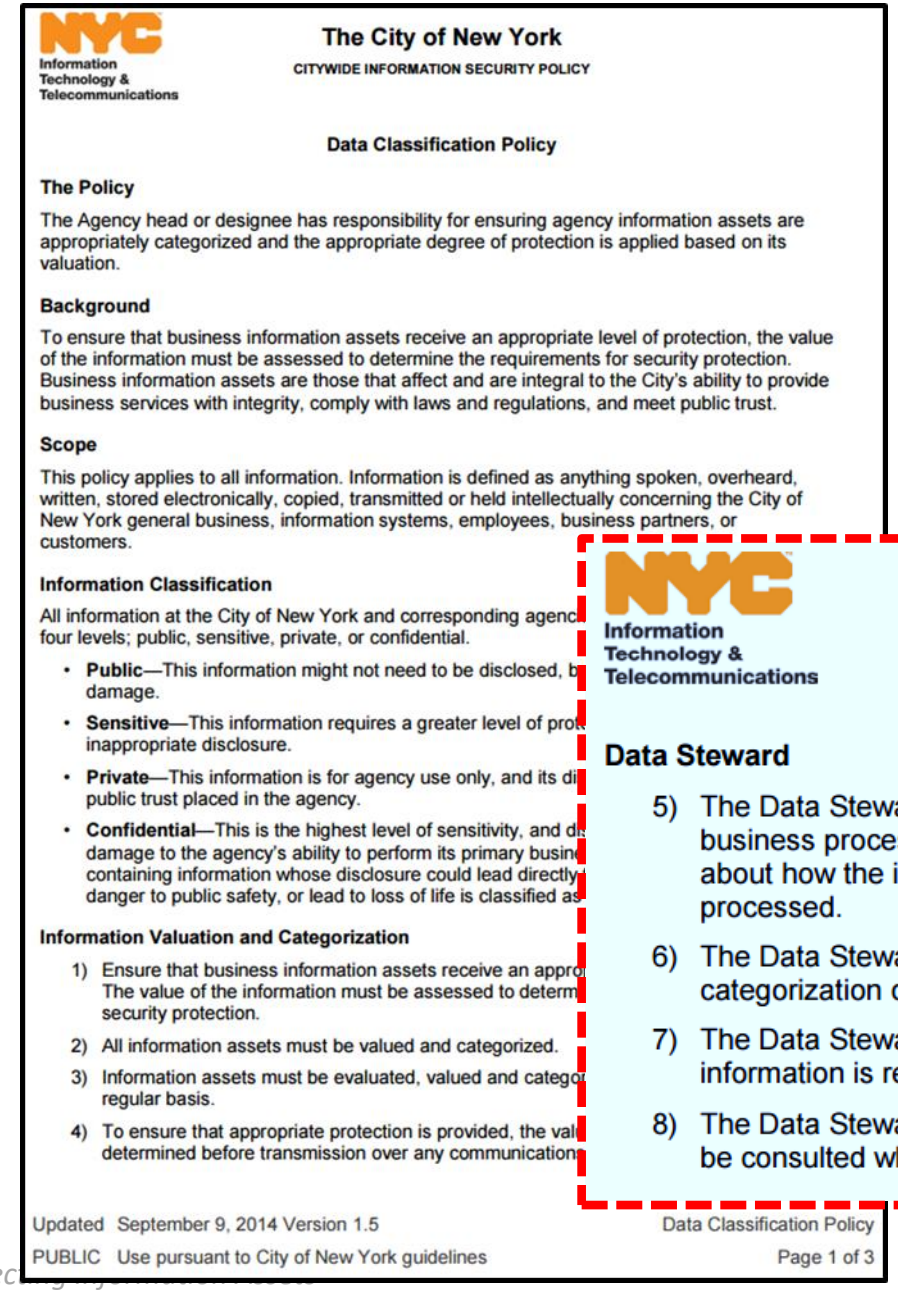
Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis.			A/R				I		I		I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

But… who really knows the value and impact a breach implies for the business?







Information Technology & Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Classification Policy

The Policy

The Agency head or designee has responsibility for ensuring agency information assets are appropriately categorized and the appropriate degree of protection is applied based on its valuation.

Background

To ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection. Business information assets are those that affect and are integral to the City's ability to provide business services with integrity, comply with laws and regulations, and meet public trust.

Scope

This policy applies to all information. Information is defined as anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning the City of New York general business, information systems, employees, business partners, or customers.

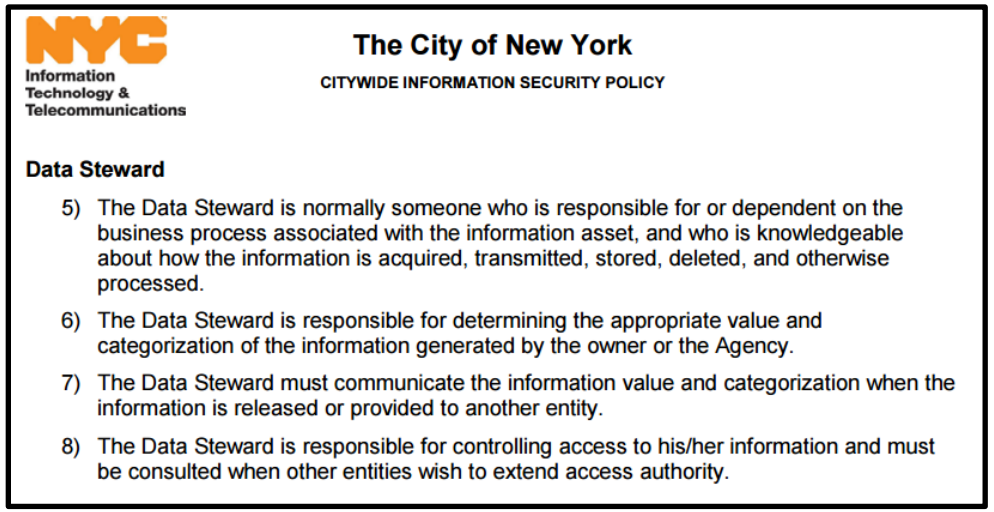
Information Classification

All information at the City of New York and corresponding agenc
four levels; public, sensitive, private, or confidential.

- **Public**—This information might not need to be disclosed, b
damage.
- **Sensitive**—This information requires a greater level of prot
inappropriate disclosure.
- **Private**—This information is for agency use only, and its di
public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and di
damage to the agency's ability to perform its primary busine
containing information whose disclosure could lead directly
danger to public safety, or lead to loss of life is classified as

Information Valuation and Categorization

1) Ensure that business information assets receive an appro
The value of the information must be assessed to determ
security protection.
2) All information assets must be valued and categorized.
3) Information assets must be evaluated, valued and categor
regular basis.
4) To ensure that appropriate protection is provided, the val
determined before transmission over any communication



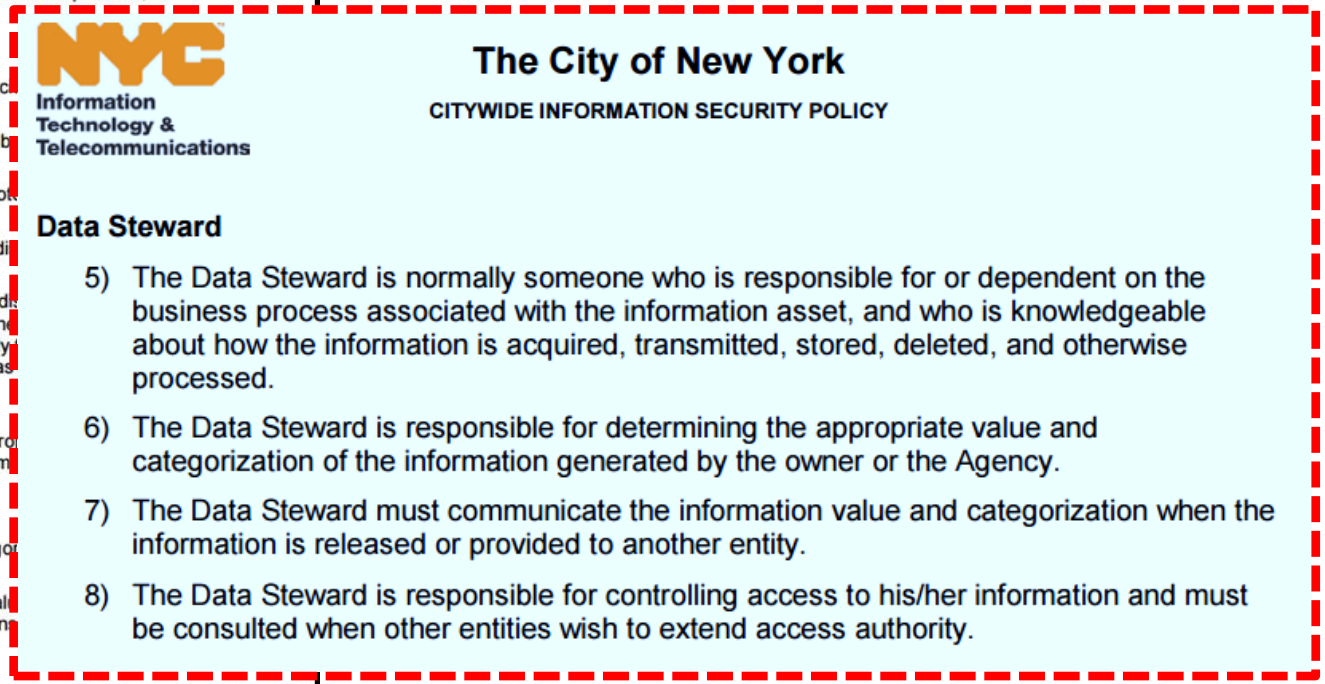
Information Technology & Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Steward

5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.
7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.
8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.



Information Technology & Telecommunications

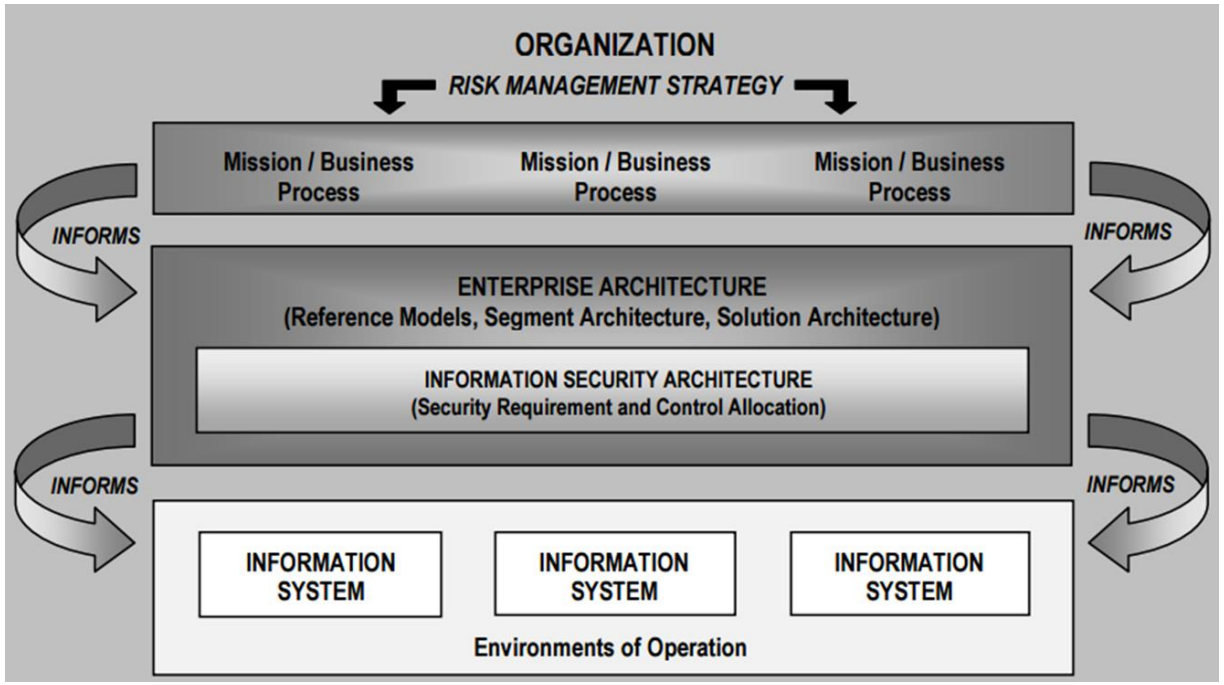
The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Steward

5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.
7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.
8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Where are the people who really know the value of the information and impact a breach implies for the business?



Maintain Risk Profile

RACI Chart **Roles**

Key Activities	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE3.1 Map IT resources to business processes.			I	R			C	A/R	C		I
RE3.2 Determine business criticality of IT resouces.		C		R		C	A	R			I
RE3.3 Understand IT capabilities.			C	A/R				C	C		I
RE3.4 Update IT risk scenario componenets.			C	R	I	C	C	A	R		C
RE3.5 Maintain the IT risk register and IT risk map.		I	A	R	I	I	I	R/C	C		I
RE3.6 Develop IT risk indicators.			A	C			C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

NYC Information Technology & Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Data Steward

5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

6) The Data Steward is responsible for determining the appropriate value and categorization of the information generated by the owner or the Agency.

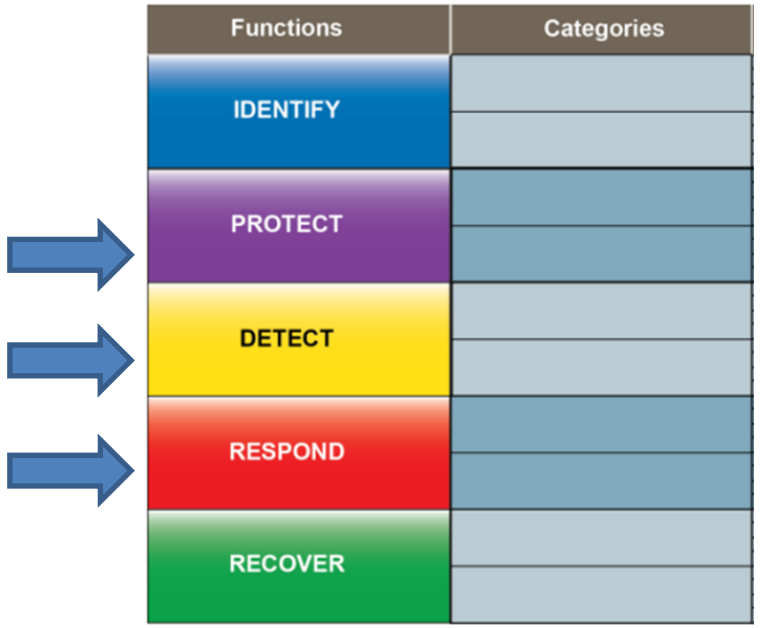
7) The Data Steward must communicate the information value and categorization when the information is released or provided to another entity.

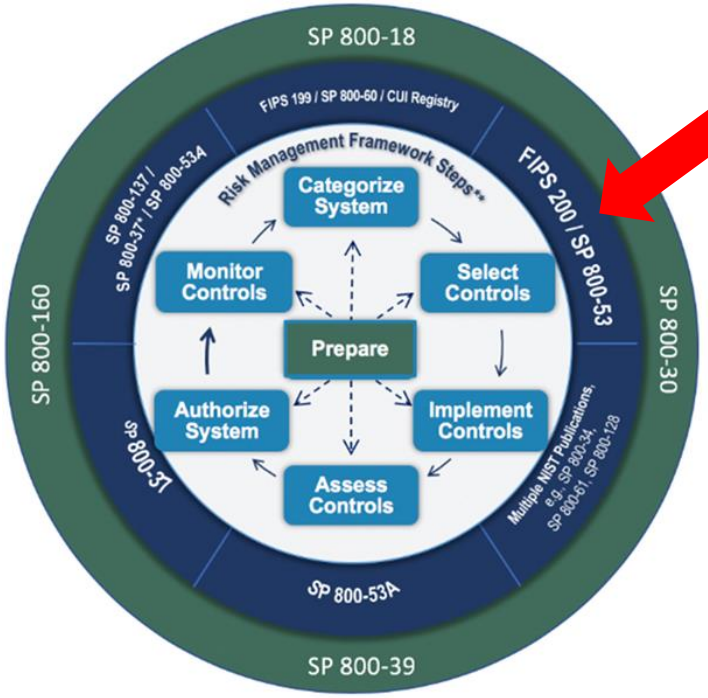
8) The Data Steward is responsible for controlling access to his/her information and must be consulted when other entities wish to extend access authority.

Review: Risk Management Techniques

Once threats and risks are identified, each risk can be managed by:

1. Avoidance
2. Acceptance
3. Transfer
4. Mitigation ("Controls")





Agenda

- ✓ In The News
- ✓ More on Confidentiality: Linked & Linkable PII
- ✓ Risk Evaluation
- ✓ Risk Management Techniques, a brief review
- Test taking tip
- Quiz

Test Taking Tip

- Eliminate any "probably wrong" answers first -

Focus on the "highest likelihood" answers for test taking efficiency

Here's why:

- Some of the answers use unfamiliar terms and stand out as unlikely and can therefore be discarded immediately
- Some answers are clearly wrong and you can recognize them based on your familiarity with the subject
- The correct answer may require a careful reading of the wording of the question and eliminating the unlikely answers early in the evaluation process helps you focus on key concepts for making the choice

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

A. Mandatory
B. Role-Based
C. Discretionary
D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

~~A. Mandatory~~ Nothing seems mandatory about this scenario

B. Role-Based

C. Discretionary

D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

~~A. Mandatory~~

B. Role-Based Maybe ….

C. Discretionary

D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

~~A. Mandatory~~

~~B. Role-Based~~ Nothing about roles other than manager in the question

C. Discretionary

D. Distributed

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

~~A. Mandatory~~
~~B. Role-Based~~
C. Discretionary
~~D. Distributed~~ Distributed is not relevant to the information in the question

Test Taking Tip

Example:

The promotion manager of Northeast Electronics has been made the owner of the department's printers and other resources. The manager can now designate who in the department can use the the large format printer. What term is used to describe this type of access control?

~~A. Mandatory~~
~~B. Role-Based~~
C. Discretionary
~~D. Distributed~~

Answer: C

Quiz

Quiz

The overall objective of risk management is to:

A. eliminate all vulnerabilities, if possible
B. reduce risk to the lowest possible level
C. manage risk to an acceptable level
D. implement effective counter measures

Quiz

The overall objective of risk management is to:

A. eliminate all vulnerabilities, if possible
B. reduce risk to the lowest possible level
C. manage risk to an acceptable level
D. implement effective counter measures

Quiz

The information security manager should treat regulatory compliance as:

A. an organizational mandate
B. a risk management priority
C. a purely operational issue
D. another risk to be managed

Quiz

The information security manager should treat regulatory compliance as:

A. an organizational mandate
B. a risk management priority
C. a purely operational issue
D. another risk to be managed

Quiz

To address changes in risk, an effective risk management program should

A. ensure that continuous monitoring processes are in place
B. establish proper security baselines for all information resources
C. implement a complete data classification process
D. change security policies on a timely basis to address changing risk

Quiz

To address changes in risk, an effective risk management program should

A. ensure that continuous monitoring processes are in place
B. establish proper security baselines for all information resources
C. implement a complete data classification process
D. change security policies on a timely basis to address changing risk

Quiz

Information classification is important to properly manage risk PRIMARILYbecause:

A. it ensures accountability for information resources as required by rolesand responsibilities
B. it is a legal requirement under various regulations
C. it ensures adequate protection of assets commensurate with the degree of risk
D. asset protection can then be based on the potential consequences ofcompromise

Quiz

Information classification is important to properly manage risk PRIMARILYbecause:

A. it ensures accountability for information resources as required by rolesand responsibilities
B. it is a legal requirement under various regulations
C. it ensures adequate protection of assets commensurate with the degree of risk
D. asset protection can then be based on the potential consequences of compromise

Quiz

Data owners are PRIMARILY responsible for creating risk mitigation strategies to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

Quiz

Data owners are PRIMARILY responsible for creating risk mitigation strategies to address which of the following areas?

A. Platform security
B. Entitlement changes
C. Intrusion detection
D. Antivirus controls

Quiz

A risk analysis should:

A. limit the scope to a benchmark of similar companies
B. assume an equal degree of protection of all assets
C. address the potential size and likelihood of loss
D. give more weight to the likelihood vs. the size of the loss

Quiz

A risk analysis should:

A. limit the scope to a benchmark of similar companies
B. assume an equal degree of protection of all assets
C. address the potential size and likelihood of loss
D. give more weight to the likelihood vs. the size of the loss

Quiz – *Bonus question*

A year ago when Sam carried out a risk analysis, he determined that the company was at too much of a risk when it came to potentially loosing trade secrets.

The countermeasures his team implemented reduced this risk, and Sam determined that the annualized loss expectancy of the risk of a trade secret being stolen once in a hundred-year period is now $400.

What is the associated single loss expectancy value in this scenario?

Agenda

- ✓ Categorizing Information for IT Risk Management
- ✓ Using Categorization to Select a Baseline of Security Controls
- ✓ Risk Evaluation
- ✓ Test taking tip
- ✓ Quiz