

MIS 5206  
Protection of Information Assets  
- Unit #3 -

Risk Evaluation

# Agenda

- In The News...
- Categorizing Information for IT Risk Management
- Revisit Risk & Controls of Publicly Shared Geographic Information
- More on Confidentiality: Linked & Linkable PII
- Risk Evaluation
- Risk Management Techniques, a brief review
- Test taking tip
- Quiz

# In the News



**Celinemary Turner** says

SEPTEMBER 10, 2023 AT 11:23 PM

Smaller Companies Must Embrace Risk Management

by Ariane Chapelle

September 08, 2023

<https://hbr.org/2023/09/smaller-companies-must-embrace-risk-management>

There are accepted rules for effective risk management: vigilance is key, and rapid intervention reduces impact. "If you see something, say something" is the New York City Subway's motto to prevent terrorist attacks. "See it, say it, sorted" is the equivalent for the London Underground.

Managing risks is inseparable from managing performance. Positive risk management aims to capture the upside of uncertainty, and to prevent the downside as much as possible.

<https://hbr.org/2023/09/smaller-companies-must-embrace-risk-management>

# In the News



**Ooreofeoluwa Koyejo says**

SEPTEMBER 12, 2023 AT 3:53 PM

Social Engineering Attacks Targeted at IT Admins

<https://blog.knowbe4.com/social-engineering-okta-credentials> Sept 7

<https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection> Aug 31

The attackers used social engineering tactics aimed at convincing the IT service desk personnel within organisations reset the MFA factors/administrative privileges of highly privileged users of US based Okta customers which would then leverage their compromise of highly privileged Okta Super Administrator accounts to abuse legitimate identity federation features that enabled them to impersonate users within the compromised organization that enabled them to impersonate users within the compromised organization.

Okta is an identity and authentication management provider, multiple reports with similar patterns were made to okta by their tenant clients.

These recent attacks highlight why protecting access to highly privileged accounts is so essential.

<https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection>

# In the News



**Jon Stillwagon** says

SEPTEMBER 12, 2023 AT 5:01 PM

<https://thehackernews.com/2023/09/vietnamese-hackers-deploy-python-based.html>

This news article is about Vietnamese hackers that use Python-based stealer to send to people on Facebook Messenger. It is a multi-stage process that is meant to steal your business account. The hackers target business accounts that basically send them messages to entice them to click on them. Then it leads them to delete all cookies and login credentials but before it deletes all the cookies it takes them from you first. Once they have your stolen cookies they then use them to change your passwords and to take control of them. Then sends the stolen data out to be sold on the market. 1 out of 250 victims are expected to be affected in the last 30 days which uses a tiny compressed file that is attached and sent to the potential victim.

<https://thehackernews.com/2023/09/vietnamese-hackers-deploy-python-based.html>

# In the News



**Edge Kroll** says

SEPTEMBER 12, 2023 AT 8:56 PM

<https://www.securityweek.com/crash-dump-error-how-a-chinese-espionage-group-exploited-microsofts-errors/>

This article explains how Microsoft has released a report revealing multiple mistakes that allowed Chinese hackers to breach U.S. government emails. The incident was attributed to a crash dump taken from a compromised engineer's corporate account in April 2021, which contained a Microsoft account (MSA) consumer key used to create tokens for unauthorized access to OWA and Outlook.com accounts. The report cited a race condition issue that permitted the key's inclusion in the crash dump, which has since been fixed. Microsoft also acknowledged the failure of its internal systems to detect sensitive data leaks from crash dumps. Furthermore, the company does not possess specific logs of the exfiltration, leading to criticism of its M365 licensing structure and prompting plans to enhance logging defaults and data retention for lower-tier customers.

This security breach resulted in the theft of emails from around 25 organizations and led to U.S. Senator Ron Wyden's call for Microsoft to be held accountable for "negligent cybersecurity practices" that facilitated the Chinese espionage campaign against the U.S. government. The U.S. government has initiated an investigation by its Cyber Safety Review Board (CSRB) into the Microsoft cloud hack and related issues concerning cloud-based identity and authentication infrastructure.

<https://www.securityweek.com/crash-dump-error-how-a-chinese-espionage-group-exploited-microsofts-errors/>

# In the News



**Bo Wang says**

SEPTEMBER 12, 2023 AT 10:26 PM

<https://www.infosecurity-magazine.com/news/cybercriminals-jailbreak-ai/>

Criminals use AI vulnerabilities to avoid asking questions that violate the law. It is possible to use AI to hack.

<https://www.infosecurity-magazine.com/news/cybercriminals-jailbreak-ai/>

*This is an example of an InTheNews post that is not properly summarized – summary is way too short to explain what the article is about.*

# Agenda

- ✓ In The News...
- Categorizing Information for IT Risk Management
- Revisit Risk & Controls of Publicly Shared Geographic Information
- More on Confidentiality: Linked & Linkable PII
- Risk Evaluation
- Risk Management Techniques, a brief review
- 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”

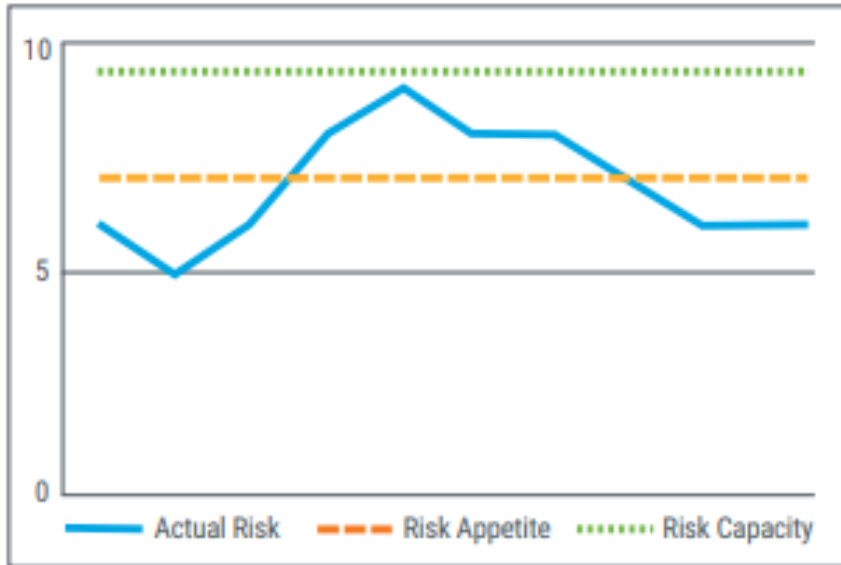


Diagram show a relatively sustainable situation

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

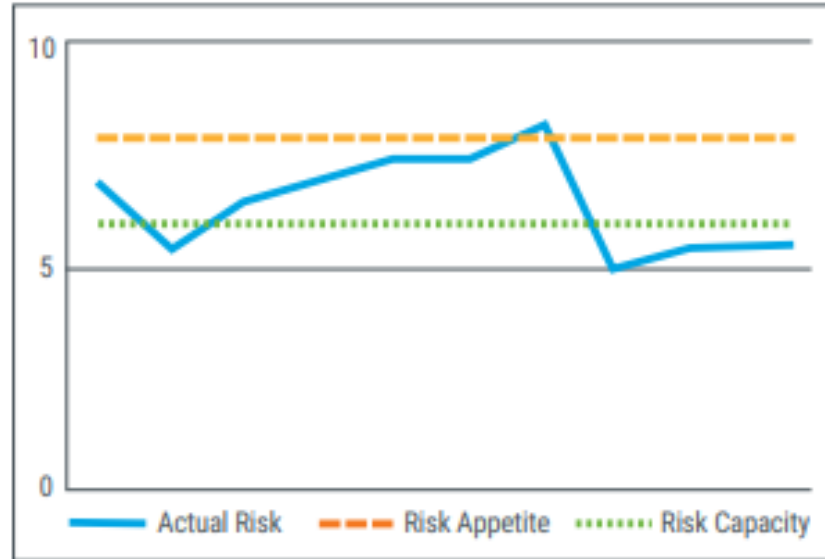
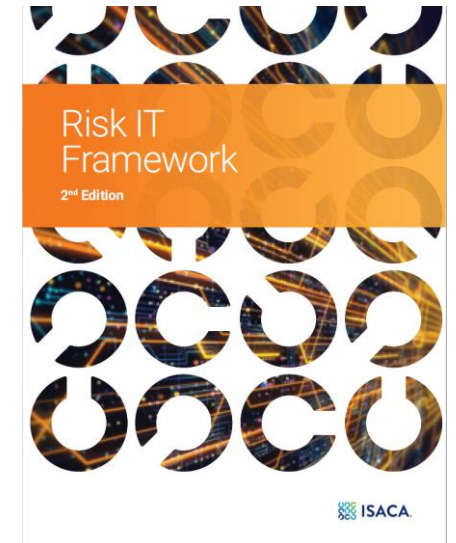


Diagram show an unsustainable situation

- 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

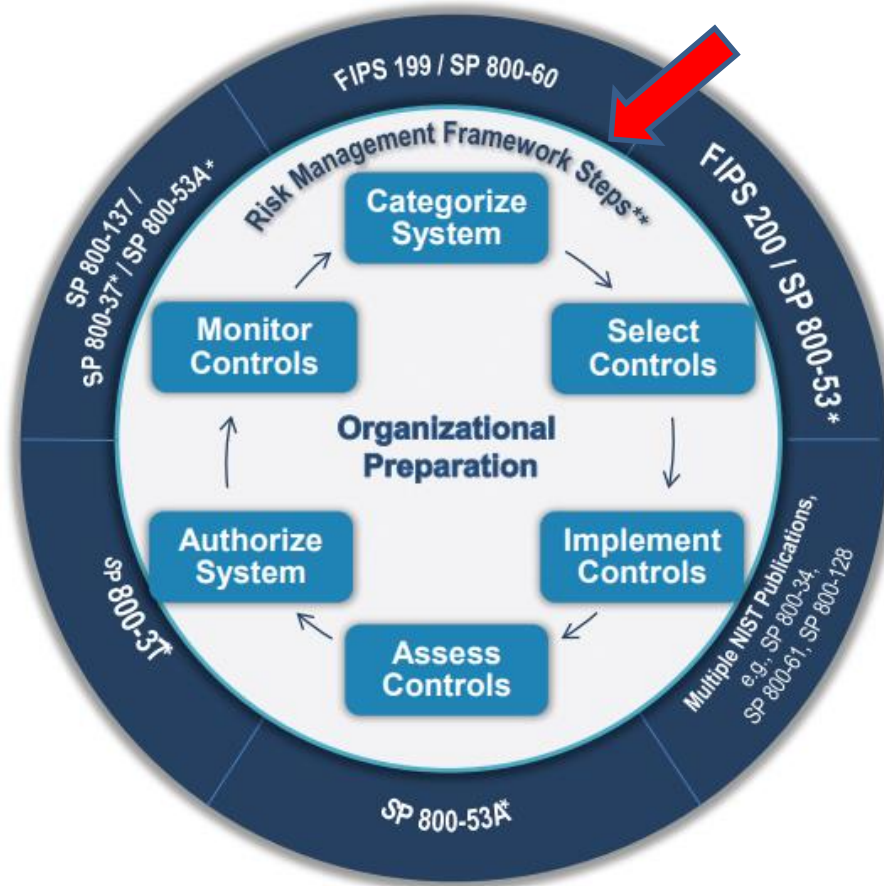
## Cybersecurity Maturity Model Certification (CMMC) levels

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



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

# Information inventory, categorization and risk evaluation form 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>

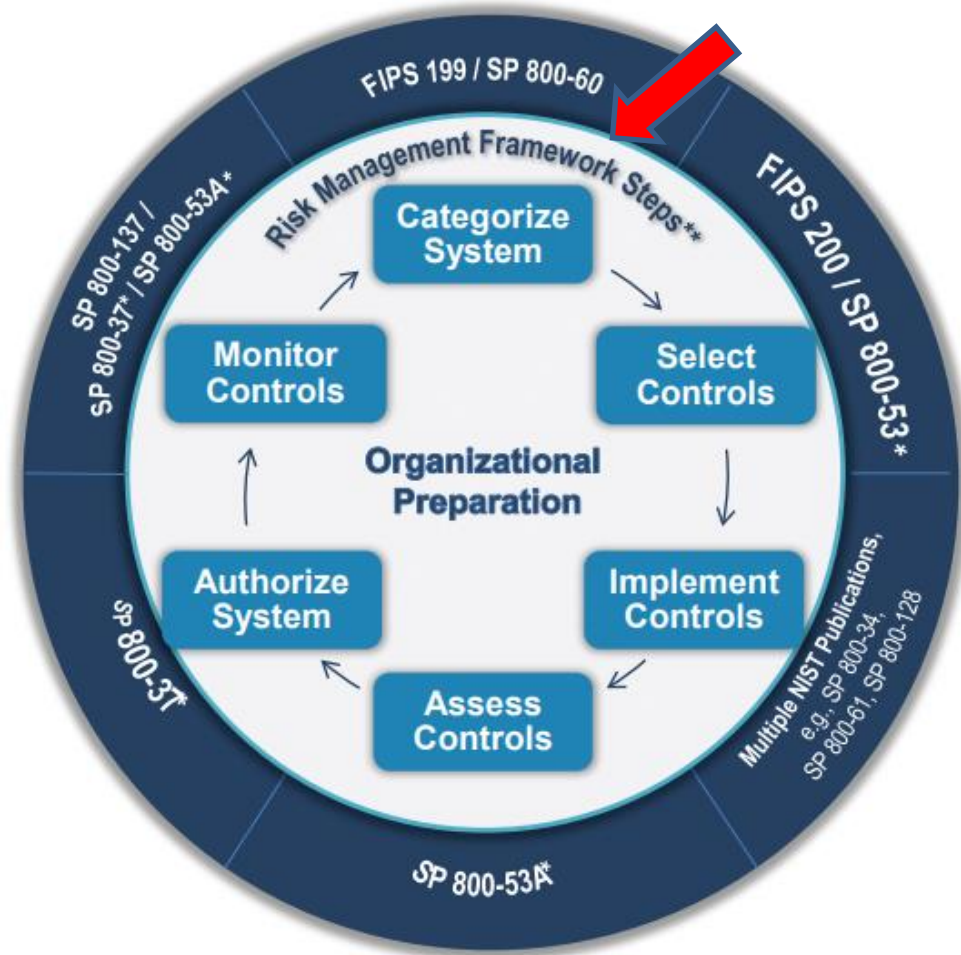
# Information Categorization is part of Risk Evaluation



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...

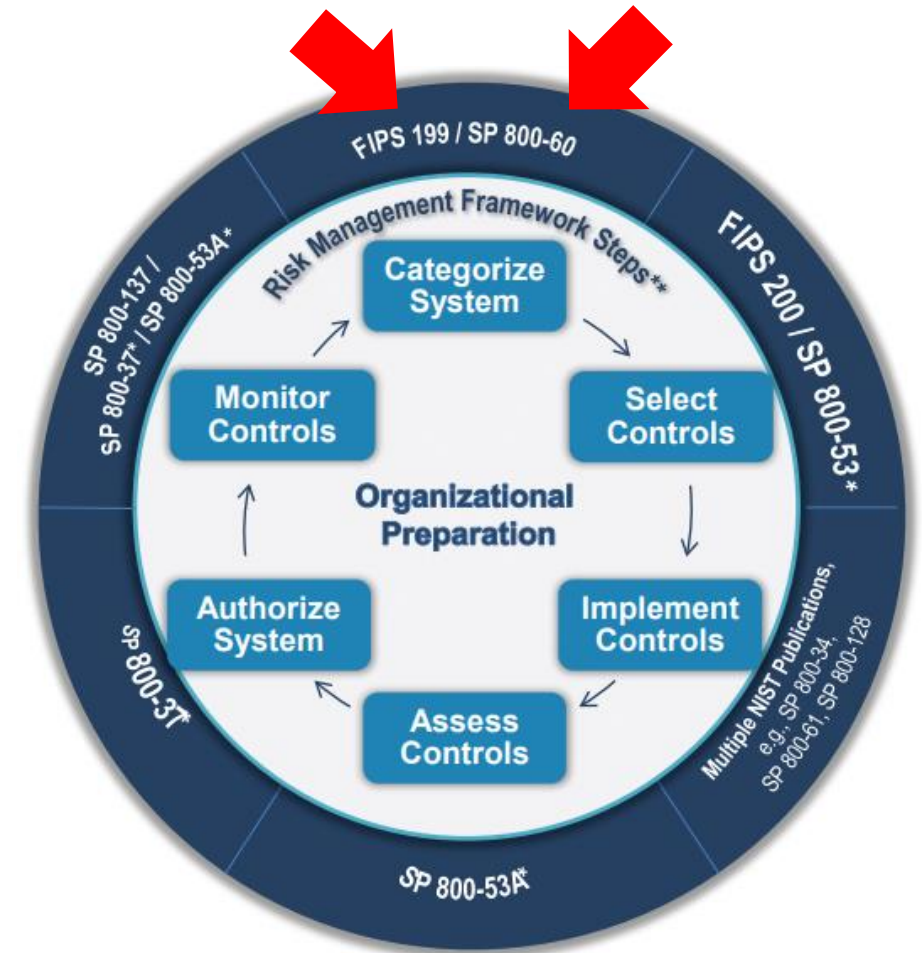
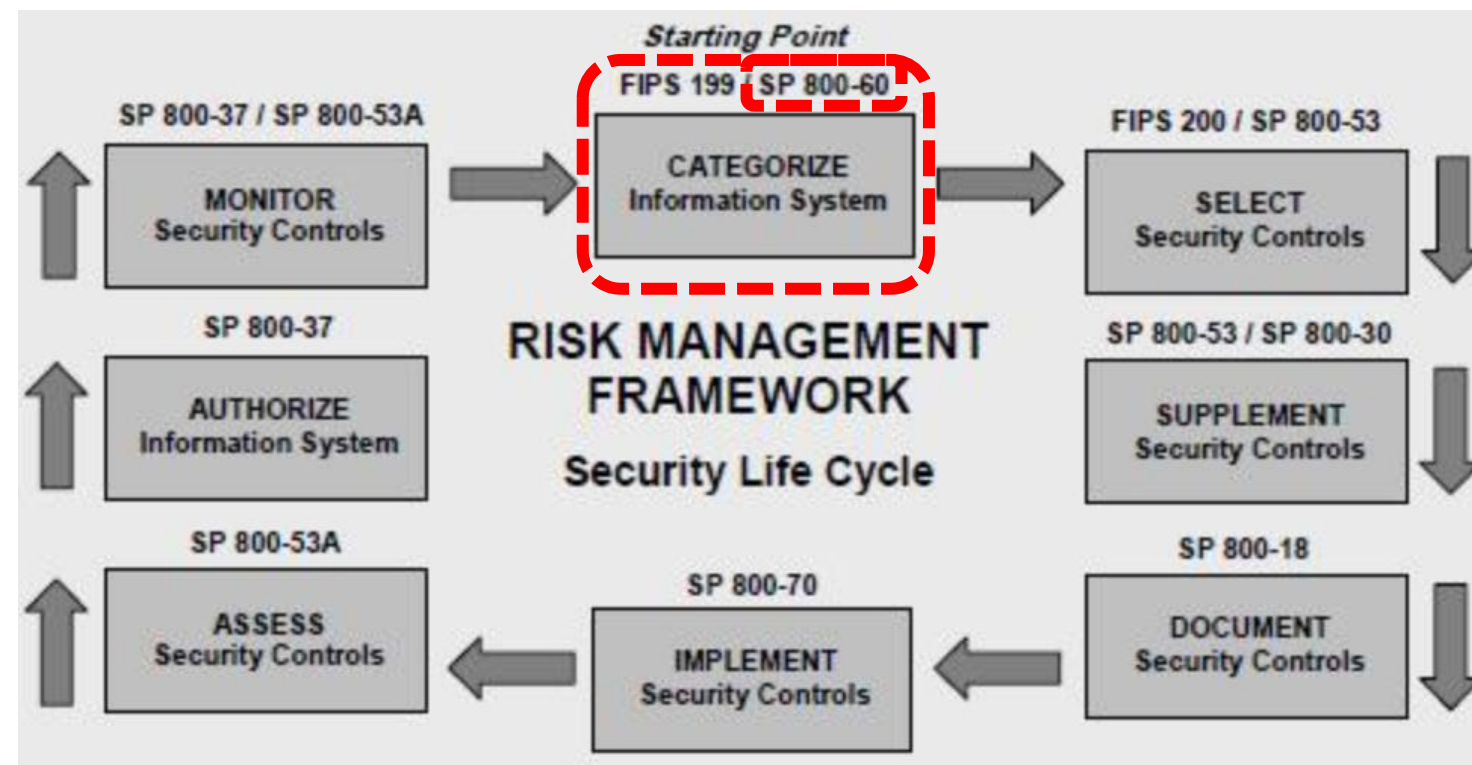


NIST Risk Management Framework

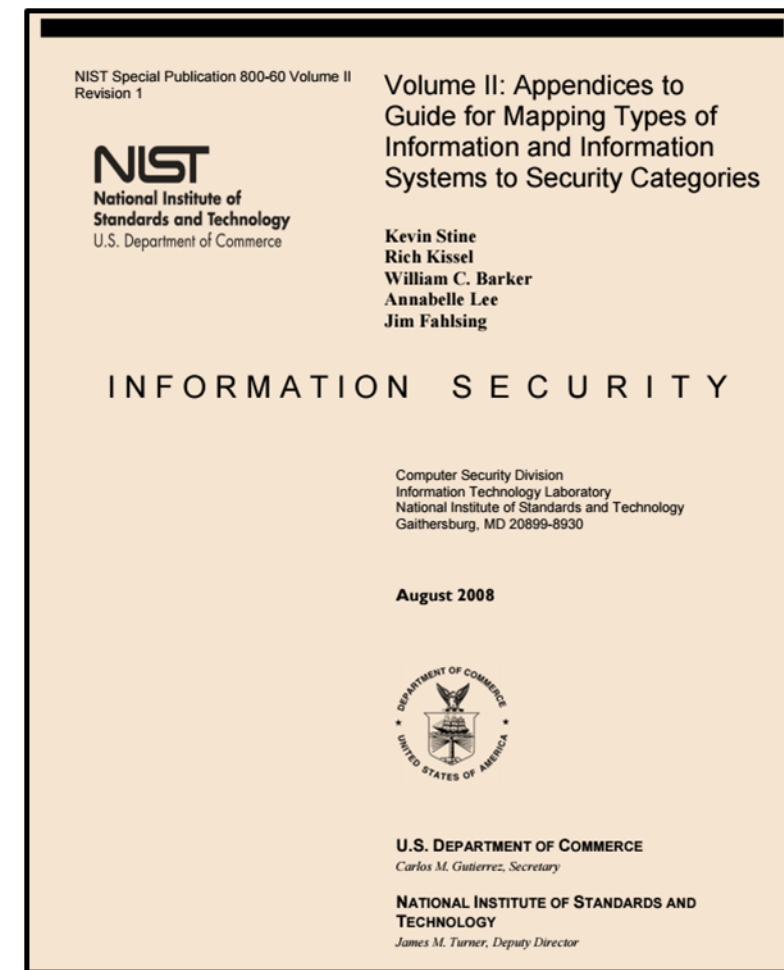
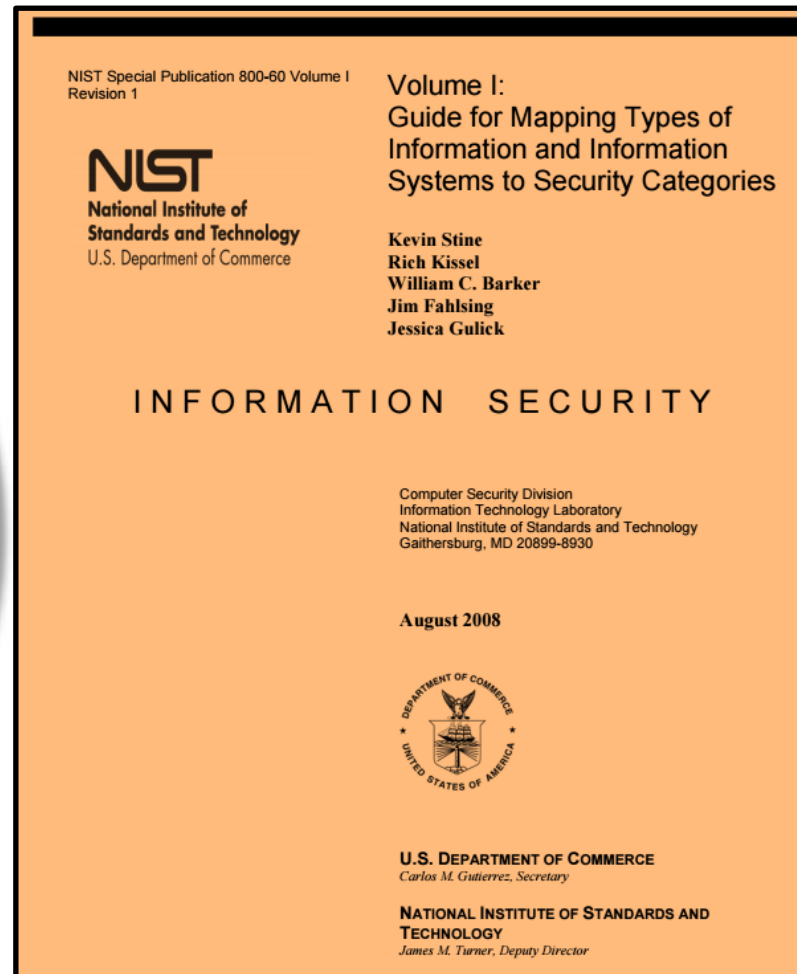
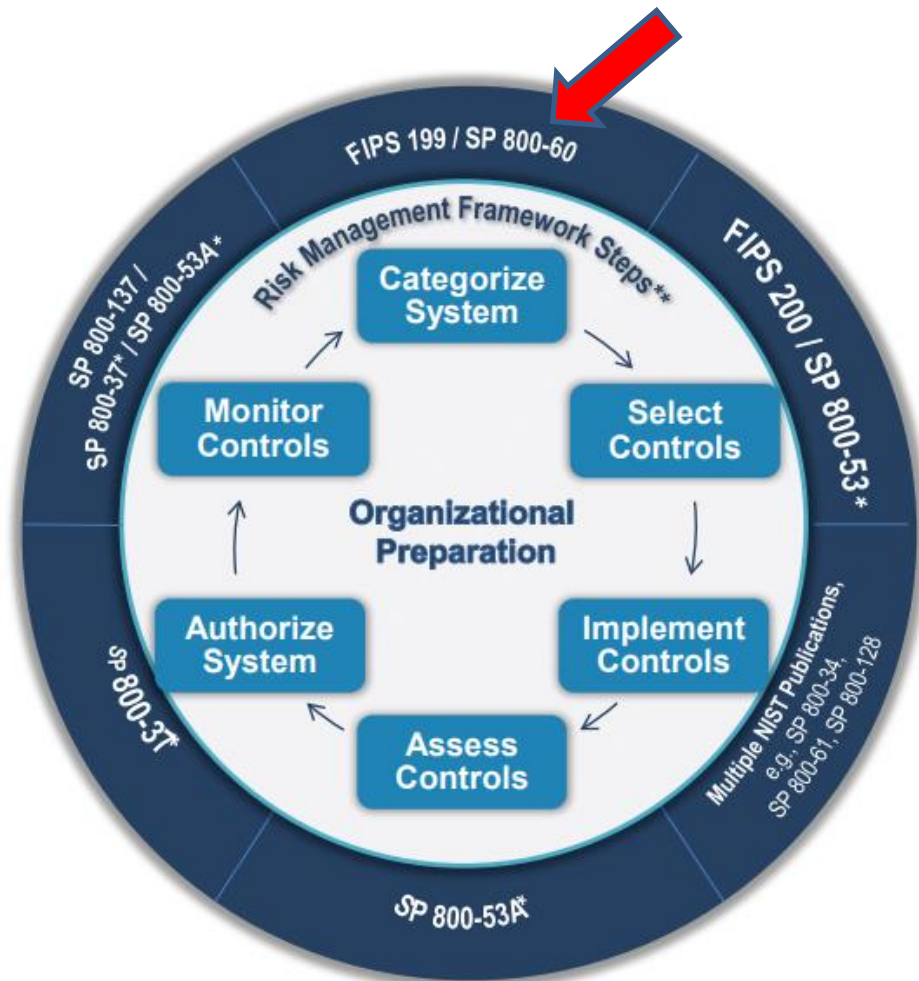
Function	Category Unique Identifier	Category
Identify	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
Protect	PR.AC	Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and 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

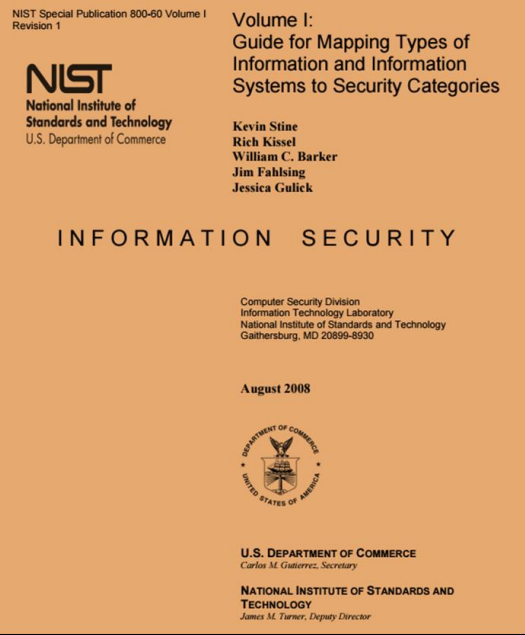
NIST Cybersecurity Framework

# Different views of the NIST Risk Management Framework

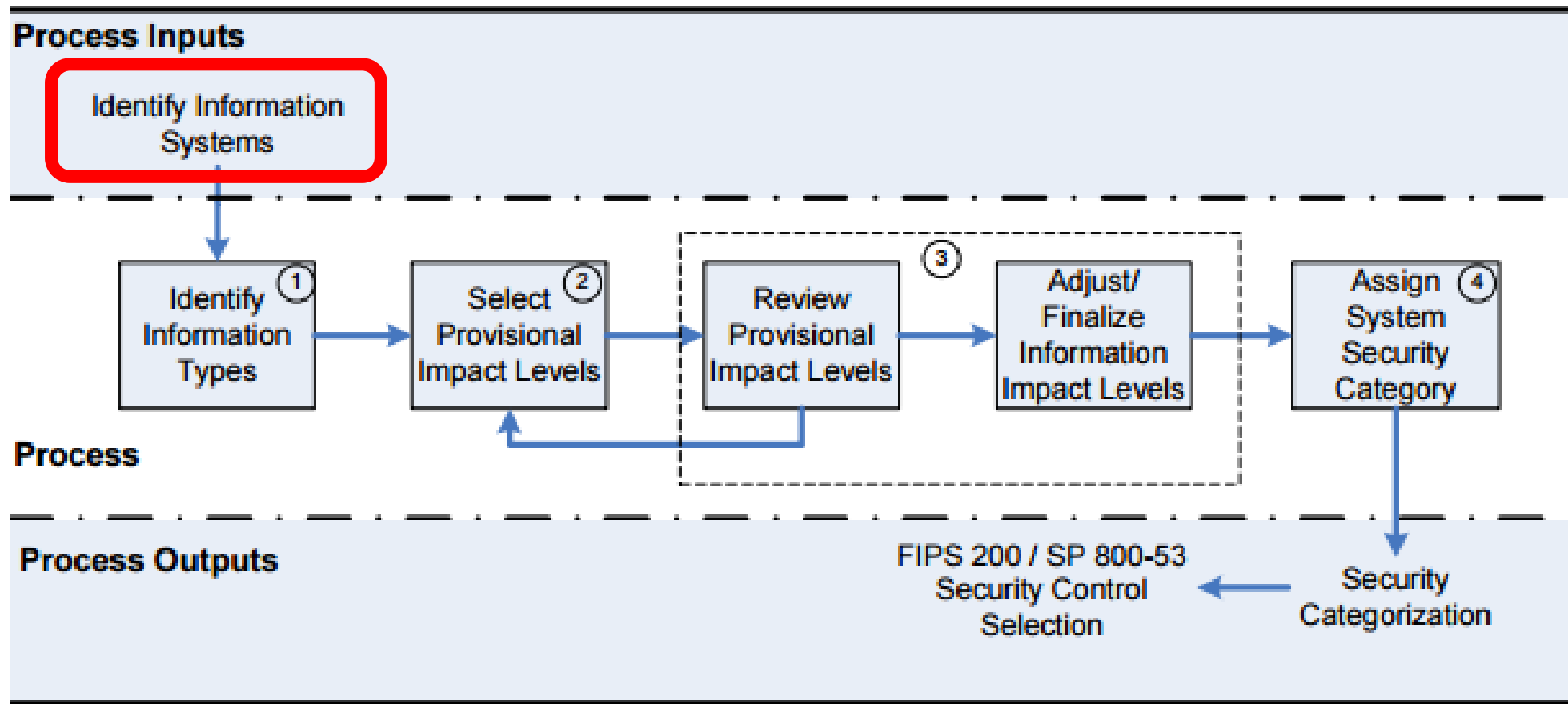


# A systematic qualitative guide for categorizing information and information systems...





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



**Figure 2: SP 800-60 Security Categorization Process Execution**



# 2 Broad types of Information and Information Systems

## 1. Mission-based Information & Information Systems

## 2. Management and Support Information & Information Systems

NIST Special Publication 800-60 Volume I  
Revision 1

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

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

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

INFORMATION SECURITY

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

August 2008



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

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

# Mission-based Information and Information Systems

1. Defense and National Security
2. Homeland Security
3. Intelligence Operations
4. Disaster Management
5. International Affairs and Commerce
6. Natural Resources
7. Energy
8. Environmental Management
9. Economic Development
10. Community and Social Services
11. Transportation
12. Education
13. Workforce Management
14. Health
15. Income Security
16. Law Enforcement
17. Litigation and Judicial Activities
18. Federal Correctional Activities
19. General Sciences and Innovation
20. Knowledge Creation and Management
21. Regulatory Compliance and Enforcement
22. Public Goods Creation and Management
23. Federal Financial Assistance
24. Credit and Insurance
25. Transfers to State/Local Governments
26. Direct Services for Citizens

# Disaster Management Information Types

Table 4: Mission-Based Information

Mission Areas and Information

**D.1 Defense & National Security**

Strategic National & Theater Defense  
Operational Defense  
Tactical Defense

**D.2 Homeland Security**

Border and Transportation Security  
Key Asset and Critical Infrastructure Protection  
Catastrophic Defense

*Executive Functions of the Executive Office of the President (EOP)*

**D.3 Intelligence Operations**

Intelligence Planning  
Intelligence Collection  
Intelligence Analysis & Production  
Intelligence Dissemination  
Intelligence Processing

**D.4 Disaster Management**

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

**D.5 International Affairs & Commerce**

Foreign Affairs  
International Development and Humanitarian Aid  
Global Trade

**D.6 Natural Resources**

Water Resource Management  
Conservation, Marine and Land Management  
Recreational Resource Management and Tourism  
Agricultural Innovation and Services

**D.7 Energy**

Energy Supply  
Energy Conservation and Efficiency  
Energy Resource Management  
Energy Production

**D.8 Environmental**

Environmental Monitoring  
Forecasting  
Environmental Remediation  
Pollution Prevention and Control

**D.9 Economic Development**

Business and Industry  
Intellectual Property  
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.4 Disaster Management

Disaster Monitoring and Prediction

Disaster Preparedness and Planning

Disaster Repair and Restoration

Emergency Response

**D.16 Law Enforcement**

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

**D.17 Litigation & Judicial Activities**

Judicial Hearings  
Legal Defense  
Legal Investigation  
Legal Prosecution and Litigation  
Resolution Facilitation

**D.18 Federal Correctional Activities**

Criminal Incarceration  
Criminal Rehabilitation

**D.19 General Sciences & Innovation**

Scientific and Technological Research and Innovation  
Space Exploration and Innovation

Mode of Delivery]

**D.24 Credit and Insurance**

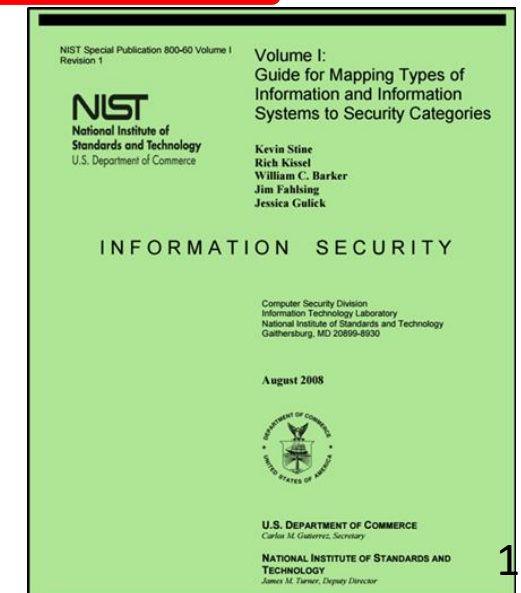
Direct Loans  
Loan Guarantees  
General Insurance

**D.25 Transfers to State/ Local Governments**

Formula Grants  
Project/Competitive Grants  
Earmarked Grants  
State Loans

**D.26 Direct Services for Citizens**

Military Operations  
Civilian Operations



# Disaster Management Information System Example

Levees of The Nation

7,026 Levee Systems 24,731 Miles of Levees 43,985 Levee Structures 57 years Average Levee Age

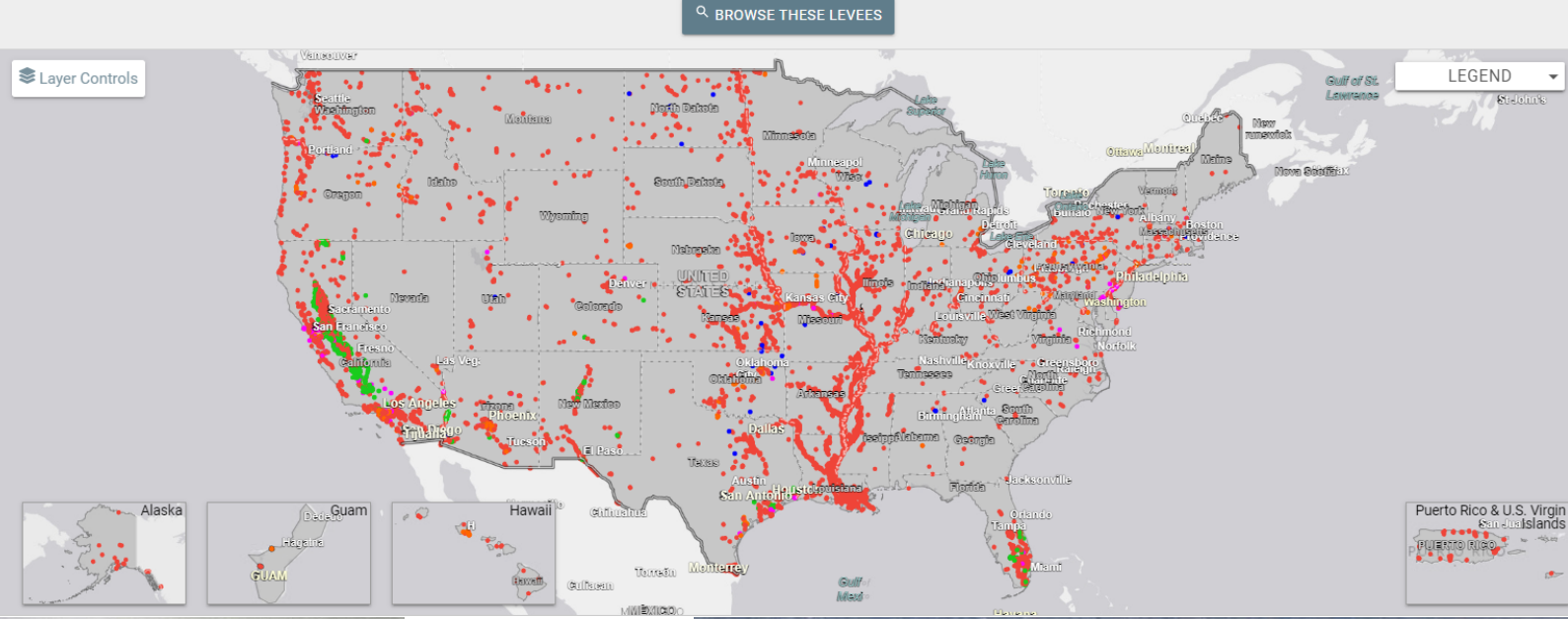
**Geography**  
Spatial Context: Filter to levees that fall within predefined geographical boundaries

**The Nation**  
Click on a state below or on the map to zoom in. You can select other territory types from the drop-down menu.

States and Counties

Q Search this list

- Alabama
- Alaska
- American Samoa
- Arizona
- Arkansas
- California
- Colorado
- Commonwealth of the Northern Mariana Islands
- Connecticut
- Delaware
- District of Columbia
- Florida



[National Levee Database](#)



## 2. Select Provisional Impact Levels for the identified information system

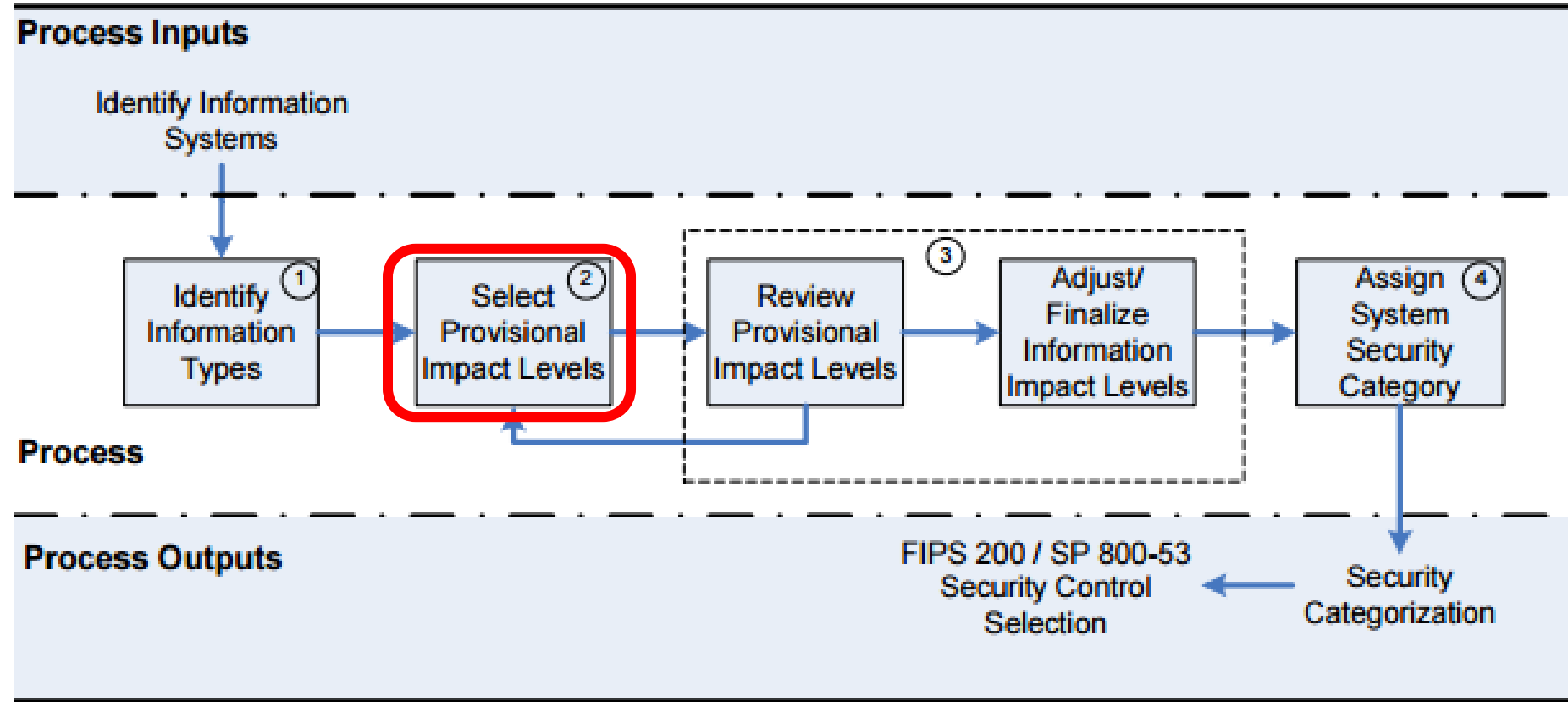


Figure 2: SP 800-60 Security Categorization Process Execution



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

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

INFORMATION SECURITY

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

August 2008



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

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



# Disaster Management Information Types

<b>APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS.....</b>	<b>102</b>
<b>D.1 Defense and National Security .....</b>	<b>107</b>
<b>D.2 Homeland Security.....</b>	<b>108</b>
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
<b>D.3 Intelligence Operations.....</b>	<b>113</b>
<b>D.4 Disaster Management .....</b>	<b>115</b>
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

# 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.

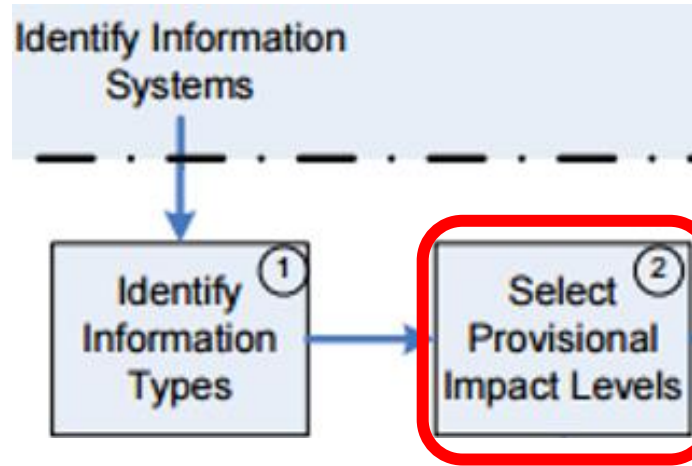
# *A spreadsheet is a useful way to organize datasets to categorize an information system*

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

- [\*NIST SP 800-60 V.2 R1\*](#) is helpful for determining a preliminary impact level categorization of Disaster Information Types



# Disaster Management Information Types



## D.4.1 Disaster Monitoring and Prediction Information Type

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

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

## D.4.2 Disaster Preparedness and Planning Information Type

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

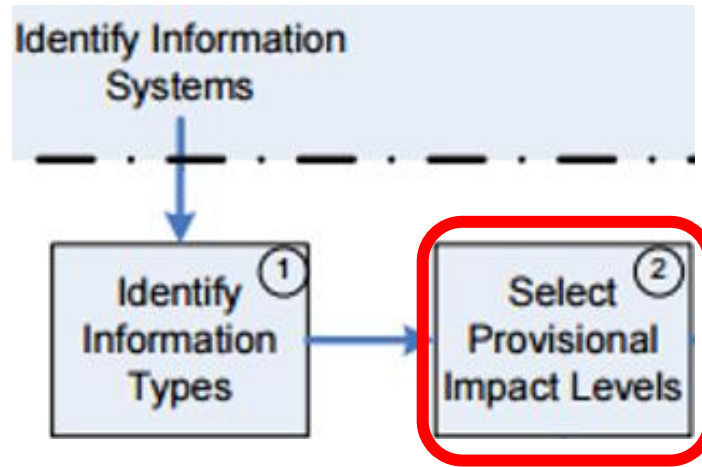
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

## D.4.3 Disaster Repair and Restoration Information Type

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

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

# Disaster Management Information Types



## D.4.4 Emergency Response Information Type

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

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

# Can you recall...

- *How to determine the Summary Impact Levels for the Disaster Information Types*

<b>Disaster Management Information Systems</b>				
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	?

*Can you determine the impact level categorization of an information system based on categorizations of the types of information it contains?*

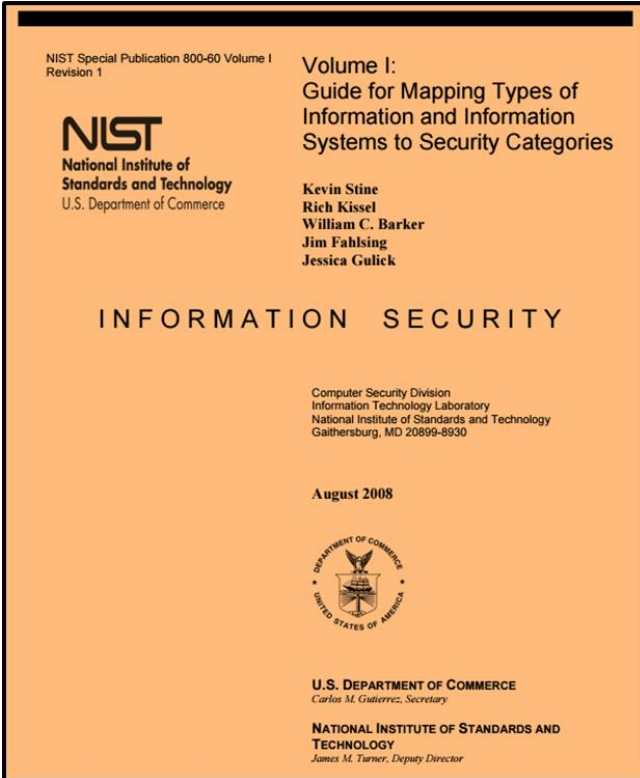
<b>Disaster Management Information Systems</b>				
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	<b>High</b>
Disaster Preparedness and Planning	Low	Low	Low	<b>Low</b>
Disaster Repair and Restoration	Low	Low	Low	<b>Low</b>
Emergency Response Information Type	Low	High	High	<b>High</b>
<b>Information System Impact Ratings:</b>	<b>?</b>	<b>?</b>	<b>?</b>	

# Can you determine the overall security categorization of a Disaster Information System?

<b>Disaster Management Information Systems</b>				
Information Types	Confidentiality	Integrity	Availability	Summary Impact Level
Disaster Monitoring and Prediction	Low	High	High	<b>High</b>
Disaster Preparedness and Planning	Low	Low	Low	<b>Low</b>
Disaster Repair and Restoration	Low	Low	Low	<b>Low</b>
Emergency Response Information Type	Low	High	High	<b>High</b>
<b>Information System Impact Ratings:</b>	Low	High	High	<b>?</b>

# Overall security categorization of a Disaster Information System

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



# Once categorized, select security control baseline for the information system

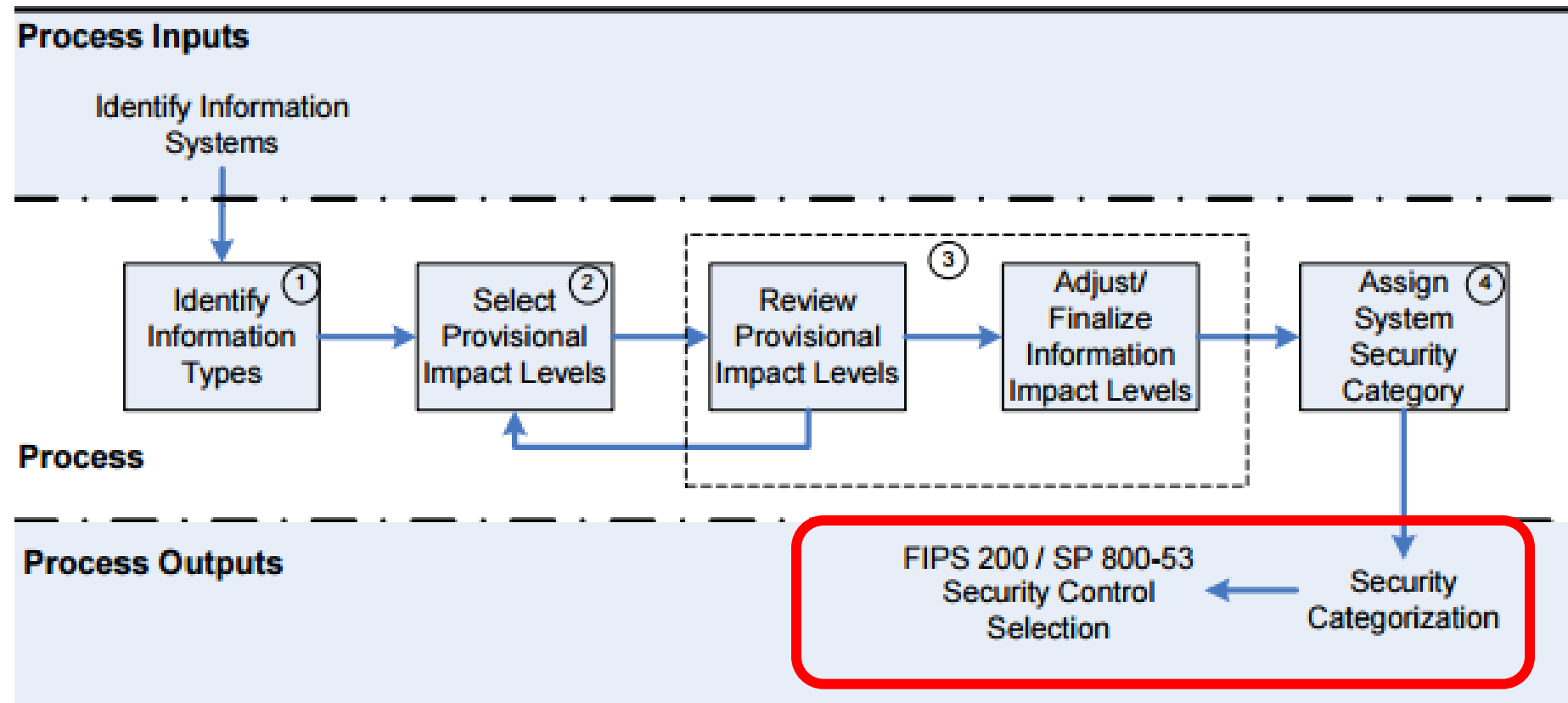
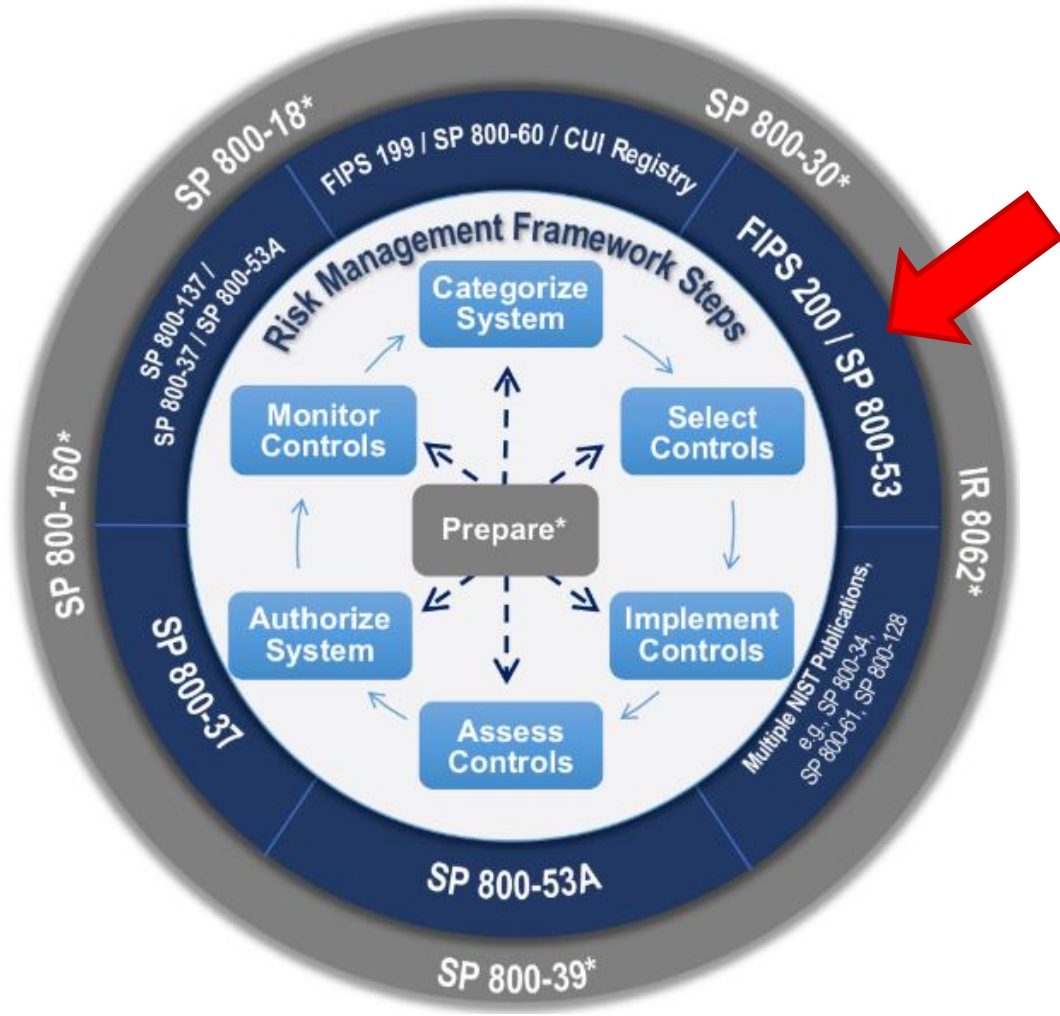


Figure 2: SP 800-60 Security Categorization Process Execution

# 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

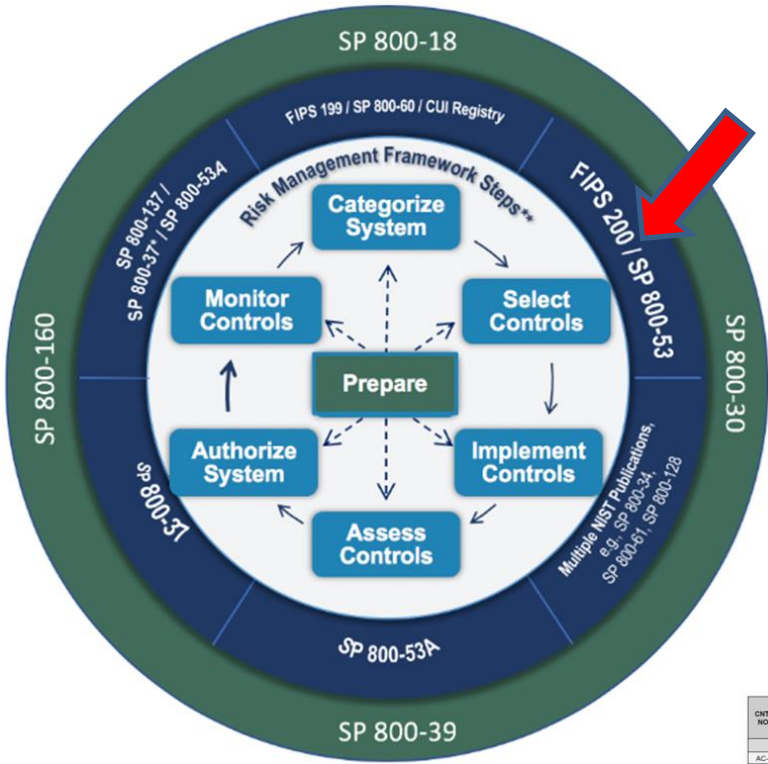
March 2006

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
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-28	Homogeneity	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)(4)	---
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
CM-4	Configuration Settings	P1	CM-4	CM-4 (1)(2)	CM-4 (1)(2)
CM-5	Least Privilege	P1	CM-5	CM-5 (1)(2)(3)(4)(5)	CM-5 (1)(2)(3)(4)(5)
CM-4	Information System Component Inventory	P1	CM-4	CM-4 (1)(2)(3)(4)(5)	CM-4 (1)(2)(3)(4)(5)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
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	---

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)(5)(11)(12)(13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1)(2)(3)(4)(5)(9)(10)	AC-6 (1)(2)(3)(4)(5)(9)(10)
AC-7	Unsuccessful Login Attempts	P1	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Login (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	AC-10	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	Withdrawn	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	Withdrawn	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P0	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)	AC-17 (1)(2)(3)(4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1)(4)(5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (3)	AC-19 (3)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1)(2)	AC-20 (1)(2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
<b>Awareness and Training</b>					
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	---	---	---	---
<b>Audit and Accountability</b>					
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
<b>Security Assessment and Authorization</b>					
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
<b>Configuration Management</b>					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

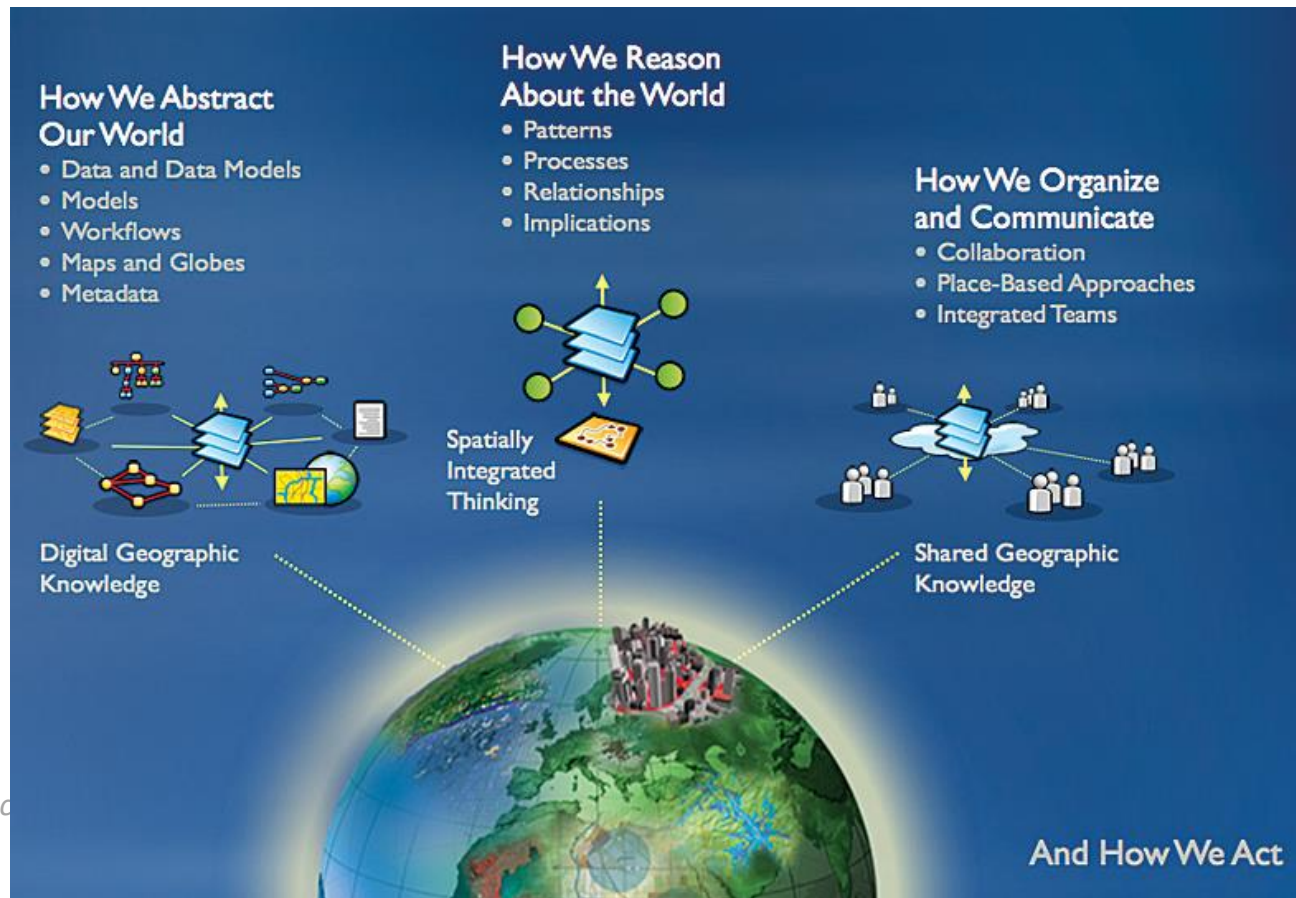
# Agenda

- ✓ In The News
- ✓ Categorizing Information for IT Risk Management
  - Revisit Risk & Controls of Publicly Shared Geographic Information
  - More on Confidentiality: Linked & Linkable PII
  - Risk Evaluation
  - Risk Management Techniques, a brief review
  - Test taking tip
  - Quiz

# Geographic information, for example, is important

Free flow of geographic information between government and public is recognized as essential to the Nation

- ***Informs public for participation in democratic decision making***
- ***Private businesses reuse the public's investment in government information***



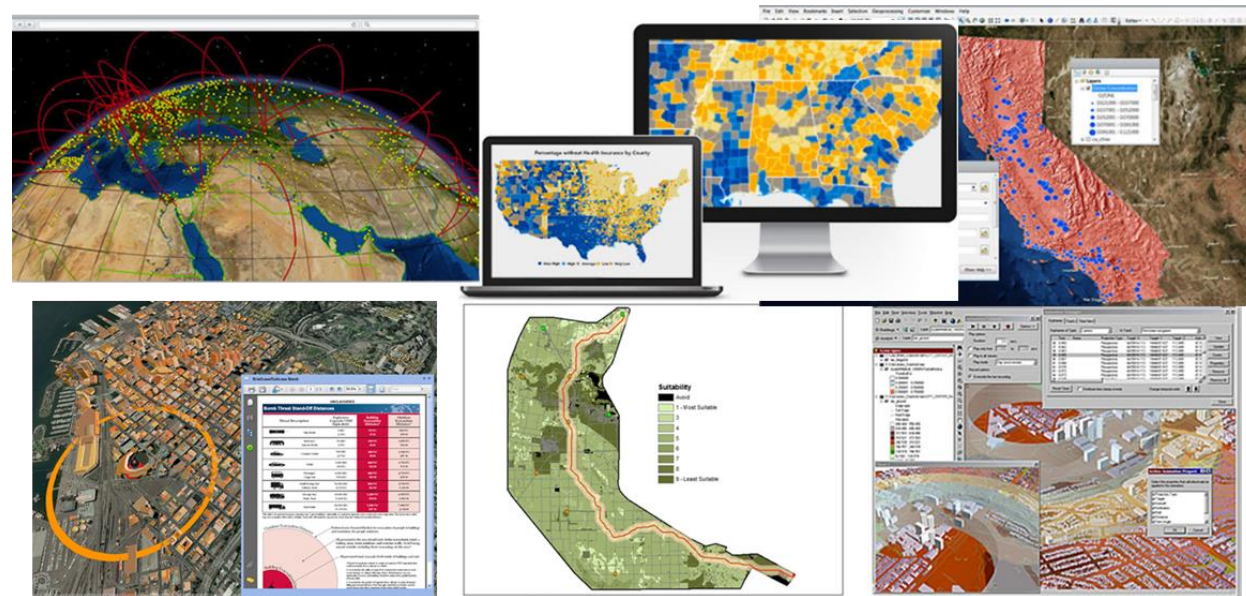
Disseminating public geospatial data is central to the missions of many public, private and non-profit organizations

From ESRI Marketing material

# Geographic data's role in government

*Geographic location is a key element of 80-90% of all governmental data*

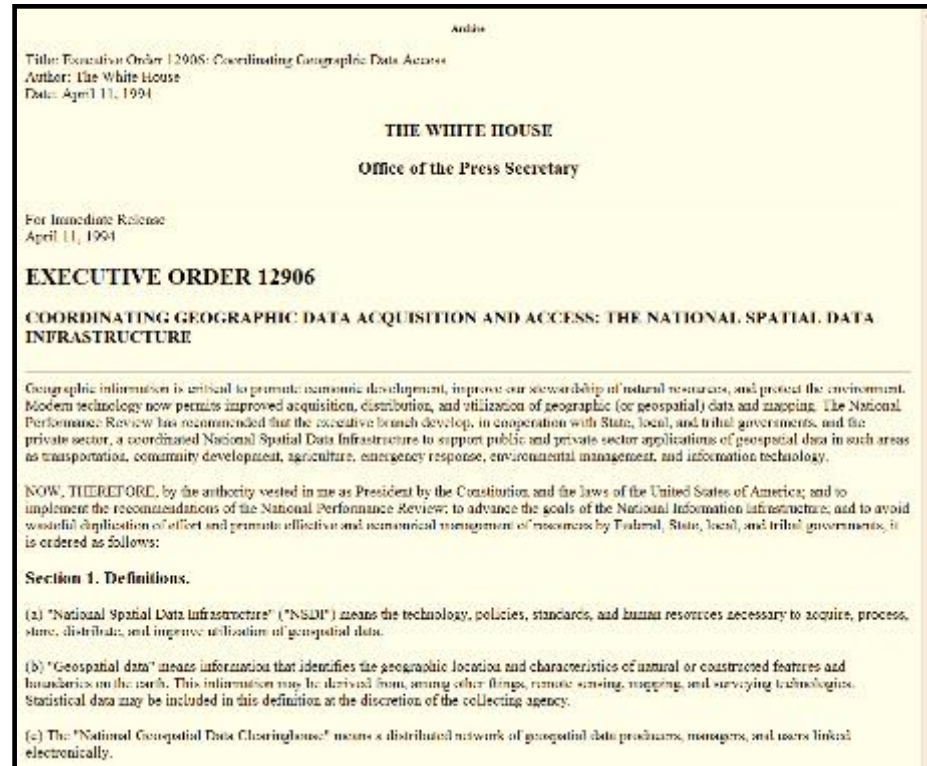
*Data produced with Geographic Information Systems (GIS) are essential to >50% of U.S. domestic economic activities*



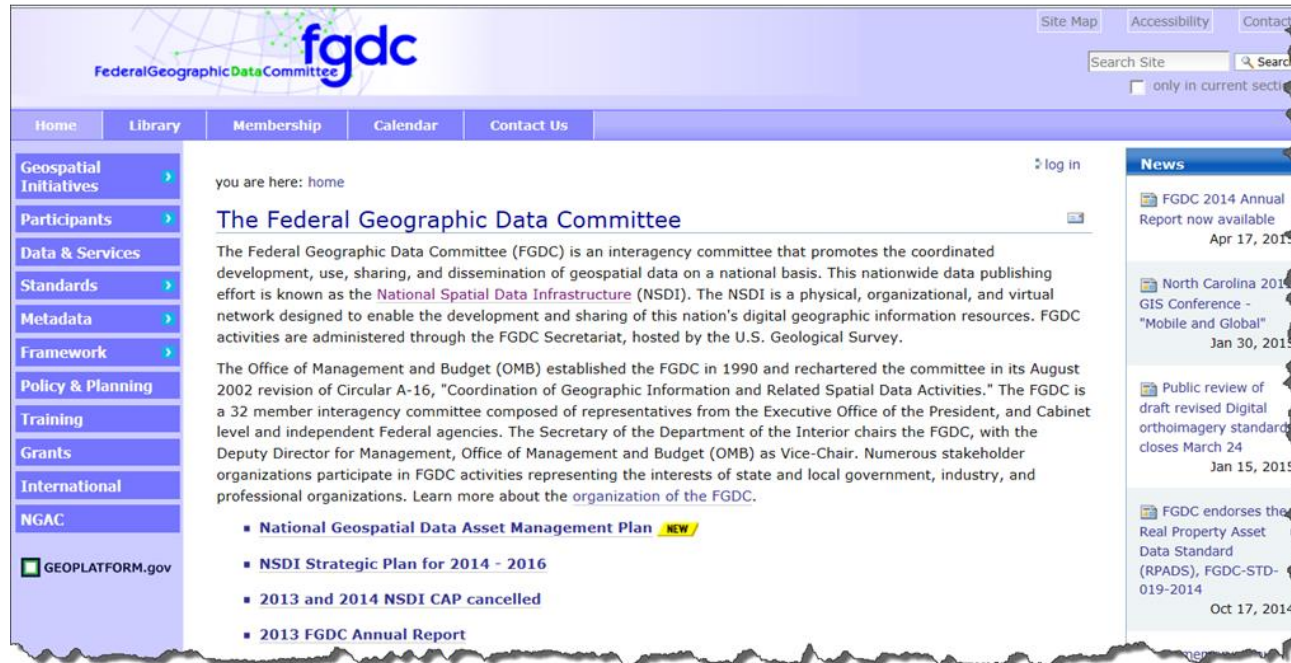
# National Spatial Data Infrastructure

1994 Executive Order instructed Federal Geographic Data Committee (FGDC) to create National Spatial Data Infrastructure (NSDI), and...

- Address \$ billions wasted
  - Redundant collection of undocumented hard to find geospatial data stored in incompatible formats
- Encourage Agencies to stand-up NSDI Clearing House nodes (i.e. websites on Internet)
  - Populated with geospatial data and their descriptive metadata

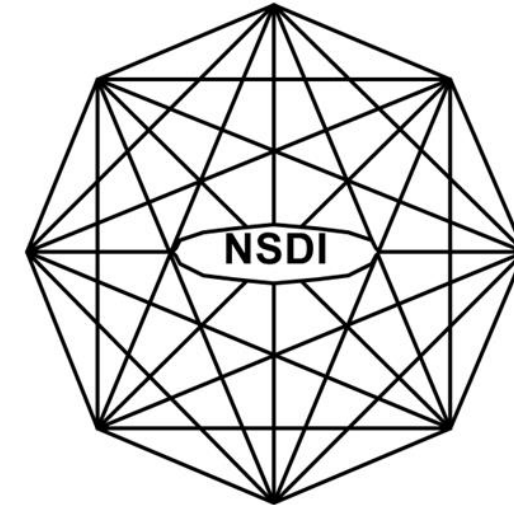


# Public GIS data are shared and distributed via the Internet-based National Spatial Data Infrastructure



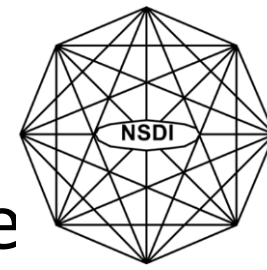
The screenshot shows the FGDC website with the following content:

- Header:** Federal Geographic Data Committee logo, Site Map, Accessibility, Contact, Search Site, and a checkbox for "only in current section".
- Navigation:** Home, Library, Membership, Calendar, Contact Us.
- Left Sidebar:** Geospatial Initiatives, Participants, Data & Services, Standards, Metadata, Framework, Policy & Planning, Training, Grants, International, NGAC, and GEOPLATFORM.gov.
- Main Content:**
  - you are here: home
  - The Federal Geographic Data Committee**
  - Text: "The Federal Geographic Data Committee (FGDC) is an interagency committee that promotes the coordinated development, use, sharing, and dissemination of geospatial data on a national basis. This nationwide data publishing effort is known as the National Spatial Data Infrastructure (NSDI). The NSDI is a physical, organizational, and virtual network designed to enable the development and sharing of this nation's digital geographic information resources. FGDC activities are administered through the FGDC Secretariat, hosted by the U.S. Geological Survey."
  - Text: "The Office of Management and Budget (OMB) established the FGDC in 1990 and rechartered the committee in its August 2002 revision of Circular A-16, 'Coordination of Geographic Information and Related Spatial Data Activities.' The FGDC is a 32 member interagency committee composed of representatives from the Executive Office of the President, and Cabinet level and independent Federal agencies. The Secretary of the Department of the Interior chairs the FGDC, with the Deputy Director for Management, Office of Management and Budget (OMB) as Vice-Chair. Numerous stakeholder organizations participate in FGDC activities representing the interests of state and local government, industry, and professional organizations. Learn more about the organization of the FGDC."
  - News List:**
    - National Geospatial Data Asset Management Plan **NEW**
    - NSDI Strategic Plan for 2014 - 2016
    - 2013 and 2014 NSDI CAP cancelled
    - 2013 FGDC Annual Report
- Right Sidebar:** News
  - FGDC 2014 Annual Report now available (Apr 17, 2015)
  - North Carolina 2015 GIS Conference - "Mobile and Global" (Jan 30, 2015)
  - Public review of draft revised Digital orthoimagery standards closes March 24 (Jan 15, 2015)
  - FGDC endorses the Real Property Asset Data Standard (RPADS), FGDC-STD-019-2014 (Oct 17, 2014)

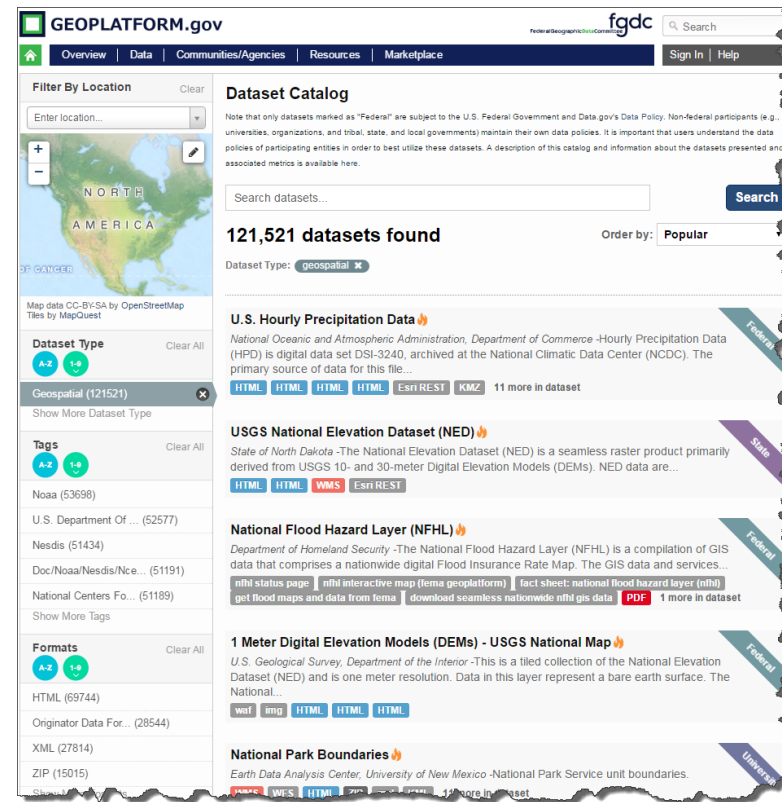
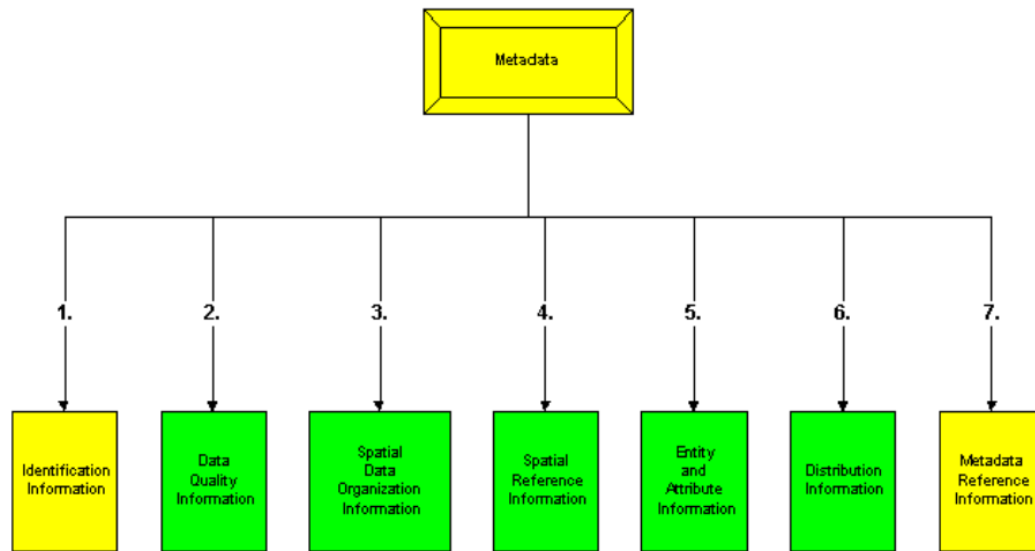


National Spatial Data Infrastructure

# National Spatial Data Infrastructure



Provides a searchable metadata-enabled online clearinghouse for finding, downloading and resusing GIS datasets



# NSDI: A data source for terrorists?

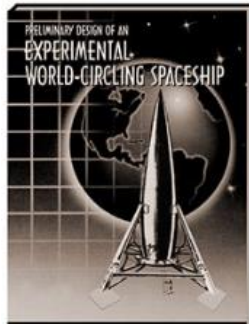
After attacks on USS Cole in 2000 and the 9/11/2001 attacks, attention focused again on protecting critical infrastructure U.S. advisories might seek to attack

*...GIS data made available through NSDI websites became **recognized as at risk of being exploited by those seeking to attack U.S. major cities and critical infrastructure***





# RAND Corporation...



1946

## The First Satellite Design

More than 11 years before *Sputnik*, RAND released its first report while still at Douglas Aircraft, *Preliminary Design of an Experimental World-Circling Spaceship*. At the time, it was the most comprehensive engineering study of the nuts-and-bolts realities of a satellite spacecraft.



1948

## The JOHNNIAC

When the need for solutions to complex analytic studies outstripped the computing power of the time, RAND decided to build its own computer. Named after mathematician John von Neumann, the JOHNNIAC was one of the first mainframe computers with stored memory.



1954

## Selection and Use of Strategic Air Bases

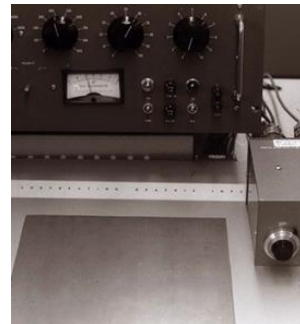
The report by a team led by Albert Wohlstetter shook the foundation of nuclear deterrence policy by shifting the United States from a first-strike to a second-strike posture. It suggested placing air bases closer to the United States and relying on long-range bombers and aerial refueling aircraft, eventually saving the Air Force billions of dollars.



1957

## Artificial Intelligence

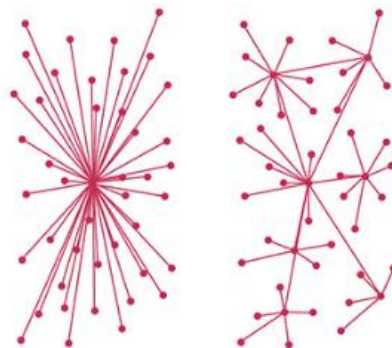
The first successful Artificial Intelligence program that used Information Processing Languages (IPLs) was developed in RAND's Systems Research Laboratory. IPLs were the precursors of popular contemporary languages such as LISP.



1961

## The RAND Tablet

The tablet was one of the first devices permitting the input of handwritten text and freehand drawings into a computer. While limited in its capabilities and far too expensive for commercial use, the RAND Tablet nonetheless showed the way for PalmPilots, Tablet PCs, and iPads.



1962

## Packet Switching: Seed of the Internet

Paul Baran developed a plan for a communication network that would withstand a nuclear attack. This notion of distributed communications, or packet switching, eventually became the foundation of the Internet.



1974

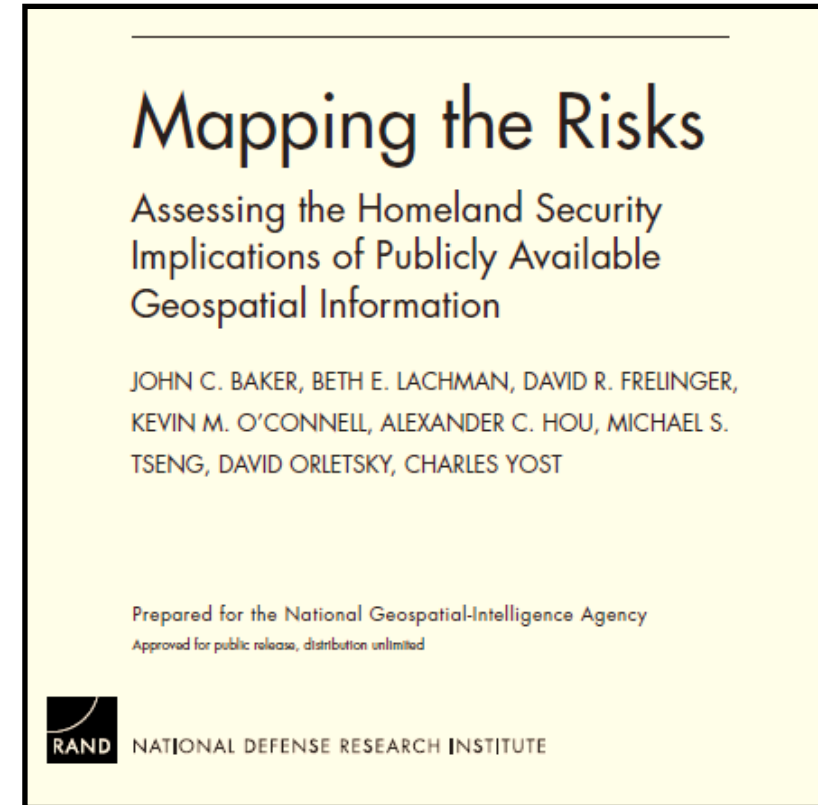
## Improving Computer Security

RAND's expertise in defense-related computer security issues was extended to the private sector during the 1970s. Willis Ware chaired a government committee that studied the problems arising from the application of computer technology to record keeping about people. This work guided the DoD computer configurations and eventually became the foundation of the Federal Privacy Act of 1974.

# Risks from public geospatial information

In 2003, Director of U.S. National Imagery and Mapping Agency asked RAND Corporation for a:

*Framework to “guide public and private decision makers in weighing homeland security implications related to release of geospatial information”*



*Today the National Imagery and Mapping Agency is called the National Geospatial-Intelligence Agency*

# Risks from public geospatial information

RAND's 2004 deliverable included a survey and analysis of

- 465 programs/offices/initiatives at 30 agencies and departments identified as providing geospatial information to the public
  - 628 public datasets sampled from NSDI Clearinghouse websites
  - 37 (~6%) found to be useful in helping an attacker select a target or plan an attack against a site
    - None were considered so critical that an “attacker could not perform the attack without” them
  
- Conclusions
  - Publically available geospatial “information needed for identifying and locating potential targets is widely accessible”
  - “...detailed and up-to-date information required for attack planning against a particular target is much less readily available”

# RAND's assessment of risks posed by GIS data shared publically over the Internet is focused by 3 "filters"

## Framework for Analyzing the Homeland Security Sensitivity of Geospatial Data and Information Sources

Filter	Key Questions for Decisionmakers
Usefulness	<ul style="list-style-type: none"><li>• Is the information useful for target selection or location purposes?</li><li>• Is the information useful for attack planning purposes?</li></ul>
Uniqueness	<ul style="list-style-type: none"><li>• Is the information readily available from other geospatial information sources?</li><li>• Is the information available from direct observation or other nongeospatial information types?</li></ul>
Societal benefits and costs	<ul style="list-style-type: none"><li>• What are the expected security benefits of restricting public access to the source?</li><li>• What are the expected societal costs of restricting public access to the source?</li></ul>

# Federal Geographic Data Committee's risk assessment and control guidelines for...

- Identifying sensitive information contents of geospatial data that pose a risk to security
- Making information security decisions and applying safeguards to sensitive geospatial data contents

*“Does knowledge of the location and purpose of a feature as described in the data, have the potential to significantly compromise the security of persons, property, or systems?”*

FGDC 2005, based on RAND's 2004 study




FIG 1  
June 2005

## Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

**What is the purpose of the guidelines?**  
Many public, private, and non-profit organizations originate and publicly disseminate geospatial data. Dissemination is essential to the missions of many organizations and the majority of these data are appropriate for public release. However, a small portion of these data could pose risks to security and may therefore require safeguarding. Although there is not much publicly available geospatial information that is sensitive (Baker and others, 2004, page 123), managers of geospatial information have safeguarded information using different decision procedures and criteria.

The guidelines provide standard procedures to:

1. Identify sensitive information content of geospatial data that pose a risk to security.
2. Review decisions about sensitive information content during reassessments of safeguards on geospatial data.

Additionally, the guidelines provide a method for balancing security risks and the benefits of geospatial data dissemination. If safeguarding is justified, the guidelines help organizations select appropriate risk-based safeguards that provide access to geospatial data and still protect sensitive information content.

The guidelines do not grant any new authority and are to be carried out within existing authorities available to organizations. They apply to geospatial data irrespective of the means of data access or delivery method, or the format.

**How are the guidelines organized?**  
The guidelines provide a procedure consisting of a sequence of decisions (see Figure 1) that an originating organization should make about geospatial data. Each decision is accompanied by related instructions and discussion.

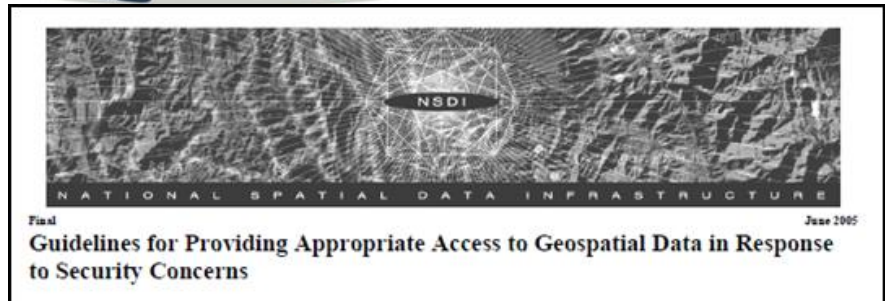
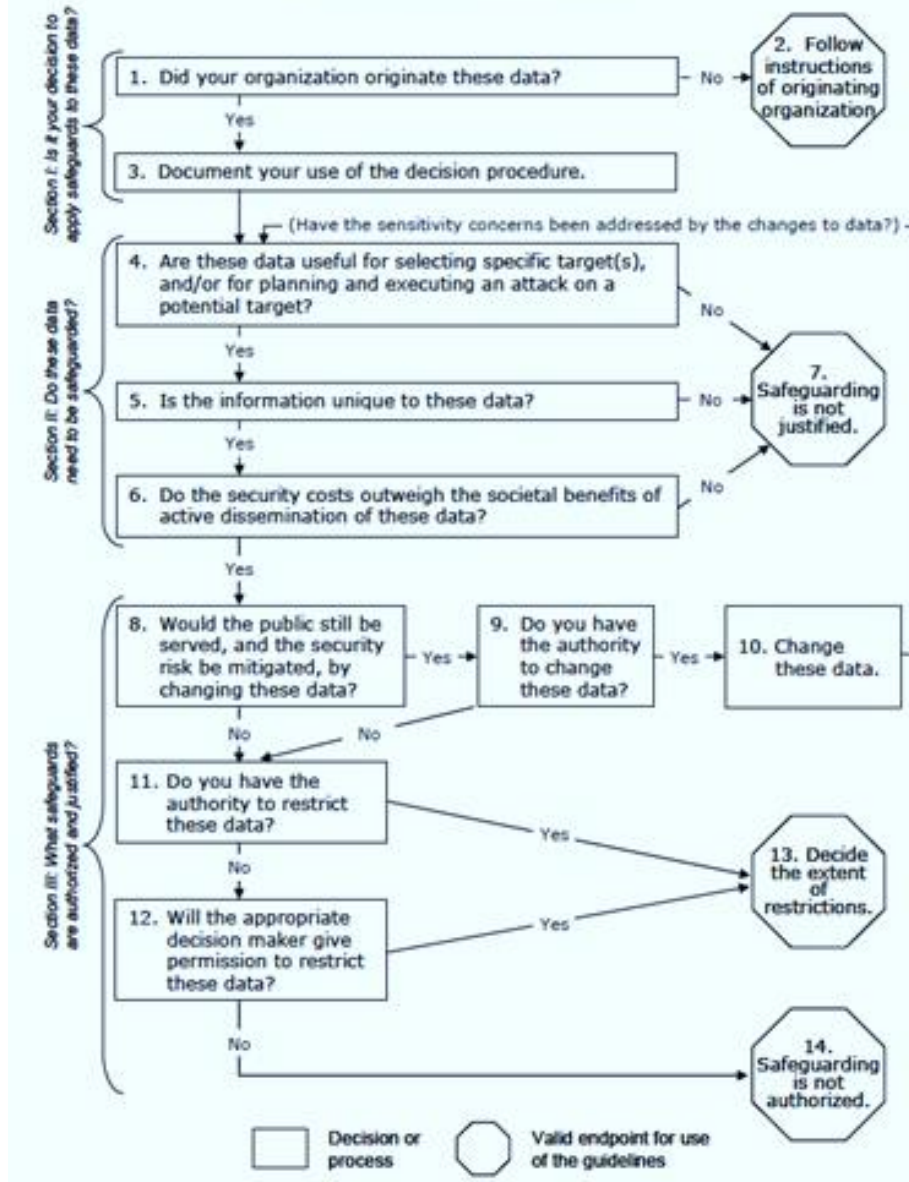
The decision sequence is organized using the following rationale:

- I. Do the geospatial data originate in the organization? If not, the organization is instructed to follow the instructions related to safeguarding that accompany the data.
- II. If the geospatial data originate in the organization, do the data need to be safeguarded? This decision is based on three factors:
  - **Risk to security:** Are the data useful for selecting one or more specific potential targets, and/or for planning and executing an attack on a potential target?
  - **Uniqueness of information:** If the data contain information that pose a security risk, is this sensitive information difficult to observe and not available from open sources?
  - **Net benefit of disseminating data:** If the sensitive information poses a risk to security and is unique to the geospatial data, do the security costs of disseminating the data outweigh the societal benefits of data dissemination?Safeguarding is justified only for data that contain sensitive information, that are the unique source of the sensitive information, and for which the security risk outweighs the societal benefit of dissemination.
- III. If the data need to be safeguarded, what safeguards are justified? The guidelines offer two options:
  - **Change the data:** Change the data to remove or modify the sensitive information and then make the changed data available without further safeguards. Organizations are advised to review the changed data to ensure that the change(s) dealt effectively with the security concern.

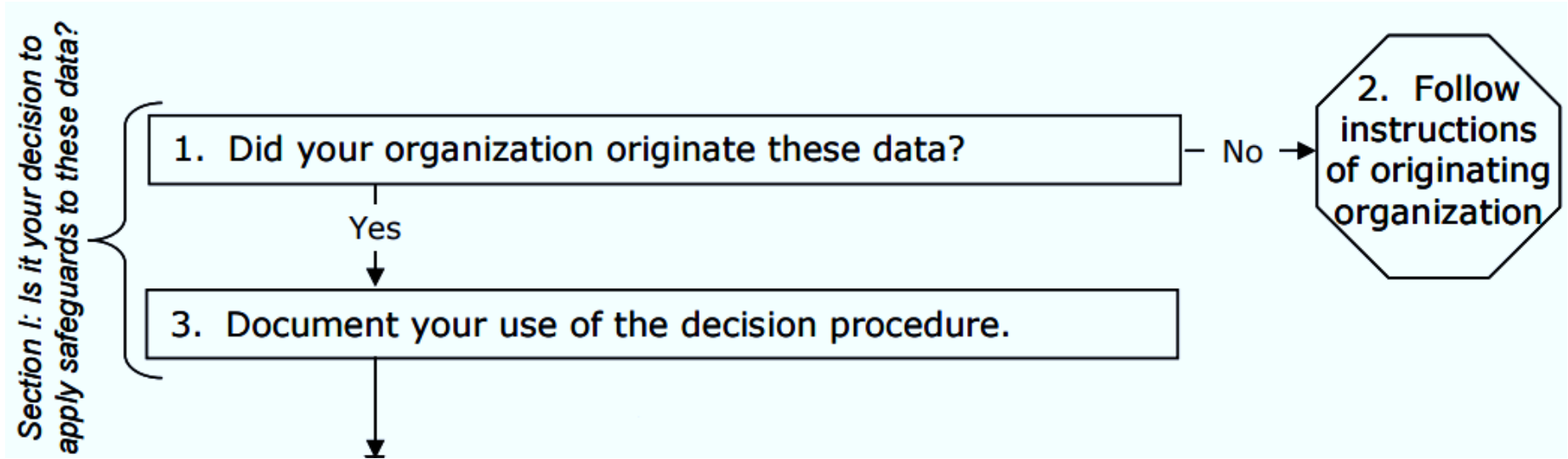
FEDERAL GEOGRAPHIC DATA COMMITTEE  
U.S. GEOLOGICAL SURVEY, 950 NATIONAL CENTER  
RESTON, VIRGINIA 20192  
<http://www.fgdc.gov>

PHONE: 703-648-3314  
FAX: 703-648-7755  
EMAIL: [fgdc@fgdc.gov](mailto:fgdc@fgdc.gov)

Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns



# Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns



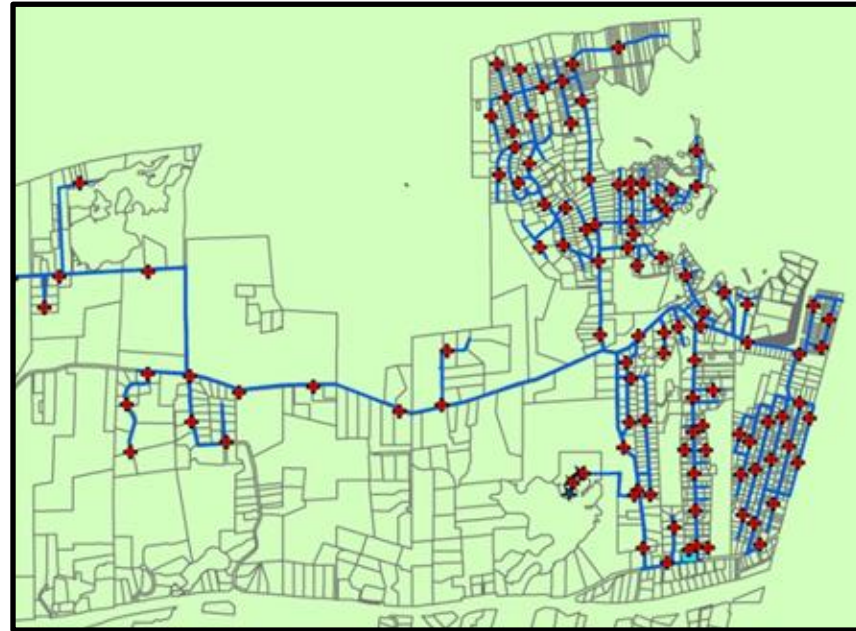
## *...risk assessment...*



4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

*“Sensitivity” of geospatial data is based on usefulness to terrorists*

*Do the data show “choke points to increase effectiveness of an attack ?”*





# ...risk assessment...



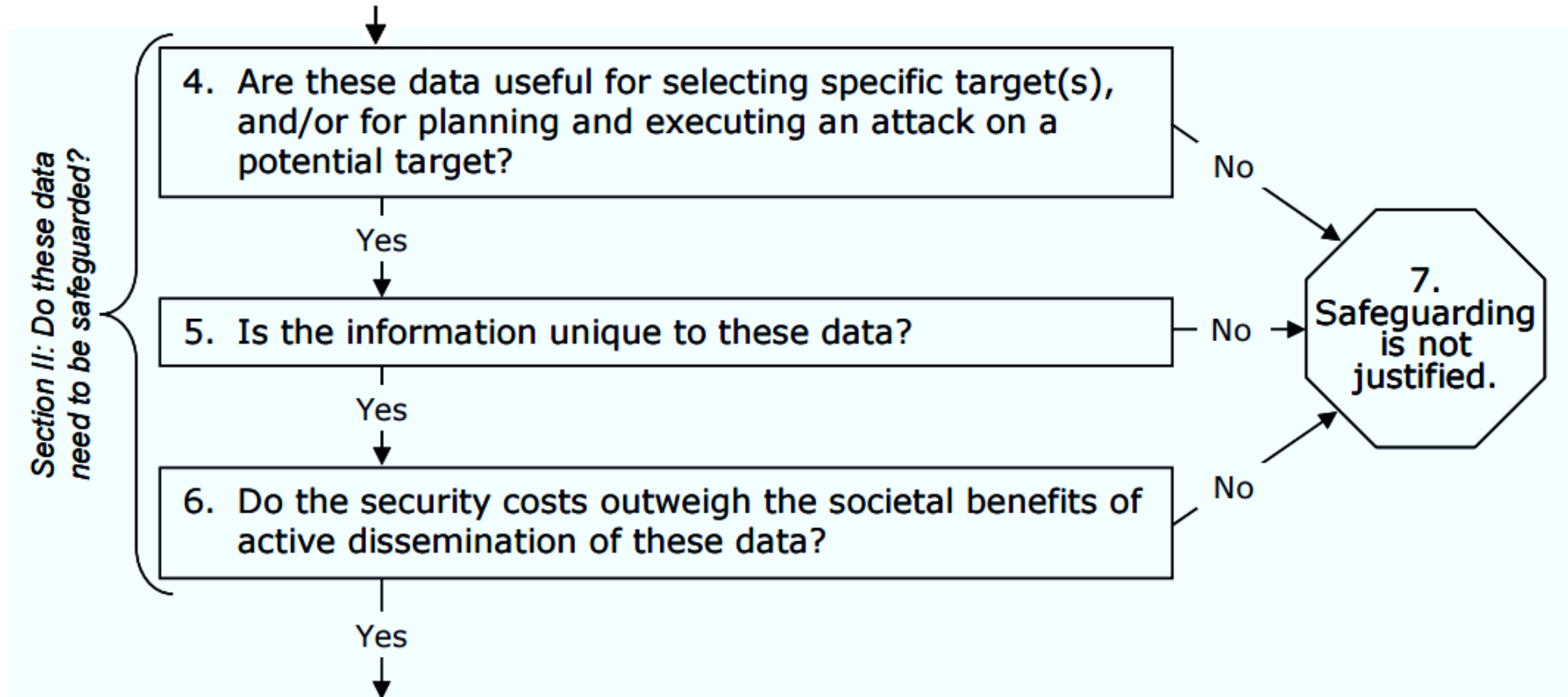
4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

*“Sensitivity” of geospatial data is based on usefulness to terrorists*

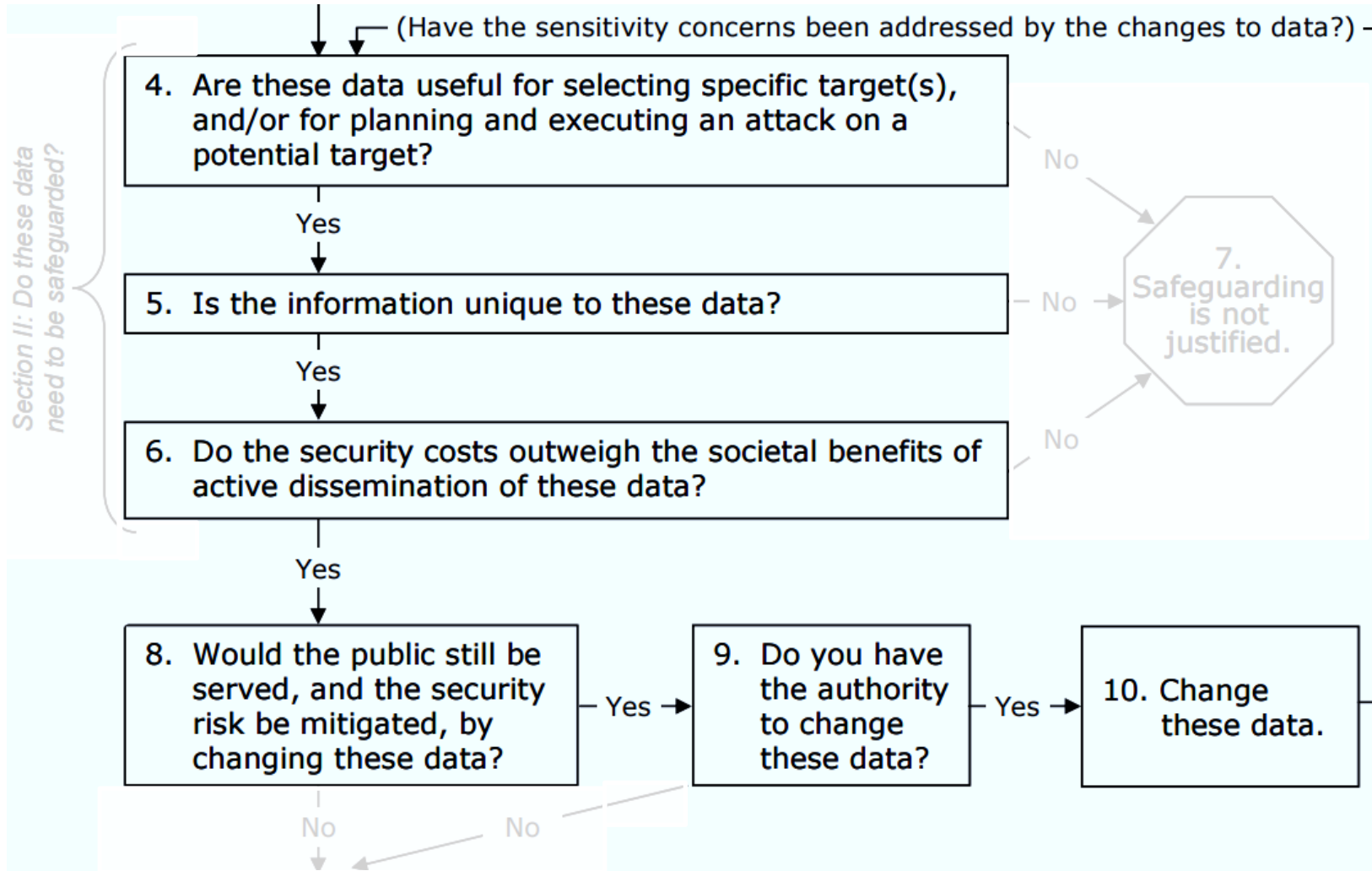
*Do the data “provide relevant current (real-time, near real-time, or very recent) security-related data” that can help an attacker “find the best way to cause catastrophic failure?”*



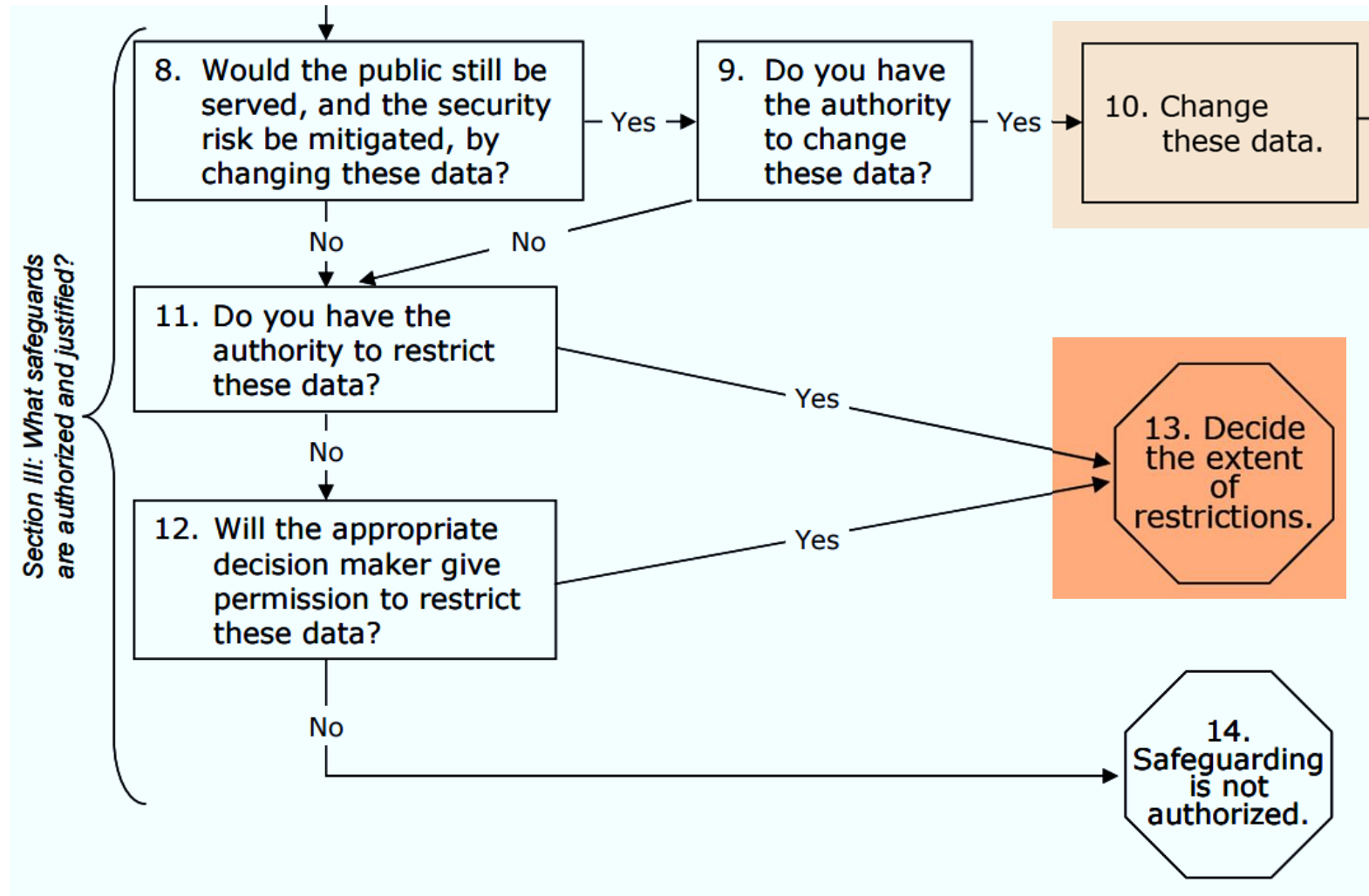
# Assess the risk...



# ...control/mitigate the risk...



# *...control/mitigate the confidentiality risk...*

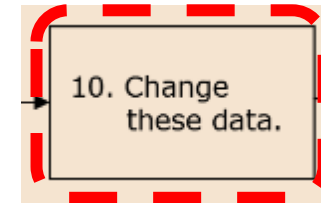


## *...control/mitigate the risk...*

If security risks outweigh benefits of releasing the data to the public, agency can choose to safeguard data by:

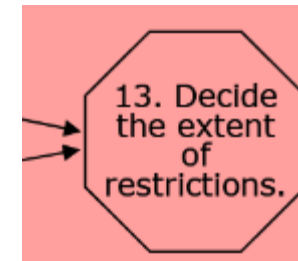
- **Modifying data**

- Remove or reduce detail in offending data elements
  - either in the attributes, spatial representations, or both



- **Restricting access to data**

- If agency lacks authority to change data, or believes modifying data will undermine its value to the public, then agency can restrict access



# *...control/mitigate risk...*

10. Change these data.

To remove or reduce detail in offending data elements apply techniques of **Cartographic Generalization**

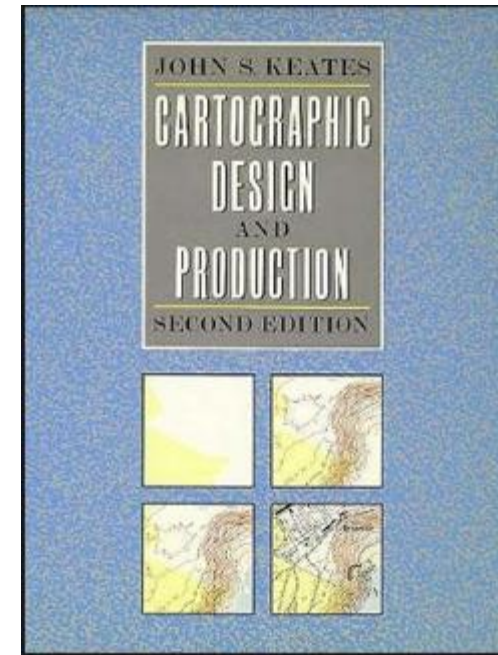


*Before...*



*...after*

1. *Selective Omission*
2. *Simplification*
3. *Combination*
4. *Exaggeration*
5. *Displacement*



# FIPS 199's and FGDC Guidelines' share a mutual security objective...

## **Confidentiality**

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.



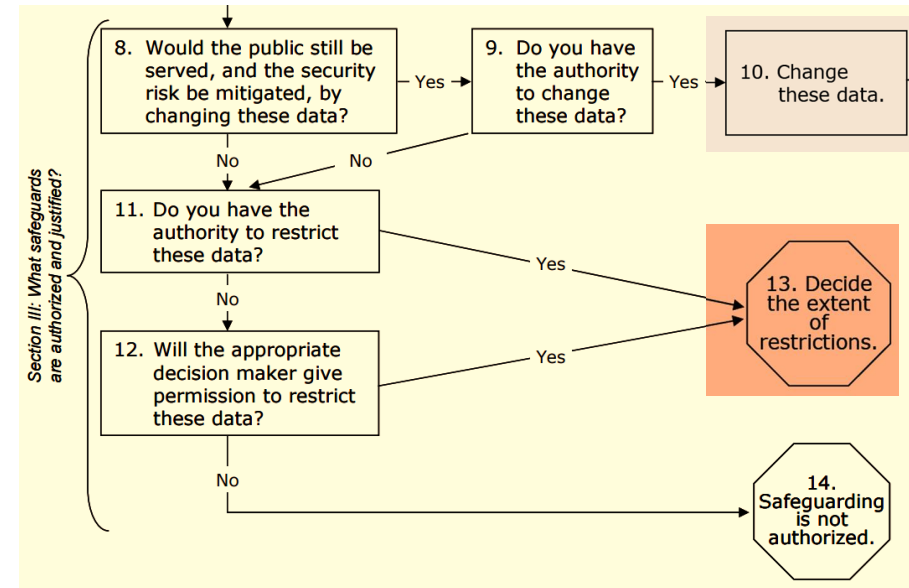
**FGDC Guidelines' security objective**

## **Integrity**

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

## **Availability**

Ensuring timely and reliable access to and use of information.




*What FIPS 199 security objectives are at risk by implementing the FGDC's Guidelines ?*

# Metadata enables communicating data classification information

2 examples of metadata standards that include security categorization information for geographic datasets



FGDC-STD-001-1998



National Spatial Data Infrastructure

Content Standard for Digital Geospatial Metadata

Metadata Ad Hoc Working Group  
Federal Geographic Data Committee

Federal Geographic Data Committee  
Department of Agriculture • Department of Commerce • Department of Defense • Department of Energy  
Department of Housing and Urban Development • Department of the Interior • Department of State  
Department of Transportation • Environmental Protection Agency  
Federal Emergency Management Agency • Library of Congress  
National Aeronautics and Space Administration • National Archives and Records Administration  
Tennessee Valley Authority

EUROPEAN STANDARD **EN ISO 19115-1**  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

April 2014

ICS 35.240.70 Supersedes EN ISO 19115:2005

English Version  
Geographic information —  
Metadata —  
Part 1: Fundamentals  
(ISO 19115-1:2014)

Information géographique —  
Métadonnées —  
Partie 1: Principes de base  
(ISO 19115-1:2014)


Geoinformation —  
Metadaten —  
Teil 1: Grundsätze  
(ISO 19115-1:2014)

This European Standard was approved by CEN on 22 February 2014.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN/CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN/CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

© 2014 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members. Ref. No. EN ISO 19115-1:2014 E



# Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

*Section 1: Is it your decision to apply safeguards to these data?*

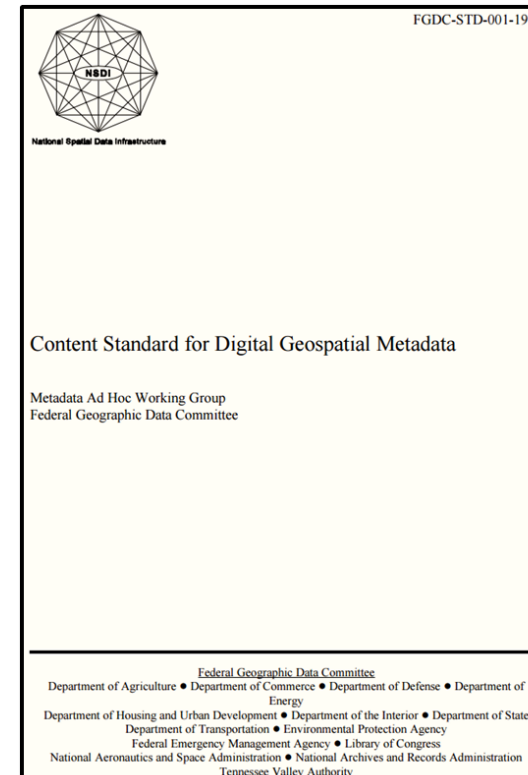
1. Did your organization originate these data?

No

2. Follow instructions of originating organization

Yes

3. Document your use of the decision procedure.



### Appendix 2: Documenting Use of the Guidelines in Metadata Accompanying Geospatial Data

This appendix identifies data elements in the "Content Standard for Digital Geospatial Metadata" (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were

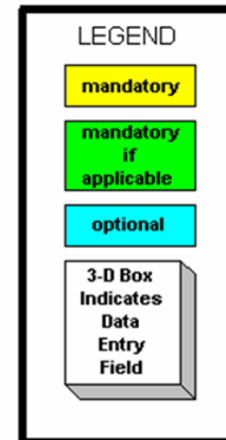
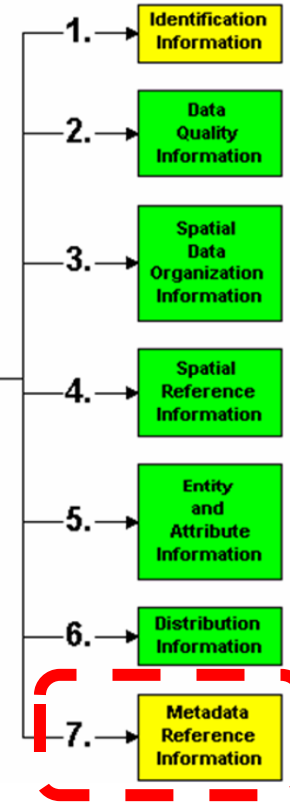
If your organization has a formal classification system you also can report the classification level of the geospatial data by category under "Security Information" (element 1.12).

Geospatial metadata can also be subject to safeguarding. To document the details of restrictions on access, use, or dissemination of the metadata:

- Report restrictions on access to the geospatial metadata under "Metadata Access Constraints" (element 7.8).
- Report restrictions on use or dissemination of the metadata.

### 3. Document your use of the decision procedure.

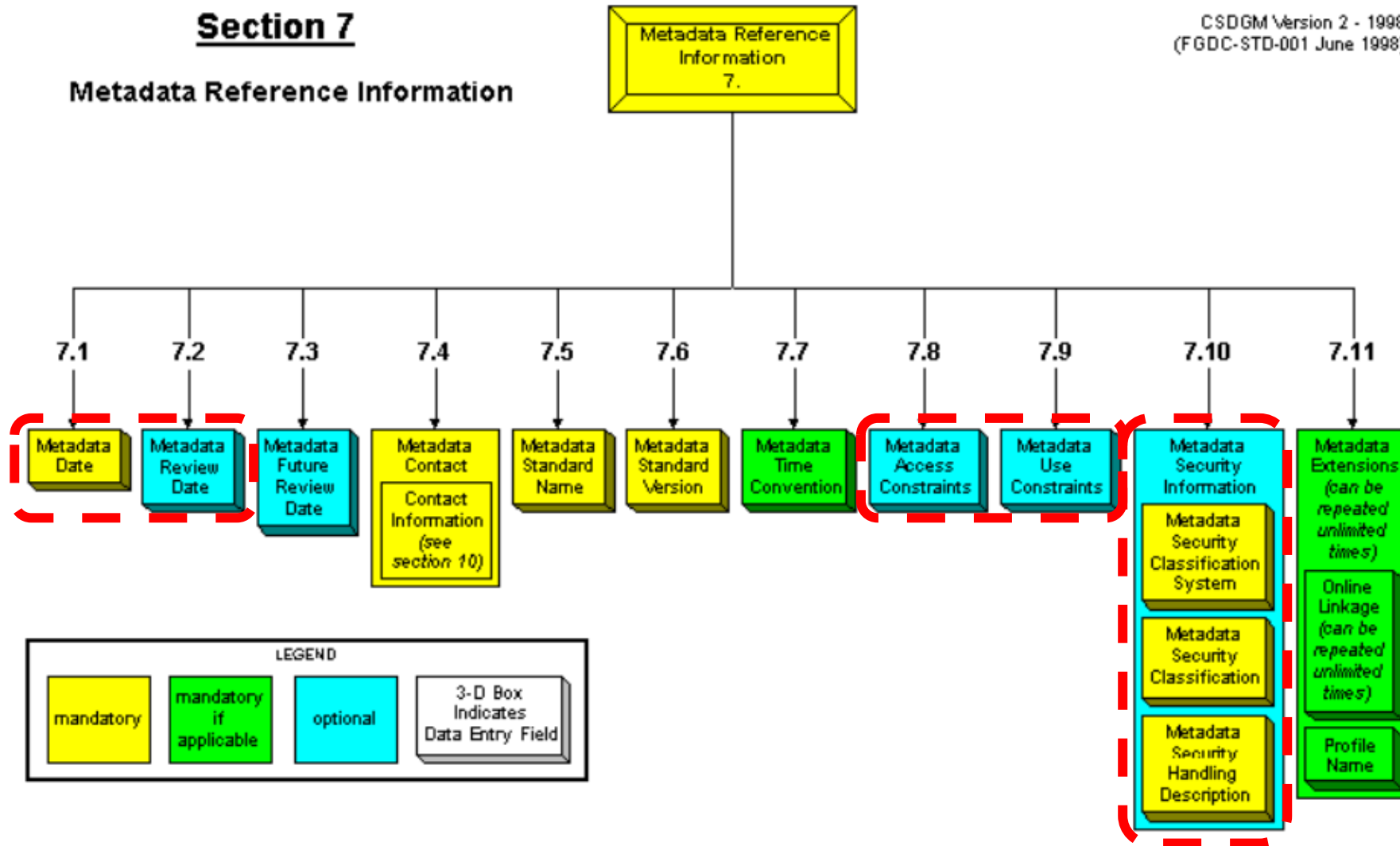
Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

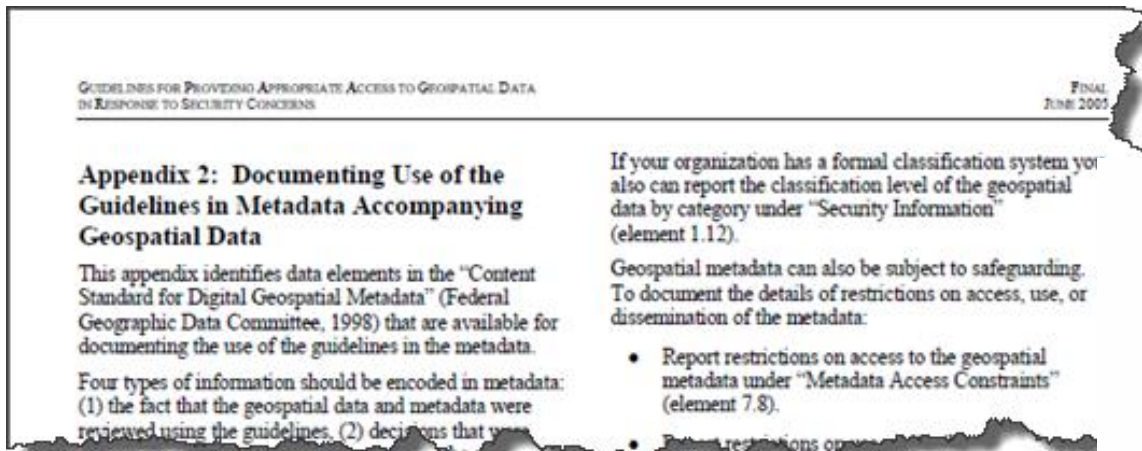


## Section 7

### Metadata Reference Information

CSDGM Version 2 - 1998  
(FGDC-STD-001 June 1998)





3. Document your use of the decision procedure.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

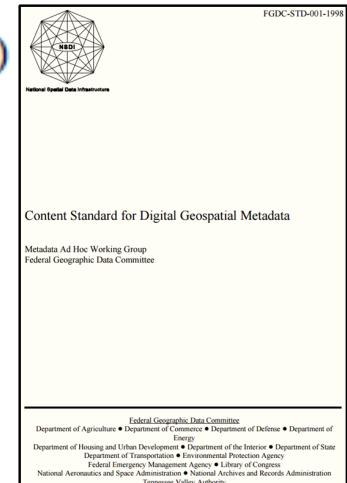
Metadata

1. Identification Information
2. Data Quality Information
3. Spatial Data Organization Information
4. Spatial Reference Information
5. Entity and Attribute Information
6. Distribution Information
7. Metadata Reference Information

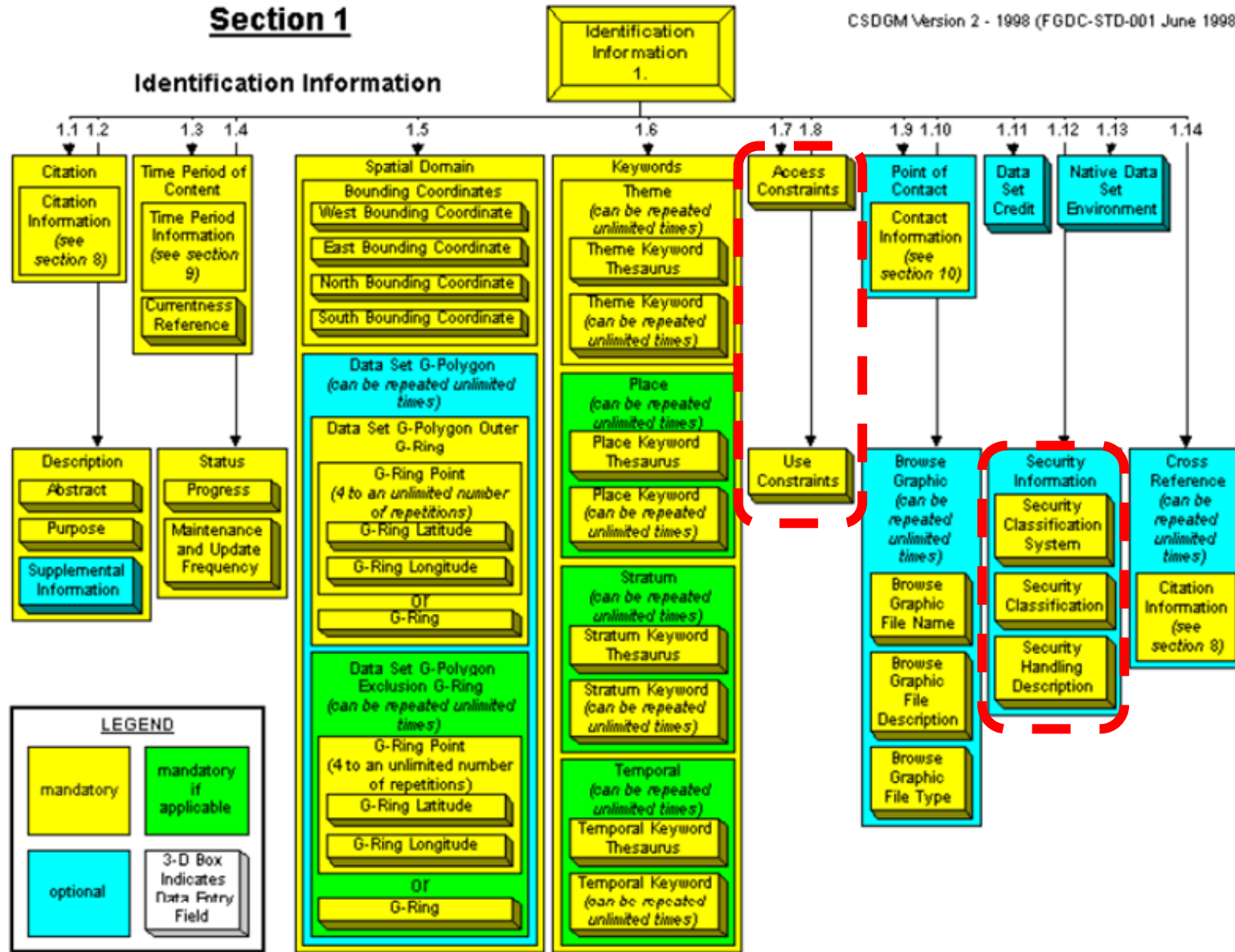
LEGEND

- mandatory
- mandatory if applicable
- optional
- 3-D Box Indicates Data Entry Field

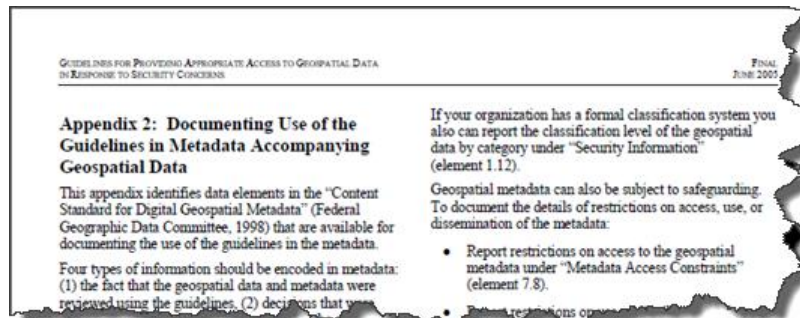
13. Decide the extent of restrictions.



# Section 1



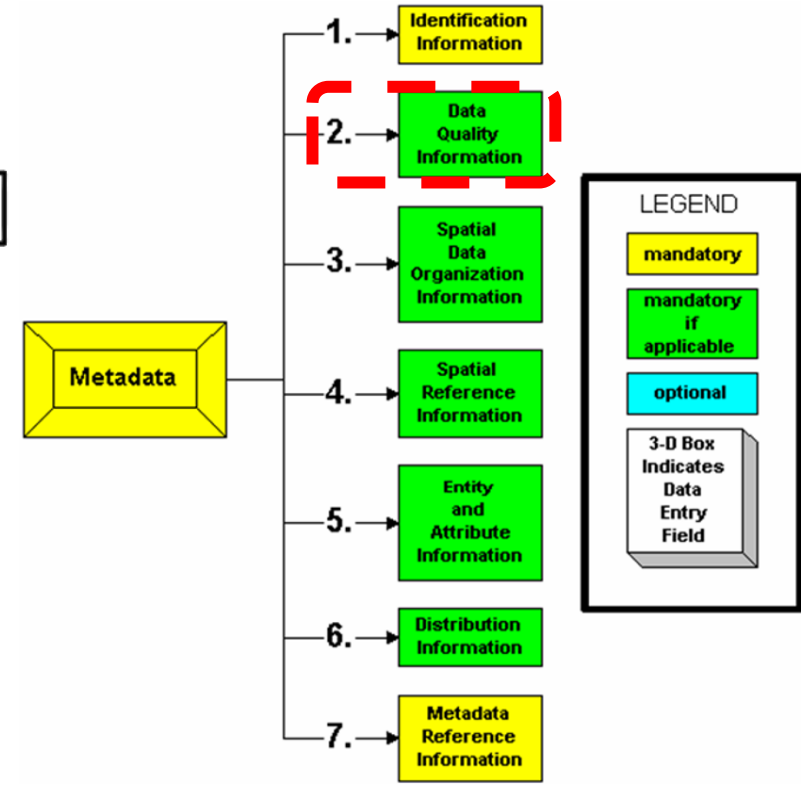
13. Decide the extent of restrictions.



**3. Document your use of the decision procedure.**

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

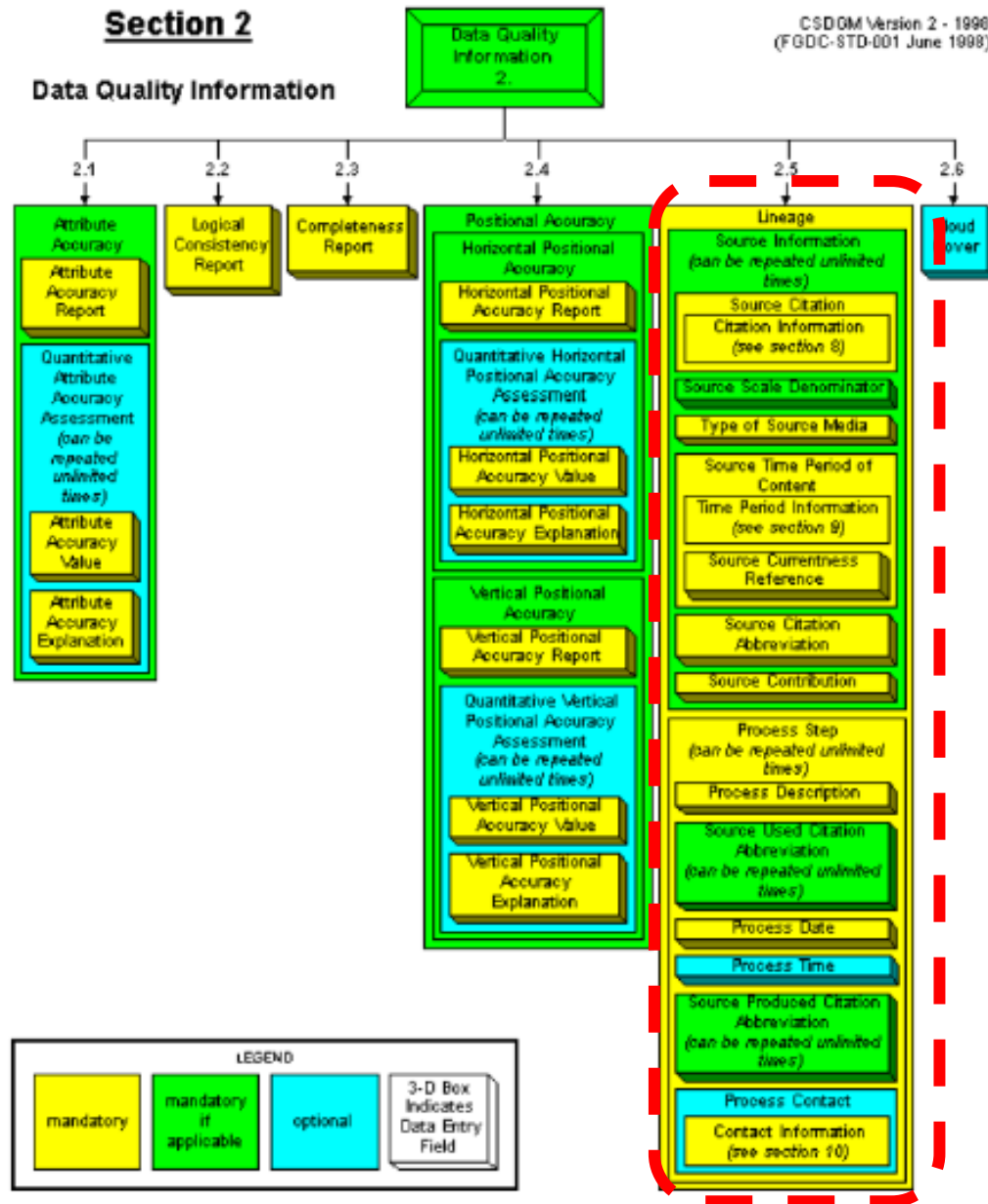
10. Change these data.



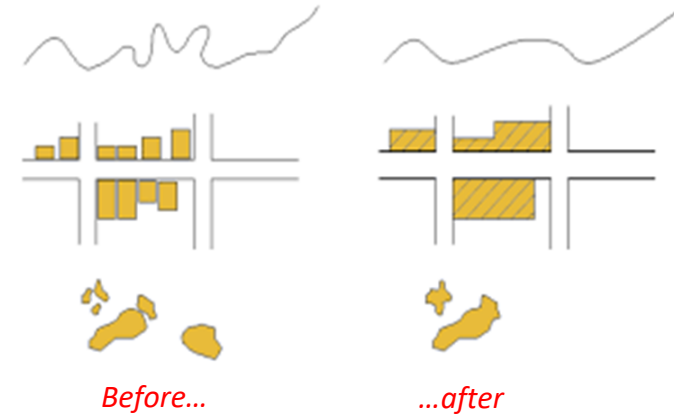
## Section 2

CSDGM Version 2 - 1998  
(FGDC-STD-001 June 1998)

### Data Quality Information



10. Change these data.



### Techniques of Cartographic Generalization

1. Selective Omission
2. Simplification
3. Combination
4. Exaggeration
5. Displacement

# ArcGIS Resources

Home   Communities   Help

## ArcGIS Help 10.

Resource Center

- Welcome to the ArcGIS Help Library
- What's New
- Desktop
- Geodata
  - Introduction
  - Databases
  - Geodatabases
  - Administering geodatabases
  - Data types
    - Introduction
    - Annotations
    - CAD
    - Coverages
    - Dimension features
    - Domains
    - Feature classes
    - Feature datasets
    - Geometric networks
    - KML
    - LAS dataset
    - Locators
    - Metadata**
    - NETCDF
    - Network datasets

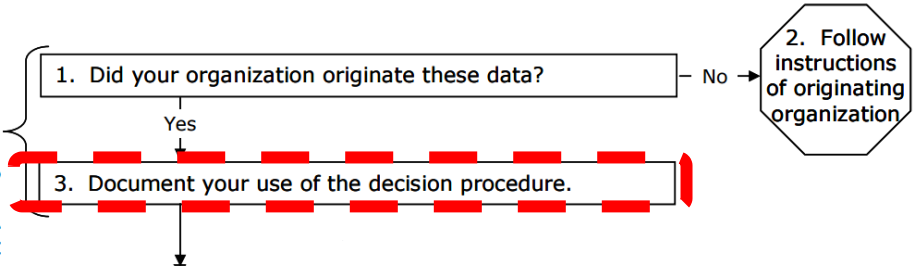
### Metadata

- What is metadata?
- Essential metadata vocabulary
- About viewing metadata
- Viewing metadata
- Metadata styles and standards
- Choosing a metadata style
- The ArcGIS metadata format
- Editing metadata**
- Importing and exporting metadata
- Printing metadata
- Automatic metadata updates

### Editing metadata

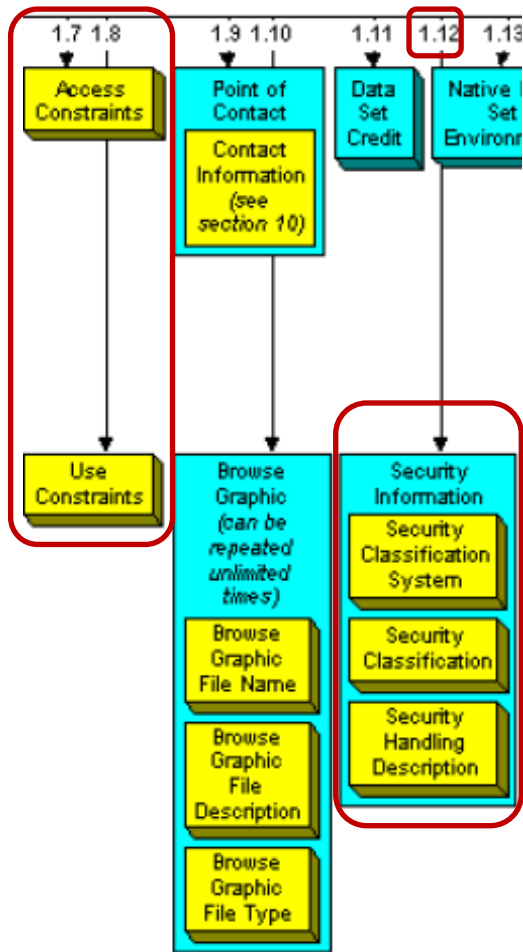
- A quick tour of creating and editing metadata
- Upgrading existing FGDC metadata from the Description tab
- Editing metadata
- About creating thumbnails
- Creating thumbnails
- Creating standard-compliant metadata
- About validating metadata
- Validating metadata
- Metadata workflows

Section 1: Is it your decision to apply safeguards to these data?





# Communicating risk classification and controls...



**Note: Be wary of metadata with undefined or free text domains which block use in automated controls...**

1.7 Access Constraints -- restrictions and legal prerequisites for accessing the data set. These include any access constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on obtaining the data set.

Type: text  
 Domain: "None" free text ←  
 Short Name: accconst

1.8 Use Constraints -- restrictions and legal prerequisites for using the data set after access is granted. These include any use constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on using the data set.

Type: text  
 Domain: "None" free text ←  
 Short Name: useconst

1.12 Security Information -- handling restrictions imposed on the data set because of national security, privacy, or other concerns.

Type: compound  
 Short Name: secinfo

1.12.1 Security Classification System -- name of the classification system.

Type: text  
 Domain: free text ←  
 Short Name: secsys

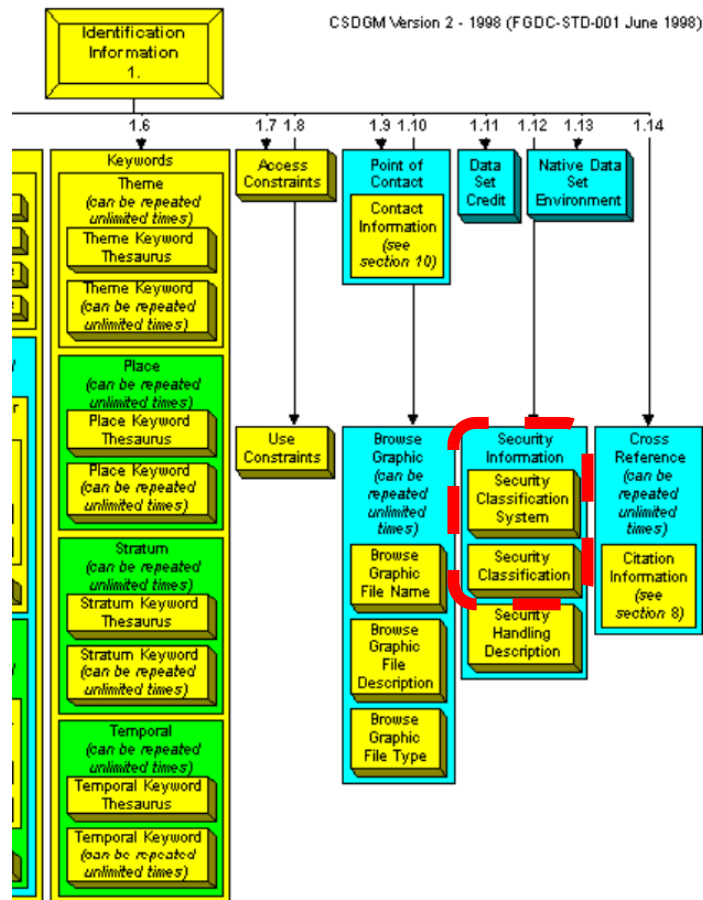
1.12.2 Security Classification -- name of the handling restrictions on the data set.

Type: text  
 Domain: "Top secret" "Secret" "Confidential" "Restricted" "Unclassified" "Sensitive" free text ←  
 Short Name: secclass

1.12.3 Security Handling Description -- additional information about the restrictions on handling the data set.

Type: text  
 Domain: free text ←  
 Short Name: sechandl

# ...security classification for geospatial data...



1.12 Security Information -- handling restrictions imposed on the data set because of national security, privacy, or other concerns.

Type: compound  
Short Name: secinfo

1.12.1 Security Classification System -- name of the classification system.

Type: text  
Domain: free text  
Short Name: secsys

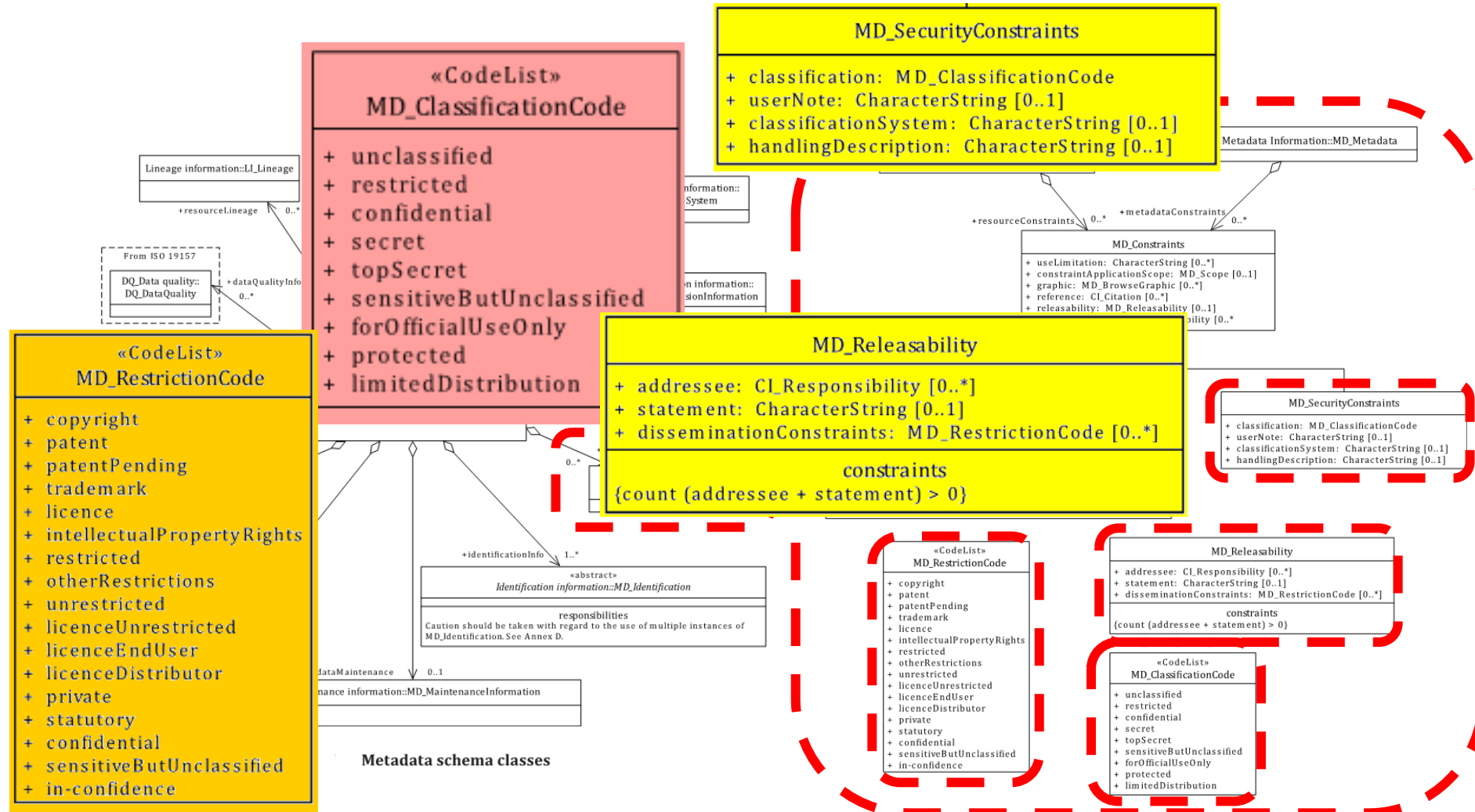
1.12.2 Security Classification -- name of the handling restrictions on the data set.

Type: text  
Domain: "Top secret" "Secret" "Confidential" "Restricted" "Unclassified" "Sensitive"  
free text  
Short Name: secclass

1.12.3 Security Handling Description -- additional information about the restrictions on handling the data set.

Type: text  
Domain: free text  
Short Name: sechandl

# ISO19115-1 Geospatial metadata standard



# Department of Defense' Information Assurance (IA)

...also categorizes information systems and data in terms of CIA...


## Confidentiality Levels

LEVEL	DEFINITION
High	Classified Information
Medium	Sensitive Information, Not Cleared for Public Release
Basic	Information Cleared for Public Release

+

## Mission Assurance Categories

- **MAC I** – vital to operational readiness or mission effectiveness of deployed or contingency forces. Loss of integrity or availability unacceptable. Requires most stringent protective measures.
- **MAC II** – important to the support of deployed or contingency forces. Loss of integrity unacceptable, unavailability tolerable only for short time. Require additional safeguards beyond best practices.
- **MAC III** – necessary to conduct of day-to-day business. Protection commensurate with commercial best practices.

 Department of Defense  
**INSTRUCTION**  
NUMBER 8580.1  
July 9, 2004  
ASD(NII)

---

SUBJECT: Information Assurance (IA) in the Defense Acquisition System

References: (a) Chapter 25 of title 40, United States Code  
(b) DoD Directive 8500.1, "Information Assurance," October 24, 2002  
(c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003  
(d) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003  
(e) through (k), see enclosure 1

1. PURPOSE

This Instruction:

- 1.1. Implements policy, assigns responsibilities, and prescribes procedures under references (a), (b), and (c) necessary to integrate information assurance (IA) into the Defense Acquisition System described in reference (d) and DoD Instruction 5000.2 (reference (e)).
- 1.2. Describes required and recommended levels of IA activities relative to the acquisition of systems and services.
- 1.3. Describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

2. APPLICABILITY AND SCOPE

This Instruction:

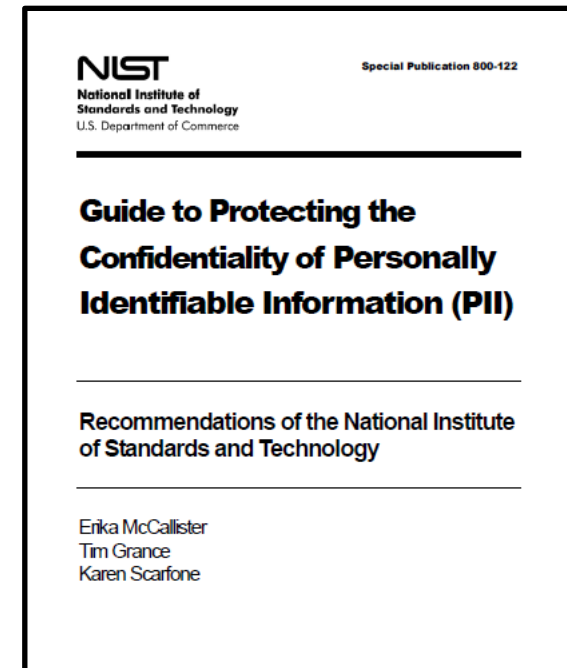
- 2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the

# Agenda

- ✓ In The News
- ✓ Categorizing Information for IT Risk Management
- ✓ Revisit Risk & Controls of Publicly Shared Geographic Information
- More on Confidentiality: Linked & Linkable PII
- Risk Evaluation
- Risk Management Techniques, a brief review
- Test taking tip
- Quiz

# NIST SP 800-122 – Guide to Protecting Confidentiality of PII

- Specifically focused on:
  - Identifying PII
  - **Determining PII confidentiality** impact level needed to supplement the FIPS 199 confidentiality impact level of an information system

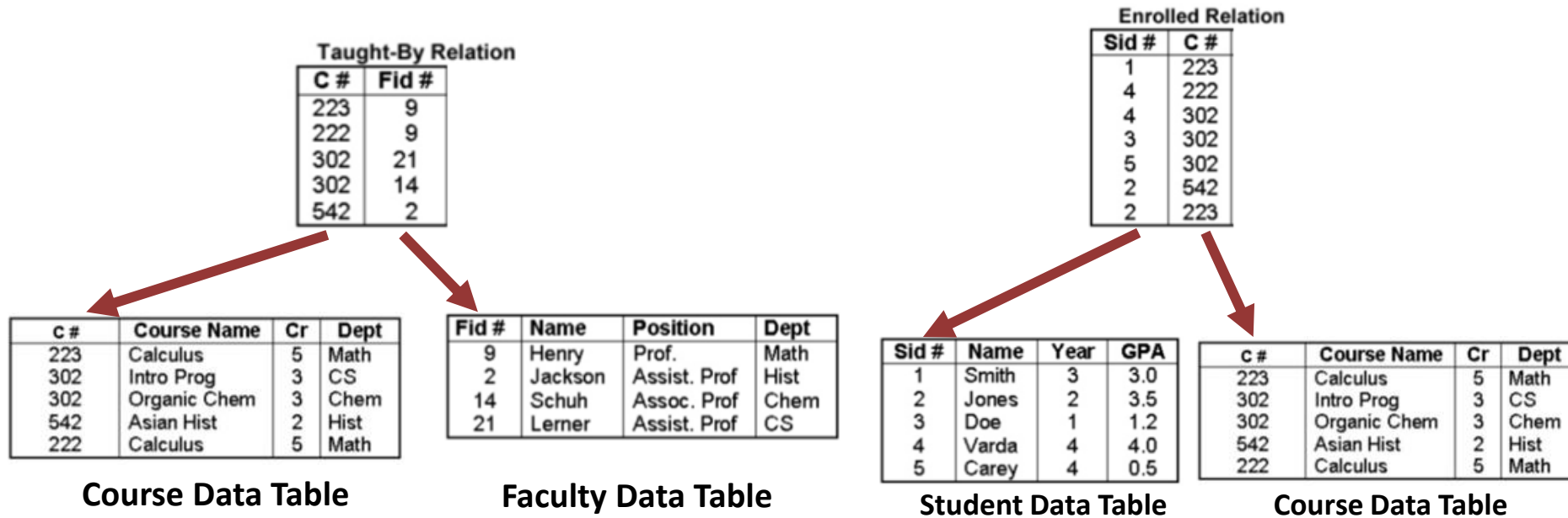


# Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including:

1. Any information that can be used to distinguish (i.e. identify) or trace an individual's identity, such as:
  - *Name*
  - *Identifying number*
  - *Address*
  - *Asset identifier*
  - *Telephone number*
  - *Personal characteristics*
  - *Personally owned property identifiers*
2. Any other information that is linked or linkable to the identifiers listed in #1:
  - Date of birth
  - Place of birth
  - Race
  - Religion
  - Weight
  - Geographic indicators
  - Medical information
  - Educational information
  - Financial information
  - Employment information
  - ...

# Linked information





# Linkable information

Property ("Parcel") Data Table

Shape	ID	PIN	Area	Addr	Code
	1	334-1626-001	7,342	341 Cherry Ct.	SFR
	2	334-1626-002	8,020	343 Cherry Ct.	UND
	3	334-1626-003	10,031	345 Cherry Ct.	SFR
	4	334-1626-004	9,254	347 Cherry Ct.	SFR
	5	334-1626-005	8,856	348 Cherry Ct.	UND
	6	334-1626-006	9,975	346 Cherry Ct.	SFR
	7	334-1626-007	8,230	344 Cherry Ct.	SFR
	8	334-1626-008	8,645	342 Cherry Ct.	SFR

*PIN ("Property Identity Number") is a common identifying attribute that can serve as a "foreign key" to link the data tables together*

Owner Tax Data Table

PIN	Owner	Acq.Date	Assessed	TaxStat
334-1626-001	G. Hall	1995/10/20	\$115,500.00	02
334-1626-002	H. L Holmes	1993/10/06	\$24,375.00	01
334-1626-003	W. Rodgers	1980/09/24	\$175,500.00	02
334-1626-004	J. Williamson	1974/09/20	\$135,750.00	02
334-1626-005	P. Goodman	1966/06/06	\$30,350.00	02
334-1626-006	K. Staley	1942/10/24	\$120,750.00	02
334-1626-007	J. Dormandy	1996/01/27	\$110,650.00	01
334-1626-008	S. Gooley	2000/05/31	\$145,750.00	02

*Is this PII ?*

# Personally Identifiable Information (PII)

Any information about an individual maintained by an agency, including:

1. Any information that can be used to distinguish (i.e. identify) or trace an individual's identity, such as:
  - Name
  - Identifying number
  - Address
  - Asset identifier
  - Telephone number
  - Personal characteristics
  - Personally owned property identifiers
2. Any other information that is linked or linkable to the identifiers listed in #1:
  - Date of birth
  - Place of birth
  - Race
  - Religion
  - Weight
  - Geographic indicators
  - Medical information
  - Educational information
  - Financial information
  - Employment information
  - ...

Property ("Parcel") Data Table

Shape	ID	PIN	Area	Addr	Code
	1	334-1626-001	7,342	341 Cherry Ct.	SFR
	2	334-1626-002	8,020	343 Cherry Ct.	UND
	3	334-1626-003	10,031	345 Cherry Ct.	SFR
	4	334-1626-004	9,254	347 Cherry Ct.	SFR
	5	334-1626-005	8,856	348 Cherry Ct.	UND
	6	334-1626-006	9,975	346 Cherry Ct.	SFR
	7	334-1626-007	8,230	344 Cherry Ct.	SFR
	8	334-1626-008	8,645	342 Cherry Ct.	SFR

Owner Tax Data Table

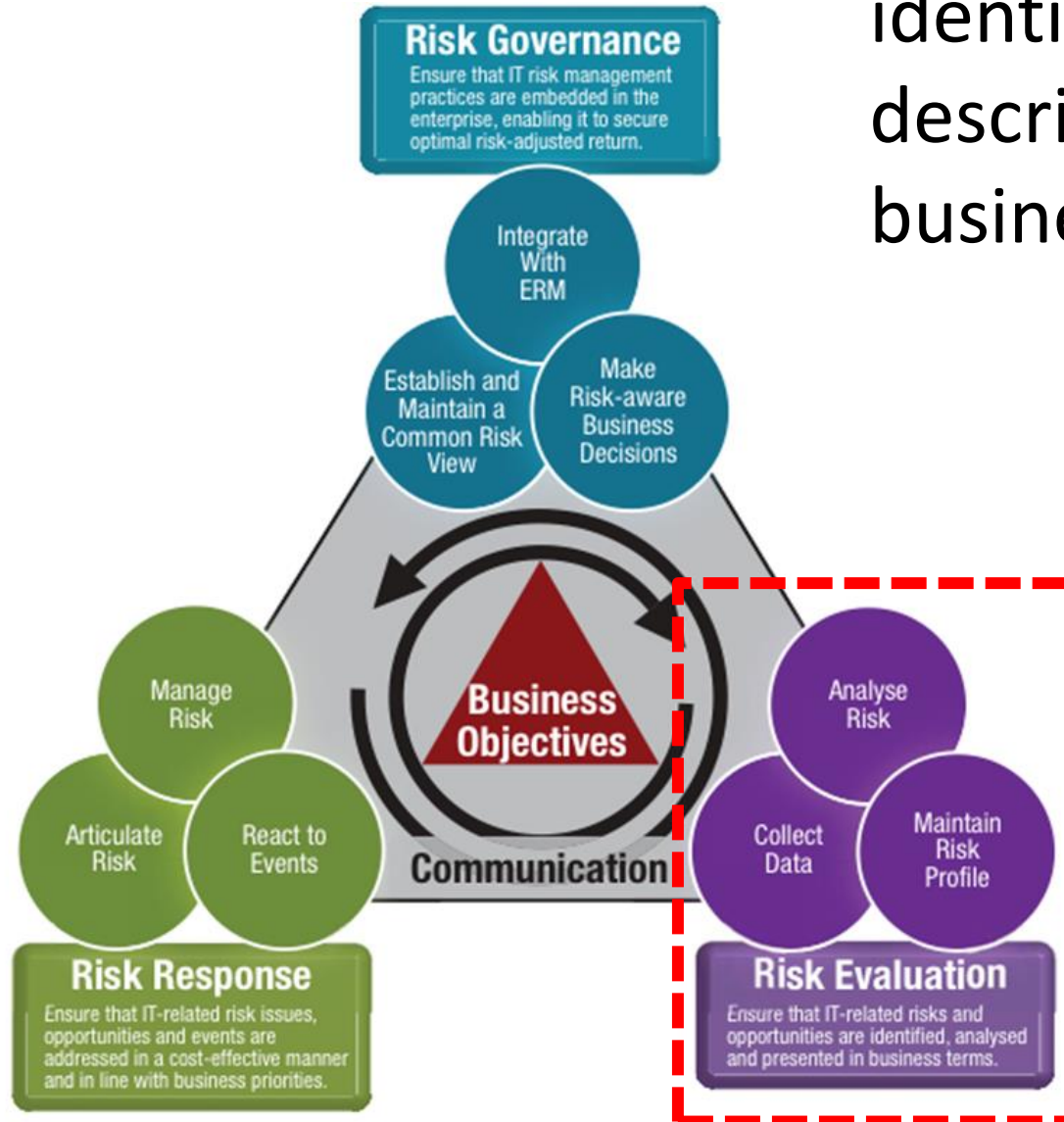
PIN	Owner	Acq.Date	Assessed	TaxStat
334-1626-001	G. Hall	1995/10/20	\$115,500.00	02
334-1626-002	H. L Holmes	1993/10/06	\$24,375.00	01
334-1626-003	W. Rodgers	1980/09/24	\$175,500.00	02
334-1626-004	J. Williamson	1974/09/20	\$135,750.00	02
334-1626-005	P. Goodman	1966/06/06	\$30,350.00	02
334-1626-006	K. Staley	1942/10/24	\$120,750.00	02
334-1626-007	J. Dormandy	1998/01/27	\$110,650.00	01
334-1626-008	S. Gooley	2000/05/31	\$145,750.00	02

# Agenda

- ✓ In The News
- ✓ Categorizing Information for IT Risk Management
- ✓ Revisit Risk & Controls of Publicly Shared Geographic Information
- ✓ More on Confidentiality: Linked & Linkable PII
- 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

## *Analyse Risk*

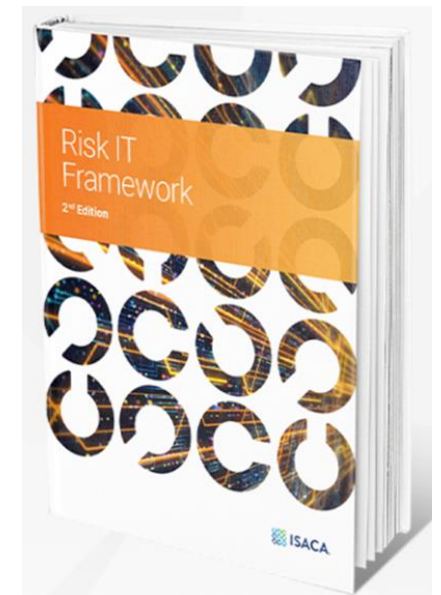
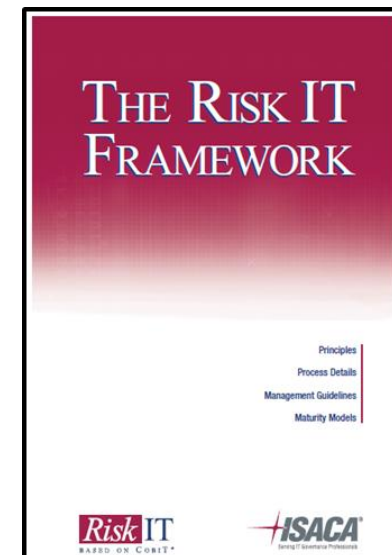
Develop useful information to support risk decisions that take into account the business impact of risk factors

## *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

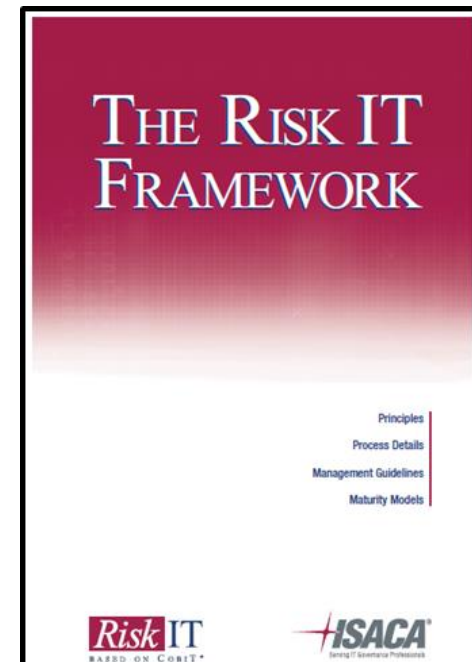
# Risk Evaluation - Collect Data (RE-1)

- **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

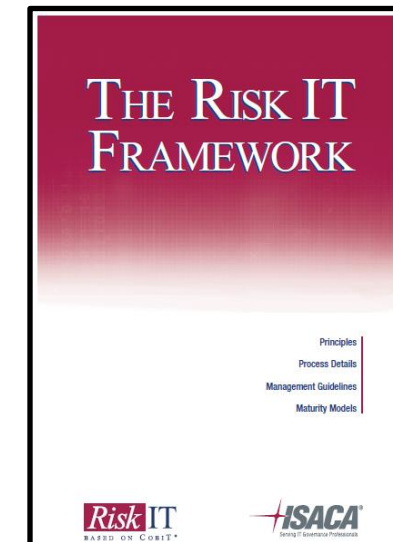
## RACI Chart

## 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

### 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, copied, New York general business, inform customers.

#### Information Classification

All information at the City of New York is classified into four levels; public, sensitive, private

- **Public**—This information might cause damage.
- **Sensitive**—This information requires protection to prevent inappropriate disclosure.
- **Private**—This information is of a nature that would damage the public trust placed in the agency.
- **Confidential**—This is the highest level of information containing information whose disclosure could cause damage to public safety, or lead to the disclosure of information that would be a significant competitive advantage to a private enterprise.

#### 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 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			Categorization
	Confidentiality	Integrity	Availability	
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	?

# Analyze risk to prioritize protection

*An authoritative lookup table for transforming ordinal to ratio risk data...*

	Impact		
<b>Threat Likelihood</b>	<b>Low (10)</b>	<b>Moderate (50)</b>	<b>High (100)</b>
<b>High (1.0)</b>	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
<b>Moderate (0.5)</b>	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
<b>Low (0.1)</b>	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$

*Risk Scale: High (>50 to 100)*

*Moderate (>10 to 50)*

*Low (1 to 10)*

01527a

NIST SP 800-100 “Information Security Handbook: A Guide for Managers”, page 90  
found via [SCHEDULE](#) menu item in MIS Community site

# Analyze risk to prioritize protection

Threat Likelihood	Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	$10 \times 1.0 = 10$	$50 \times 1.0 = 50$	$100 \times 1.0 = 100$
Moderate (0.5)	$10 \times 0.5 = 5$	$50 \times 0.5 = 25$	$100 \times 0.5 = 50$
Low (0.1)	$10 \times 0.1 = 1$	$50 \times 0.1 = 5$	$100 \times 0.1 = 10$

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



Data Classification Policy

**The Policy**

The Agency head or designee shall appropriately categorize and value information.

**Background**

To ensure that business information of the information must be protected. Business information assets are used to provide business services with interest.

**Scope**

This policy applies to all information, whether written, stored electronically, or transmitted, that is owned by the City of New York, general business information, or information of its customers.

**Information Classification**

All information at the City of New York is classified into 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.

**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

Expected 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 = Single Loss Expectancy × 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:*

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

*greatly influence the results...*

<u>Annual Loss Expectancy Calculation</u>		
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
<u>IT investigation:</u>		<u>\$ 200</u>
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
<u>IT investigation:</u>	<u>\$ 200</u>
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
<u>Managed Device Service:</u>	<u>\$ 100</u>
Annual Cost of Countermeasures:	\$ 400

# Analyze Risk

## MANAGEMENT GUIDELINES—RE2



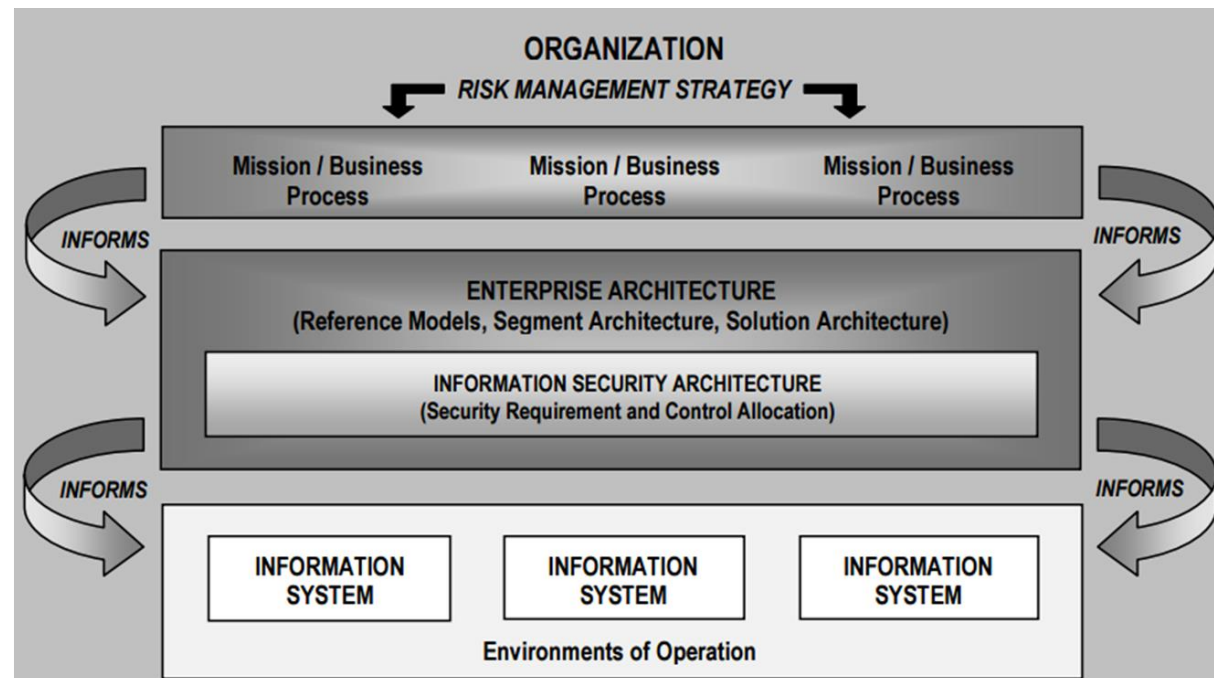
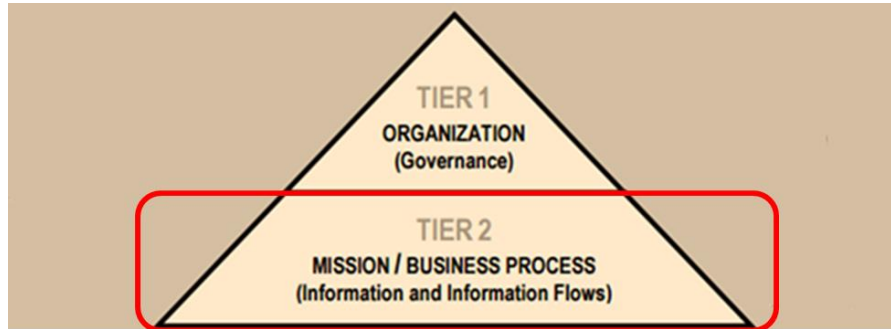
### RACI Chart

### Roles

Key Activities	Board	CEO	CRO	CFO	CFD	Enterprise Risk Committee	Business Management	Business Process Owner	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?*



**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 agencies are classified into four levels; public, sensitive, private, or confidential.

- **Public**—This information might not need to be disclosed, but its disclosure could cause damage.
- **Sensitive**—This information requires a greater level of protection than public information to prevent inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure could cause damage to the public trust placed in the agency.
- **Confidential**—This is the highest level of sensitivity, and its disclosure could cause damage to the agency's ability to perform its primary business functions. Information containing information whose disclosure could lead directly to the death of an individual, 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 appropriate level of security protection.
- 2) All information assets must be valued and categorized.
- 3) Information assets must be evaluated, valued and categorized on a regular basis.
- 4) To ensure that appropriate protection is provided, the value of the information must be determined before transmission over any communication system.

**Data Steward**

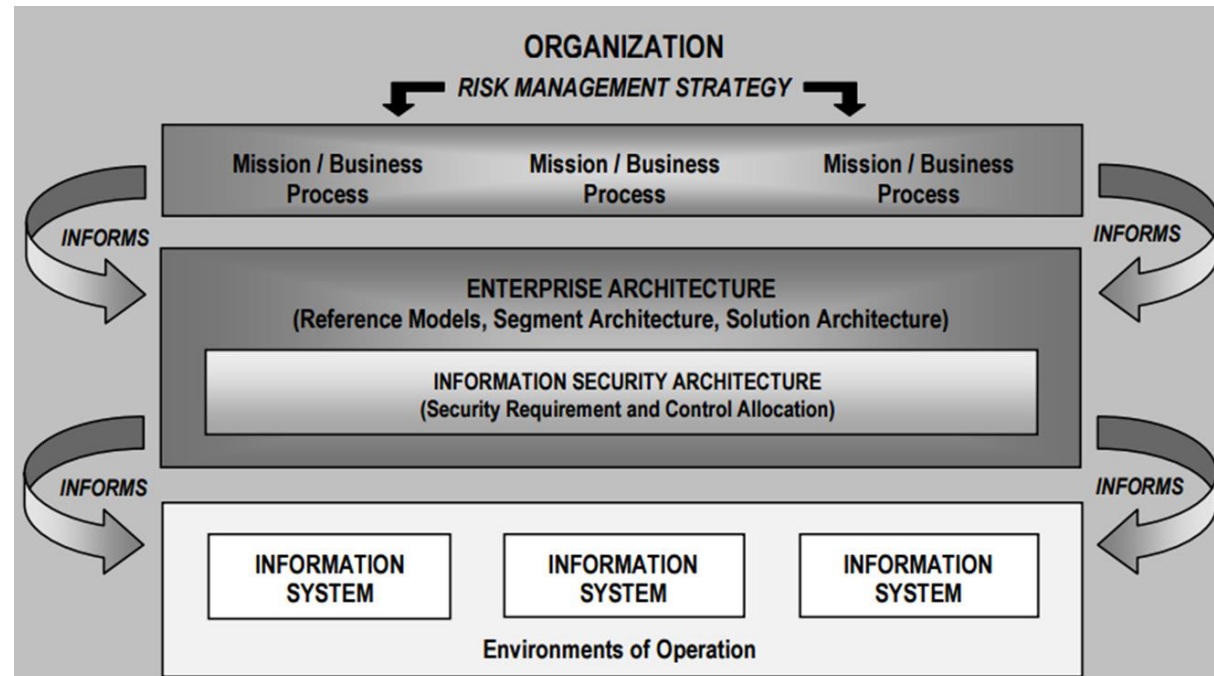
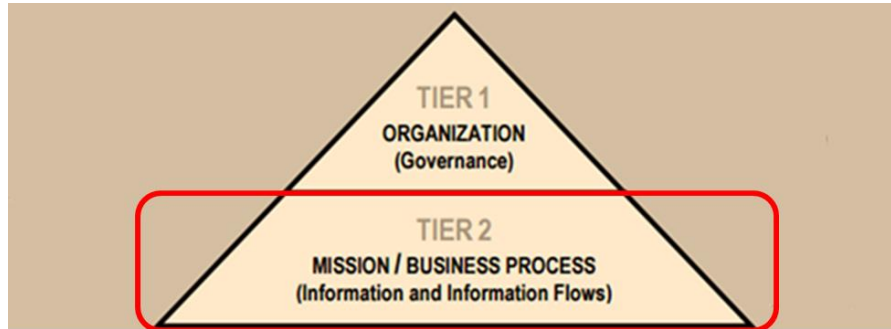
- 5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- 6) The Data Steward is responsible for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

**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	CFO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	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 resources.		C		R		C	A	R		I
RE3.3 Understand IT capabilities.			C	A/R			C	C		I
RE3.4 Update IT risk scenario components.			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

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**

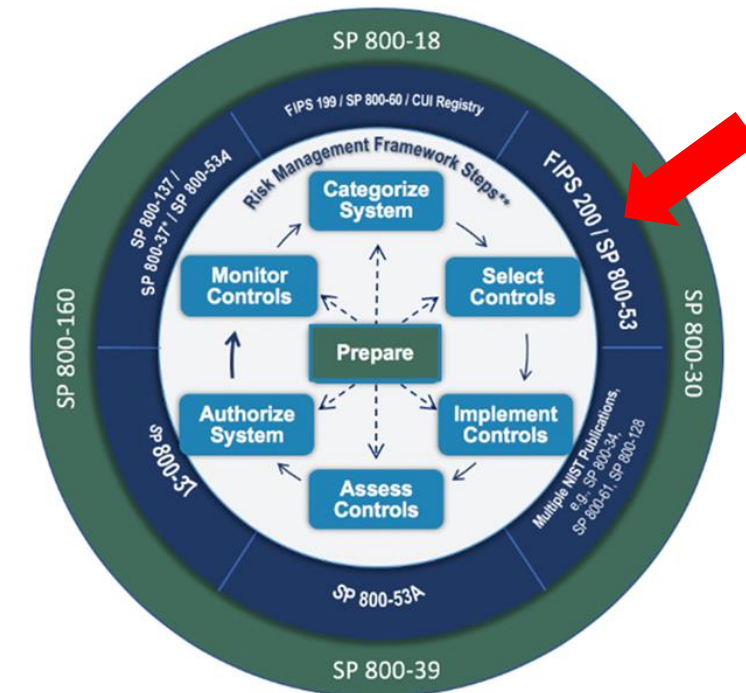
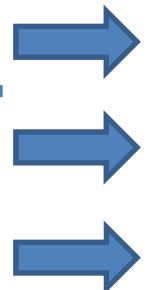
- 5) The Data Steward is normally someone who is responsible for or dependent on the business process associated with the information asset, and who is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.
- 6) The Data Steward is responsible for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

Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	



# Agenda

- ✓ In The News
- ✓ Categorizing Information for IT Risk Management
- ✓ Revisit Risk & Controls of Publicly Shared Geographic Information
- ✓ 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 PRIMARILY because:

- A. it ensures accountability for information resources as required by roles and 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

Information classification is important to properly manage risk PRIMARILY because:

- A. it ensures accountability for information resources as required by roles and 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

*An entitlement is a provision made in accordance with a legal framework of a society. Typically, entitlements are based on concepts of principle which are themselves based in concepts of social equality or enfranchisement. [Wikipedia](#)*

# 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

- ✓ In The News
- ✓ Categorizing Information for IT Risk Management
- ✓ Revisit Risk & Controls of Publicly Shared Geographic Information
- ✓ More on Confidentiality: Linked & Linkable PII
- ✓ Risk Evaluation
- ✓ Risk Management Techniques, a brief review
- ✓ Test taking tip
- ✓ Quiz