

Managing Enterprise Cybersecurity

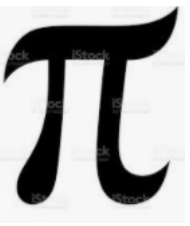
MIS 4596

Class 3

Agenda

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

Quiz



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

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

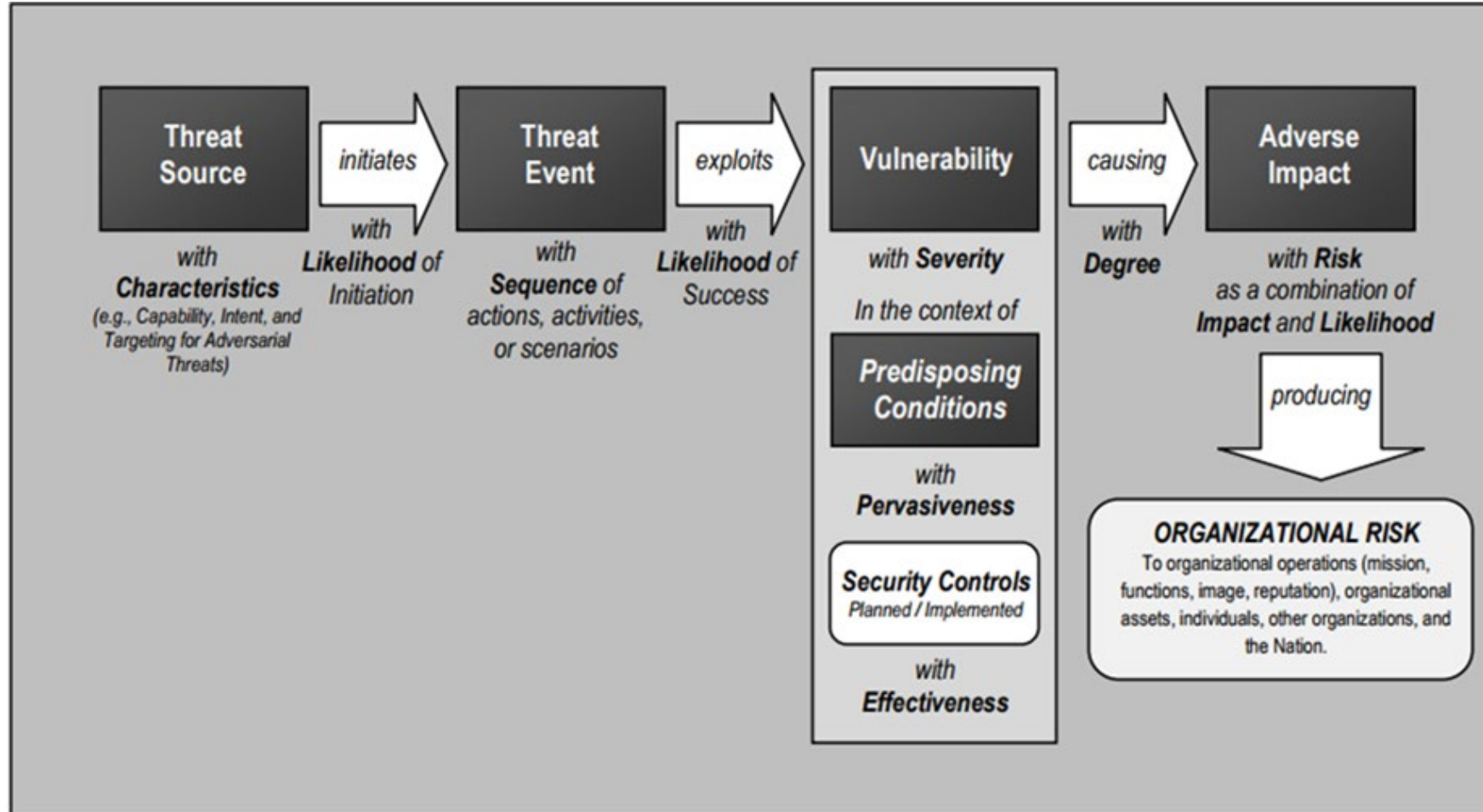
Goal: Help you develop a Security Mindset

Agenda

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

Business cybersecurity risk

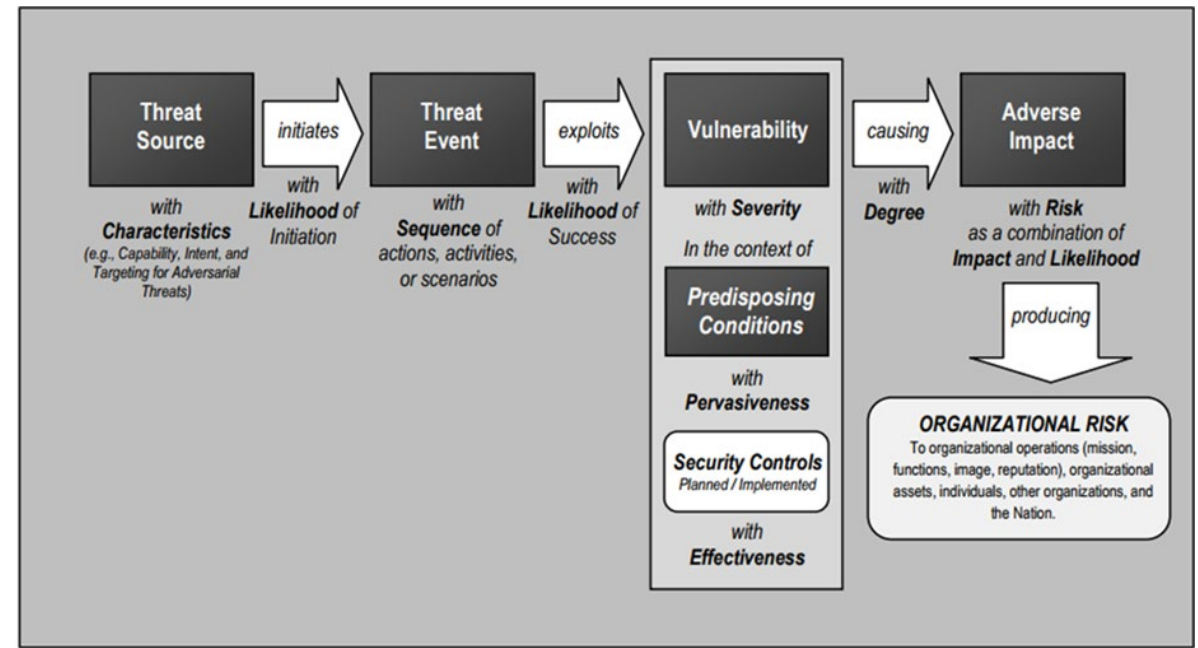
...is a function of what?



Business cybersecurity risk

...is a function of what?

cybersecurity risk = f (?, ?, ...)



f (threats, vulnerabilities, assets)

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

Results in impacts which have an adverse effect on:

- Organizational operations
- Assets
- individuals

Federal Information Security Management Act (FISMA) of 2002

Federal Information Security Modernization Act (FISMA) of 2014

Recognizes importance of information security to the economy and national security

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

NIST's "Cybersecurity Framework"

**Framework for Improving
Critical Infrastructure Cybersecurity**

Version 1.1

National Institute of Standards and Technology

April 16, 2018

What assets need protection?

IDENTIFY

What safeguards are
available?

PROTECT

What techniques can identify
incidents?

DETECT

What techniques can contain
impacts of incidents?

RESPOND

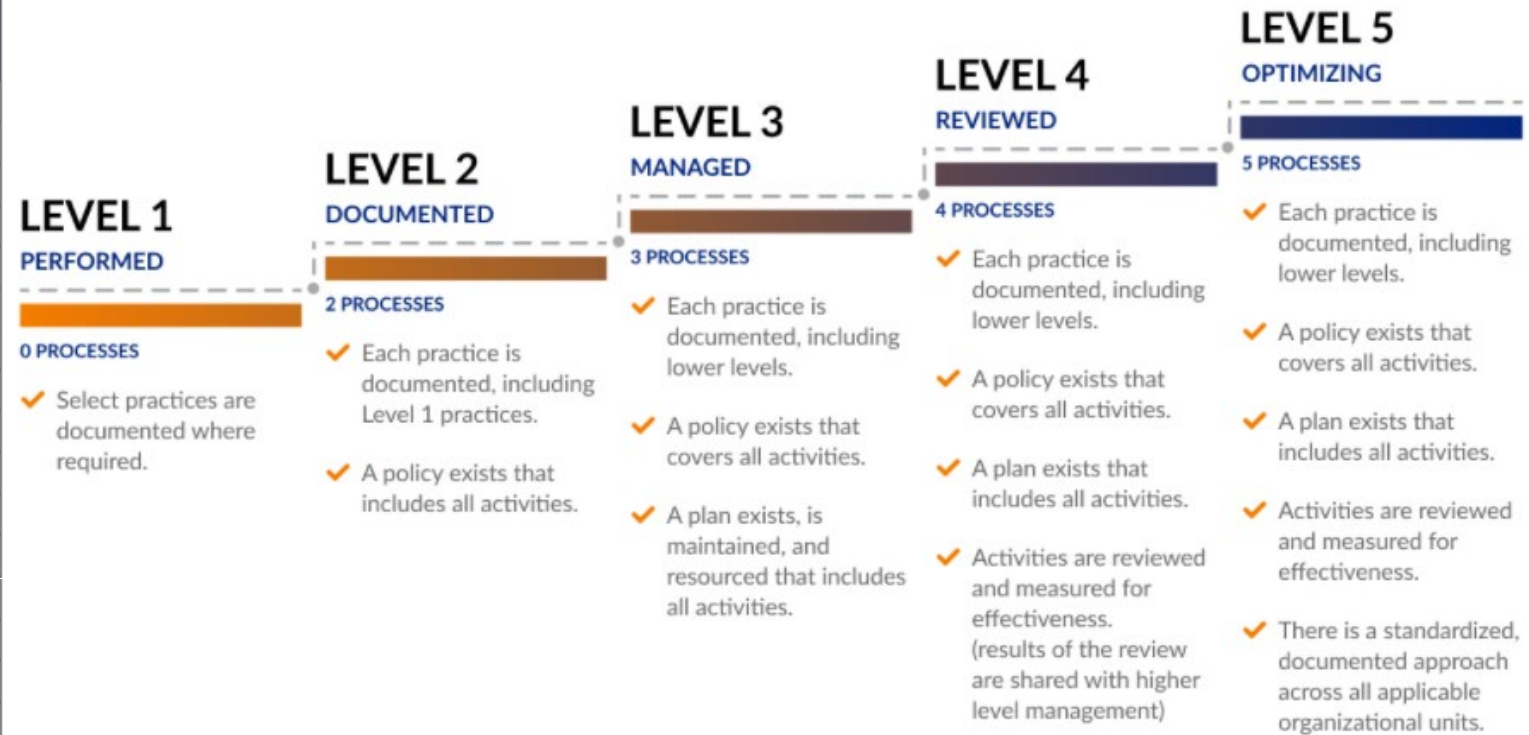
What techniques can restore
capabilities?

RECOVER

NIST Cybersecurity Framework

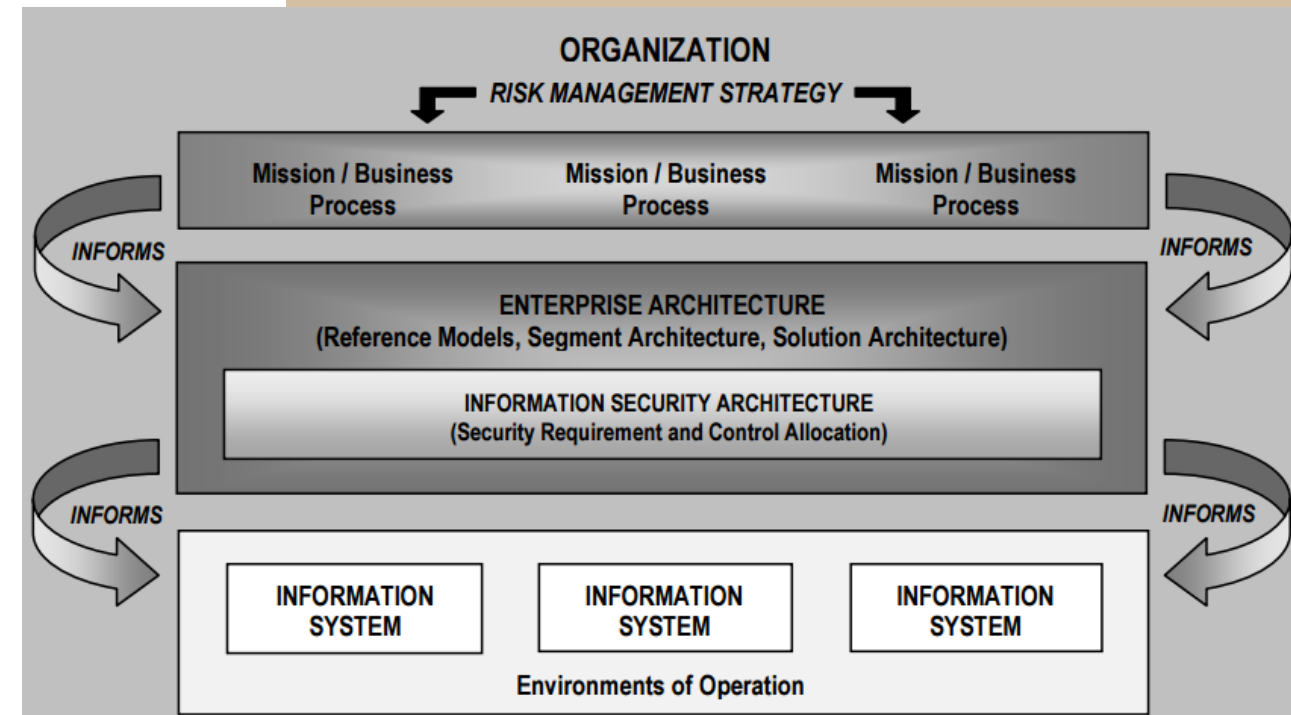
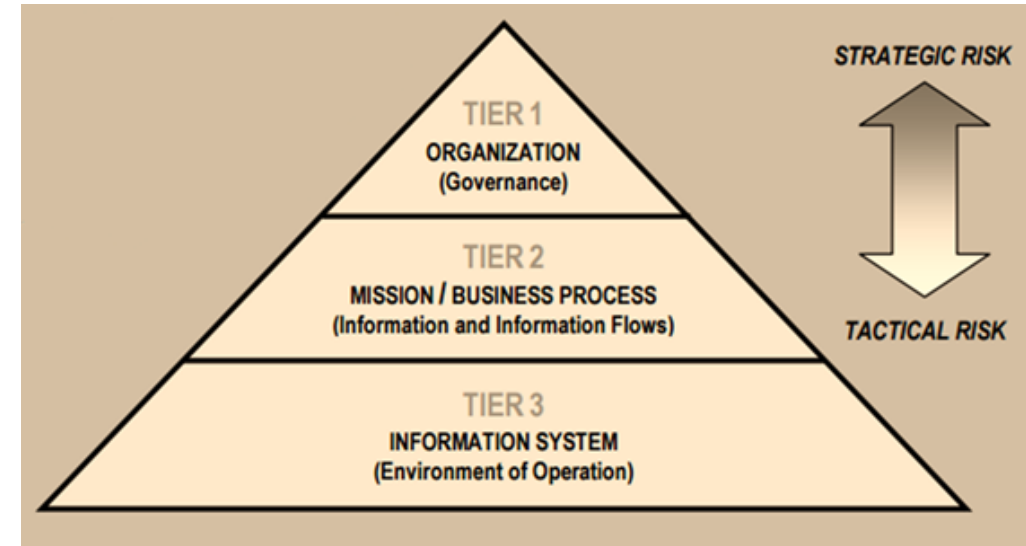
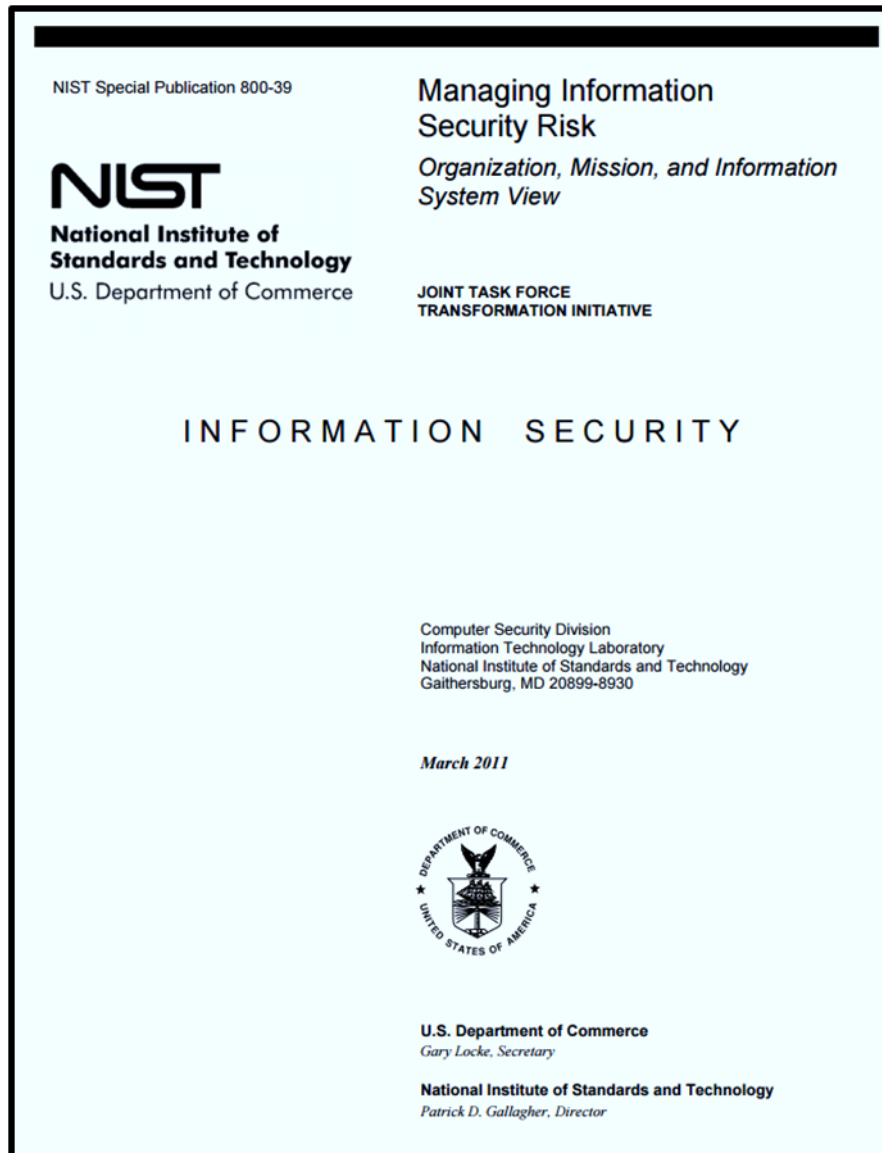
Cybersecurity Maturity Model Certification (CMMC) levels

| 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 |

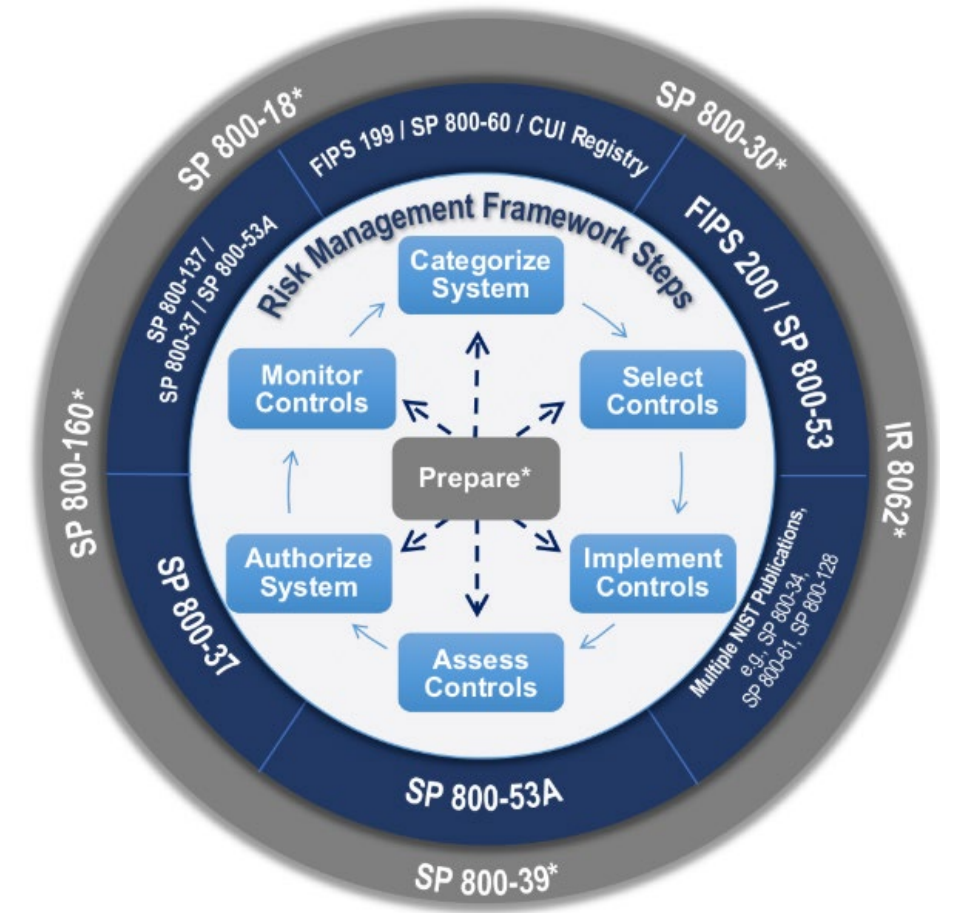
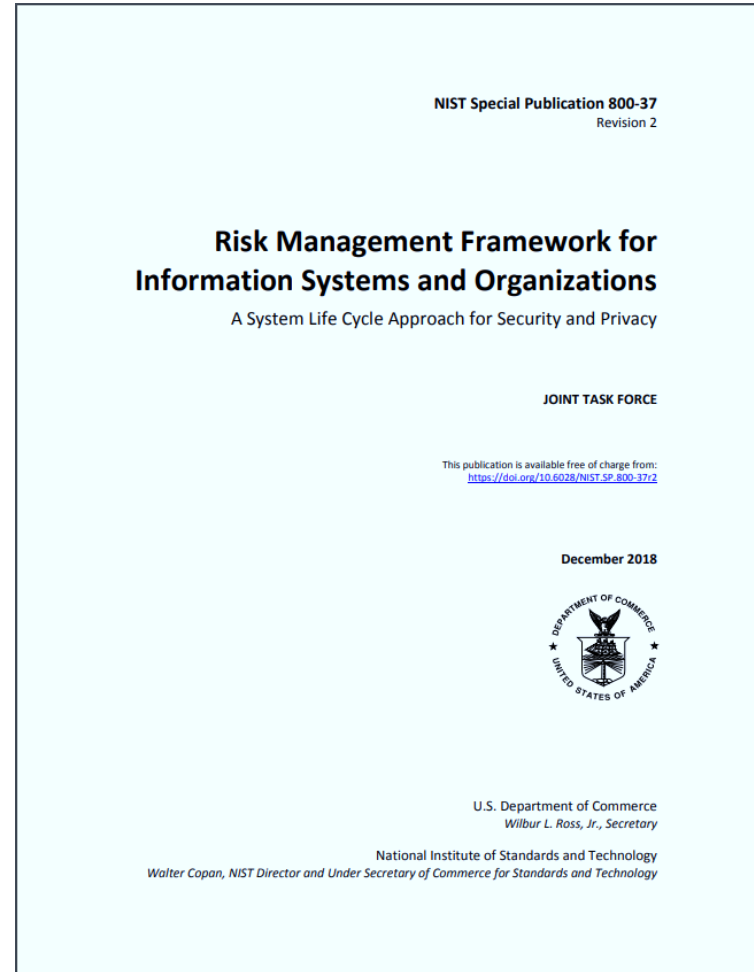


Is used to assess an organization's cybersecurity capability maturity level, and recommend steps for improvement

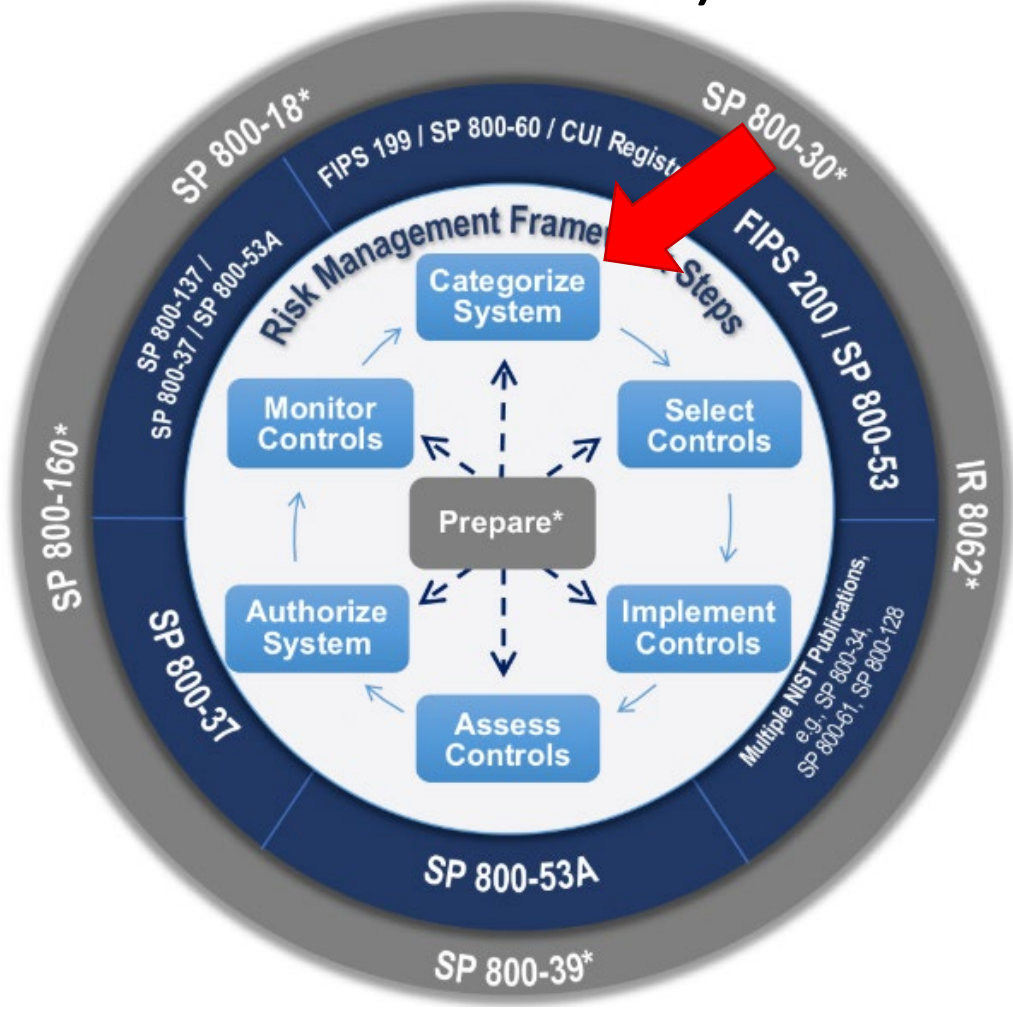
NIST's Risk Management Framework



Security Categorization & Selecting a Baseline of Cybersecurity Risk Controls



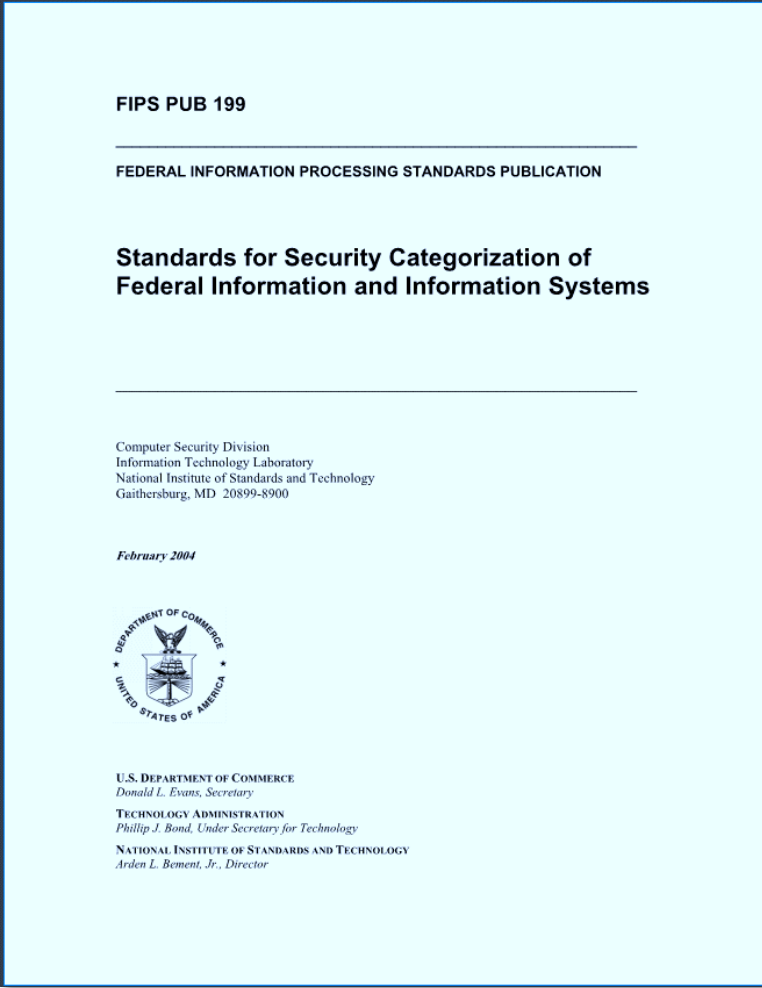
1st Step in cybersecurity is security categorization (i.e. risk assessment)



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

Risk is based on impact of a security breach

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



In the Risk Management Framework (RMF) likelihood of a breach is treated as 100%

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

FIPS Pub 199 Standards for Security Categorization

Low: Limited adverse effect

Medium: Serious adverse effect

High: Severe or catastrophic adverse effect

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

SC information system = $\{(\text{confidentiality}, \text{impact}), (\text{integrity}, \text{impact}), (\text{availability}, \text{impact})\}$,

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

Example with multiple information types:

SC contract information = $\{(\text{confidentiality}, \text{MODERATE}), (\text{integrity}, \text{MODERATE}), (\text{availability}, \text{LOW})\}$, = MODERATE rating

and

SC administrative information = $\{(\text{confidentiality}, \text{LOW}), (\text{integrity}, \text{LOW}), (\text{availability}, \text{LOW})\}$. = LOW rating

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

SC acquisition system = $\{(\text{confidentiality}, \text{MODERATE}), (\text{integrity}, \text{MODERATE}), (\text{availability}, \text{LOW})\}$, = MODERATE rating

What are the security categorizations of these datasets?

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

What are the security categorizations of the geodatabases?

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

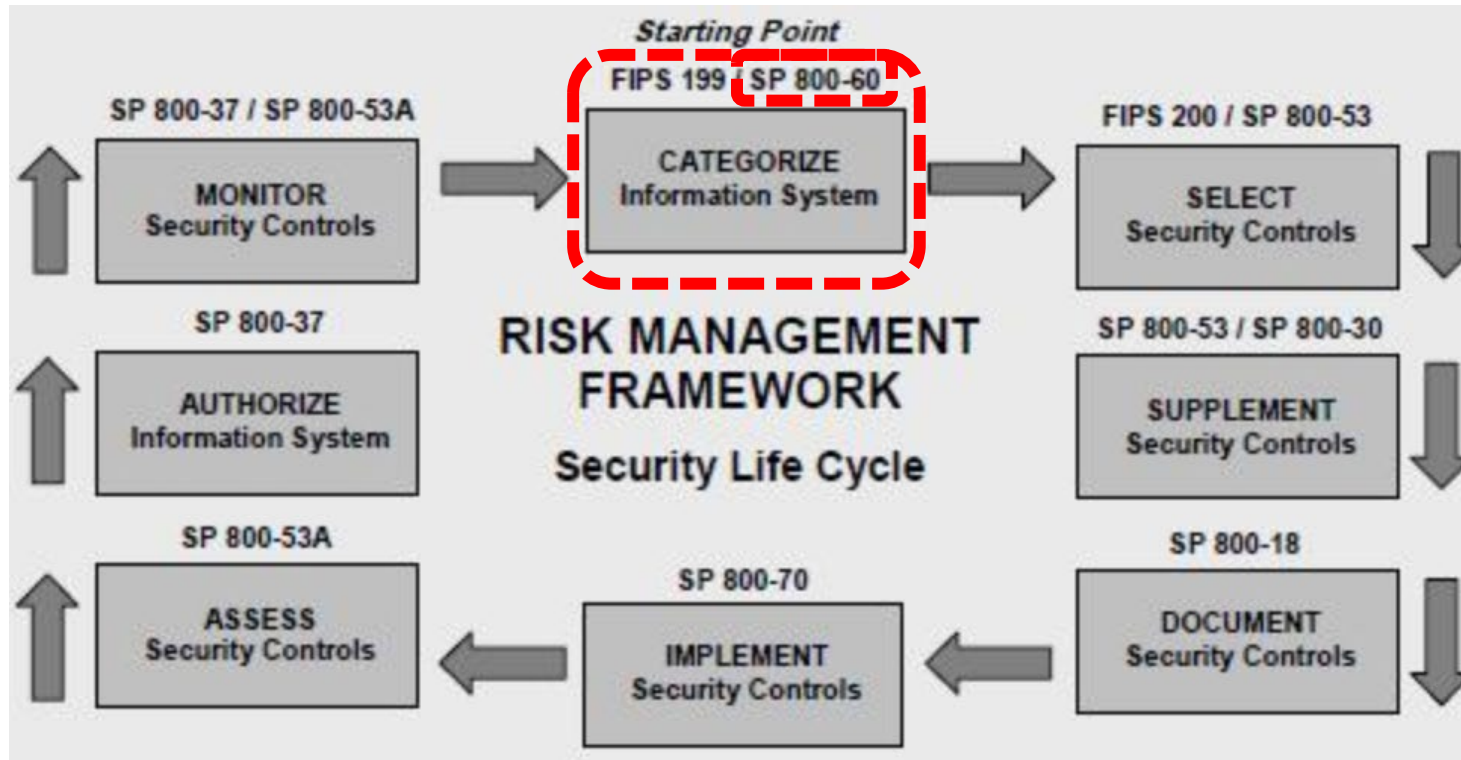
What is the overall security categorization of the information system containing these datasets?

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

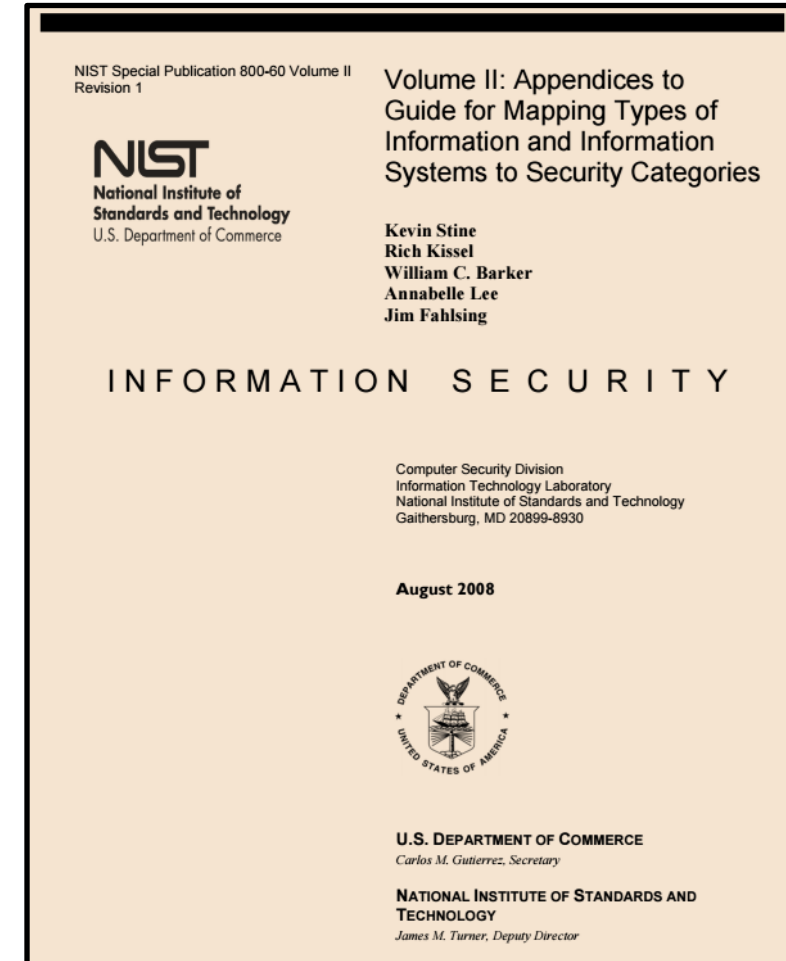
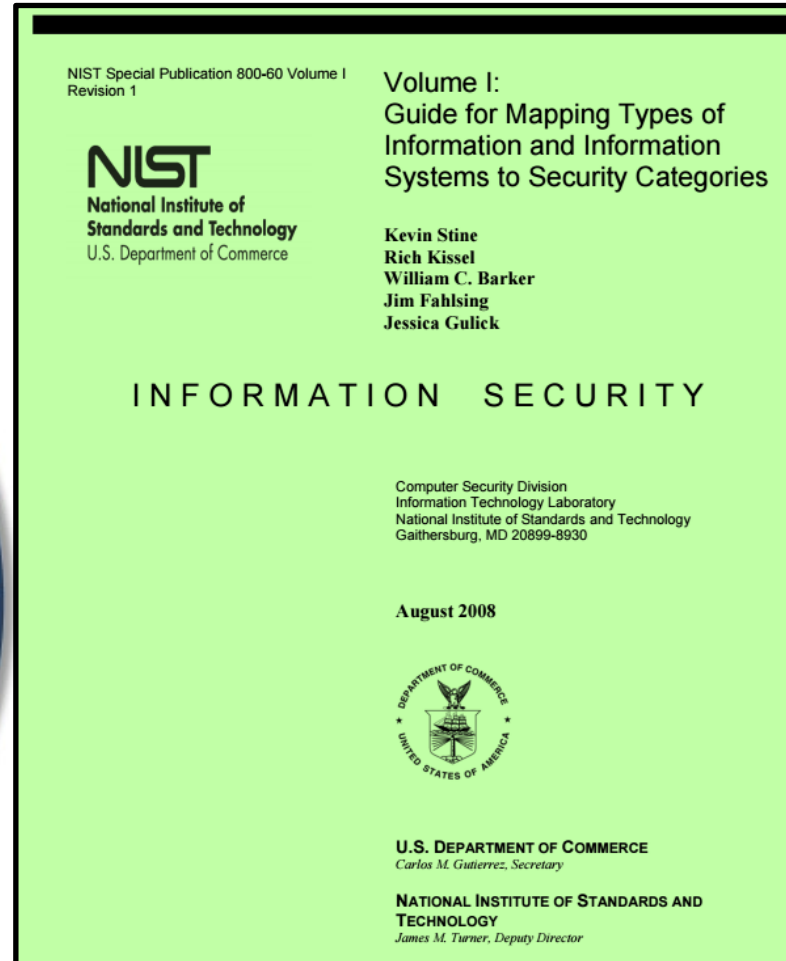
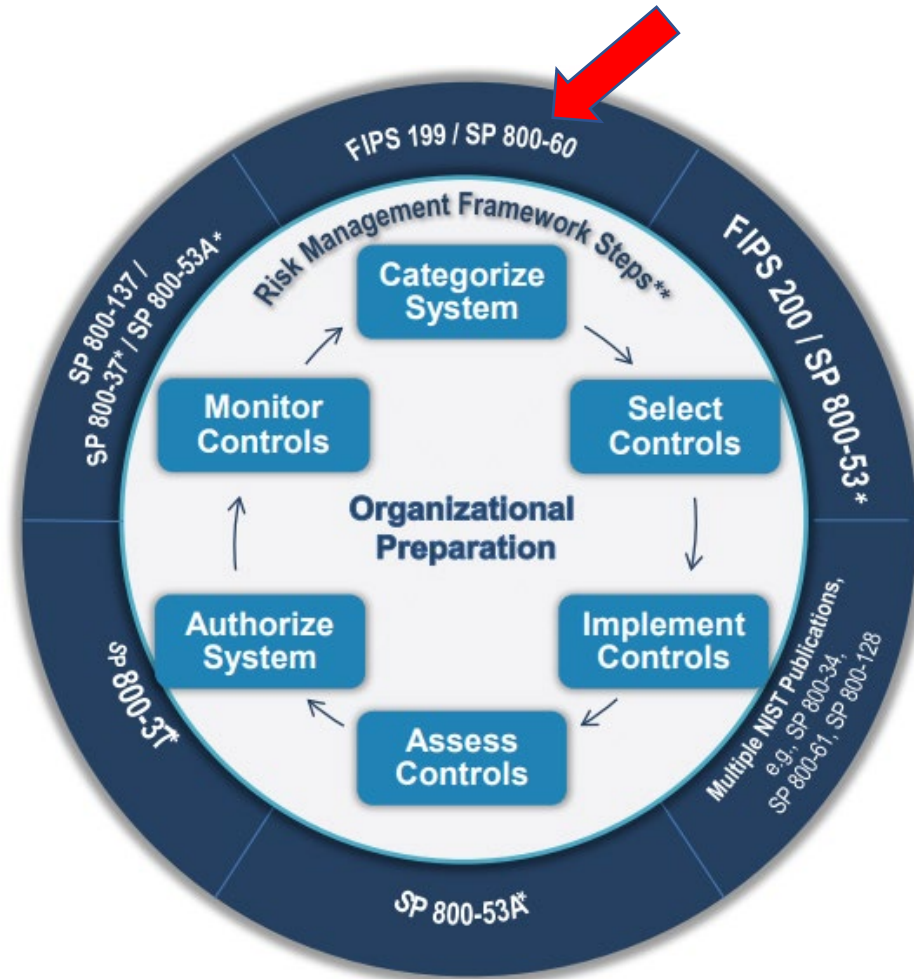
Agenda

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

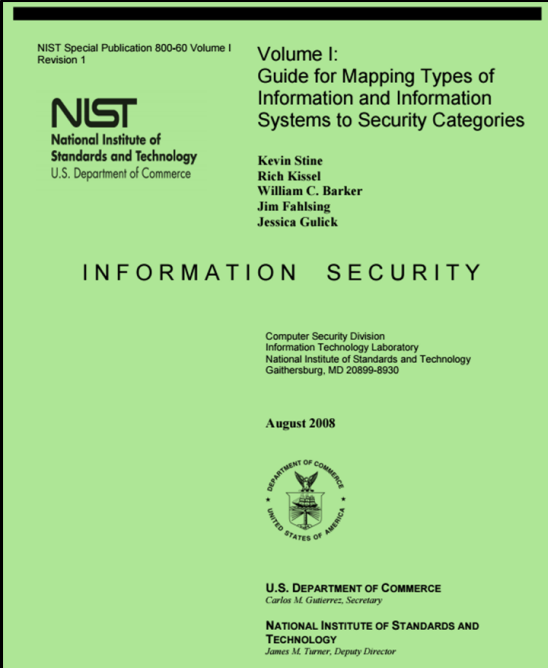
NIST Risk Management Framework



A guide for provisional security categorization



Found at NIST and on the [Lecture Materials page](#) of the MIS Community website



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

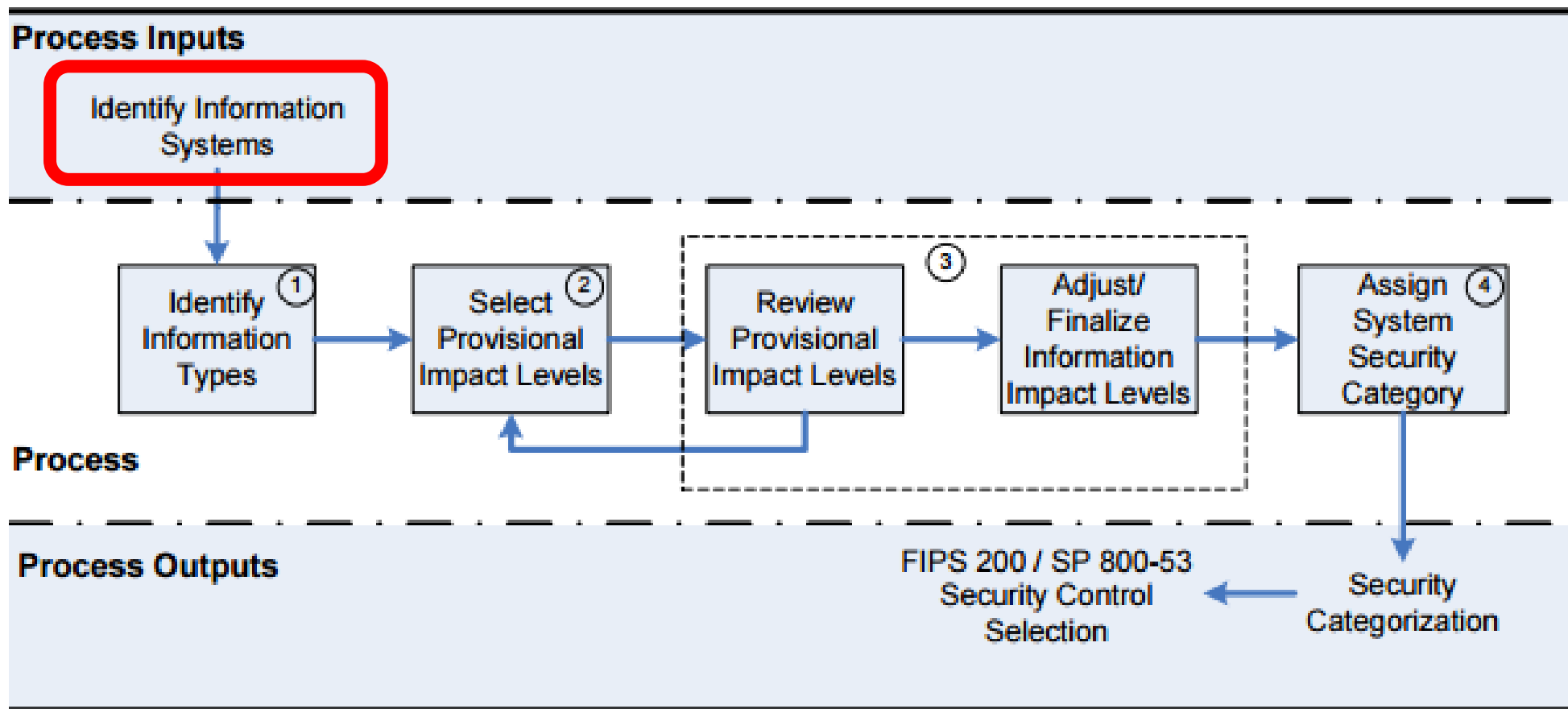


Figure 2: SP 800-60 Security Categorization Process Execution

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

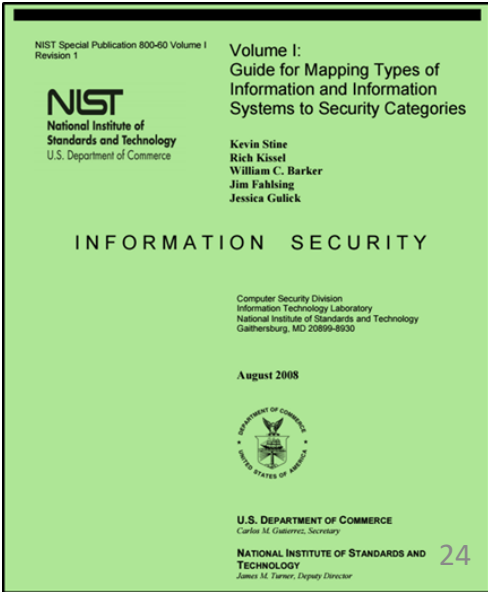
Disaster Management Information Types

Table 4: Mission-Based Information

| Mission Areas and Information | |
|---|--|
| <p>D.1 Defense & National Security Strategic National & Theater Defense Operational Defense Tactical Defense</p> <p>D.2 Homeland Security Border and Transportation Security Key Asset and Critical Infrastructure Protection Catastrophic Defense <i>Executive Functions of the Executive Office of the President (EOP)</i></p> <p>D.3 Intelligence Operations Intelligence Planning Intelligence Collection Intelligence Analysis & Production Intelligence Dissemination Intelligence Processing</p> <p>D.4 Disaster Management Disaster Monitoring and Prediction Disaster Preparedness and Planning Disaster Repair and Restoration Emergency Response</p> <p>D.5 International Affairs & Commerce Foreign Affairs International Development and Humanitarian Aid Global Trade</p> <p>D.6 Natural Resources Water Resource Management Conservation, Marine and Land Management Recreational Resource Management and Tourism Agricultural Innovation and Services</p> | <p>D.7 Energy Energy Supply Energy Conservation and Efficiency Energy Resource Management Energy Production</p> <p>D.8 Environmental Environmental Monitoring Forecasting Environmental Remediation Pollution Prevention and Control</p> <p>D.9 Economic Development Business and Industry Intellectual Property Financial Sector Oversight Industry Sector Income Stabilization</p> <p>D.10 Community & Social Services Homeownership Promotion Community and Regional Development Social Services Postal Services</p> <p>D.11 Transportation Ground Transportation Water Transportation Air Transportation Space Operations</p> <p>D.12 Education Elementary, Secondary, and Vocational Education Higher Education Cultural and Historic Preservation Cultural and Historic Exhibition</p> <p>D.13 Workforce Management Training and Employment Labor Rights Management Worker Safety</p> |
| | <p>D.16 Law Enforcement Criminal Apprehension Criminal Investigation and Surveillance Citizen Protection Leadership Protection Property Protection Substance Control Crime Prevention <i>Trade Law Enforcement</i></p> <p>D.17 Litigation & Judicial Activities Judicial Hearings Legal Defense Legal Investigation Legal Prosecution and Litigation Resolution Facilitation</p> <p>D.18 Federal Correctional Activities Criminal Incarceration Criminal Rehabilitation</p> <p>D.19 General Sciences & Innovation Scientific and Technological Research and Innovation Space Exploration and Innovation</p> |

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

| 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

6,993 Levee Systems 24,600 Miles of Levees 58 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

Search this list

Alabama

Alaska

American Samoa

Arizona

Arkansas

California

Colorado

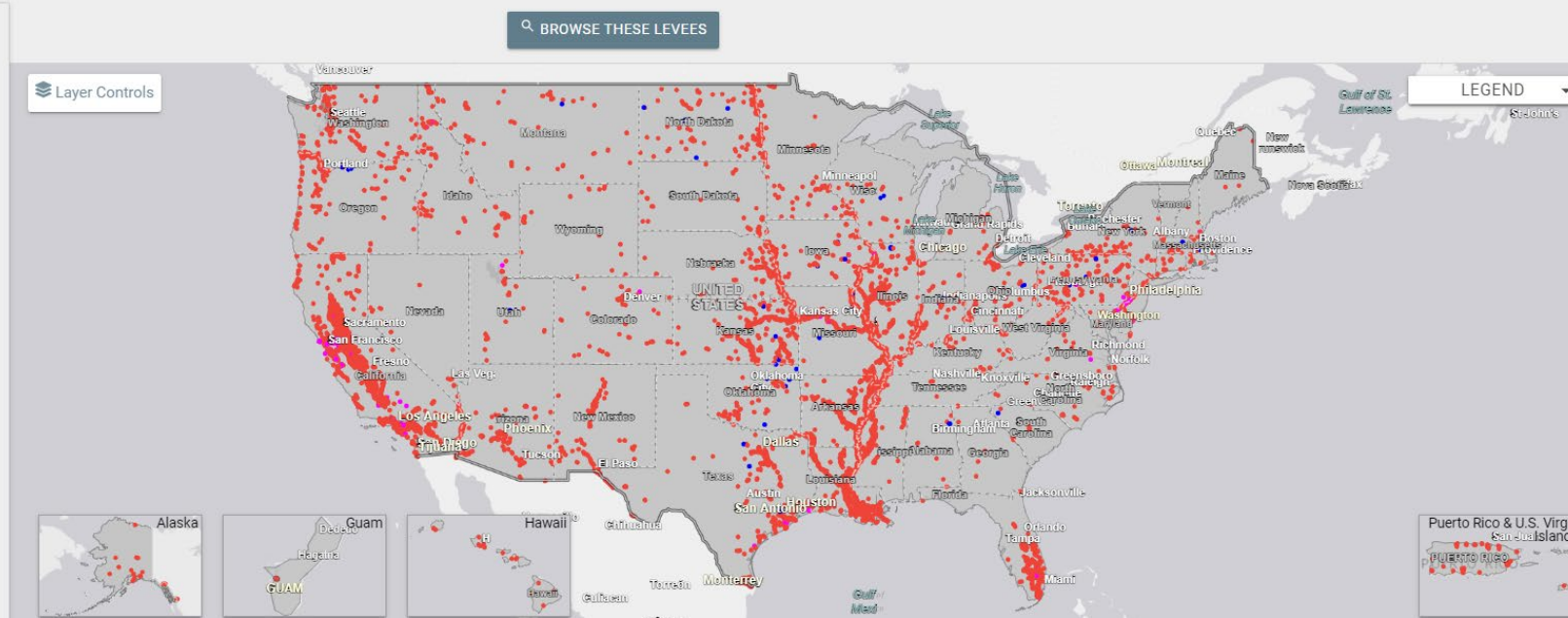
Commonwealth of the Northern Mariana Islands

Connecticut

Delaware

District of Columbia

Florida



[National Levee Database](#)



2. Select Provisional Impact Levels for the identified information system

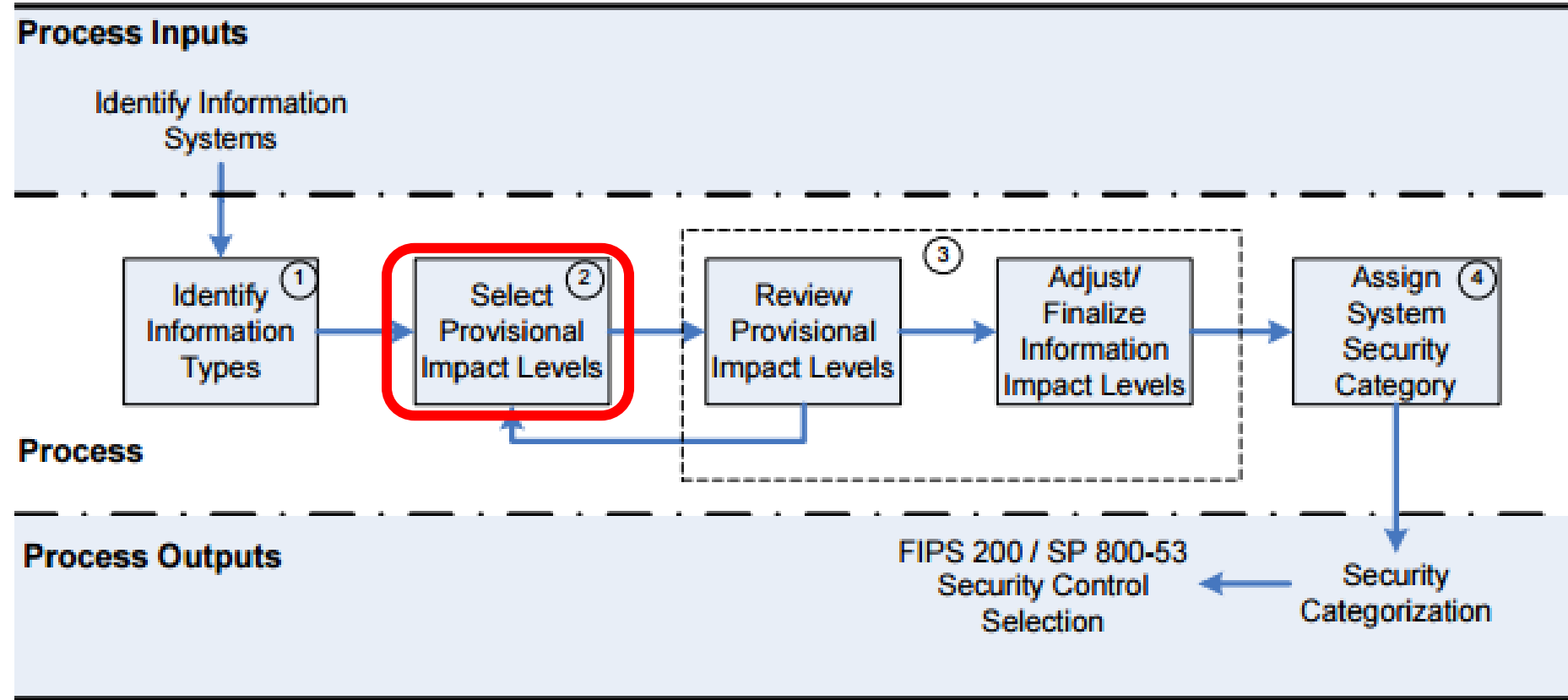


Figure 2: SP 800-60 Security Categorization Process Execution



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

| | |
|--|------------|
| APPENDIX D: IMPACT DETERMINATION FOR MISSION-BASED INFORMATION AND INFORMATION SYSTEMS..... | 102 |
| D.1 Defense and National Security | 107 |
| D.2 Homeland Security..... | 108 |
| D.2.1 Border and Transportation Security Information Type | 108 |
| D.2.2 Key Asset and Critical Infrastructure Protection Information Type..... | 110 |
| D.2.3 Catastrophic Defense Information Type | 111 |
| D.2.4 Executive Functions of the Executive Office of the President (EOP) Information Type | 112 |
| D.3 Intelligence Operations..... | 113 |
| D.4 Disaster Management | 115 |
| D.4.1 Disaster Monitoring and Prediction Information Type..... | 116 |
| D.4.2 Disaster Preparedness and Planning Information Type | 117 |
| D.4.3 Disaster Repair and Restoration Information Type | 118 |
| D.4.4 Emergency Response Information Type..... | 119 |

Disaster Management Information Impact

D.4 Disaster Management

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

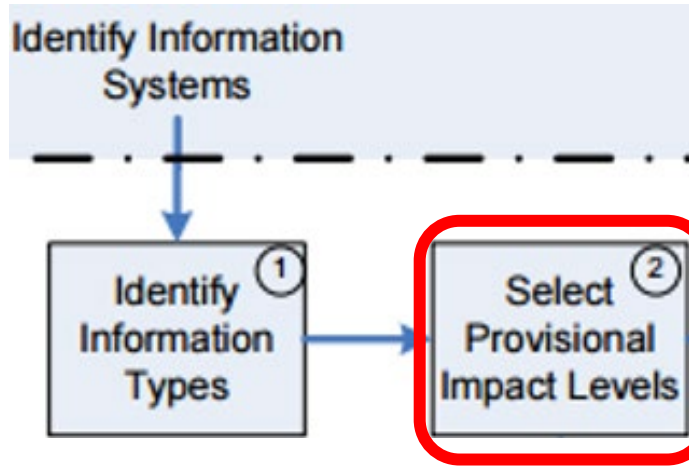
Exercise

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

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

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

Disaster Management Information Types



D.4.1 Disaster Monitoring and Prediction Information Type

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

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

D.4.2 Disaster Preparedness and Planning Information Type

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

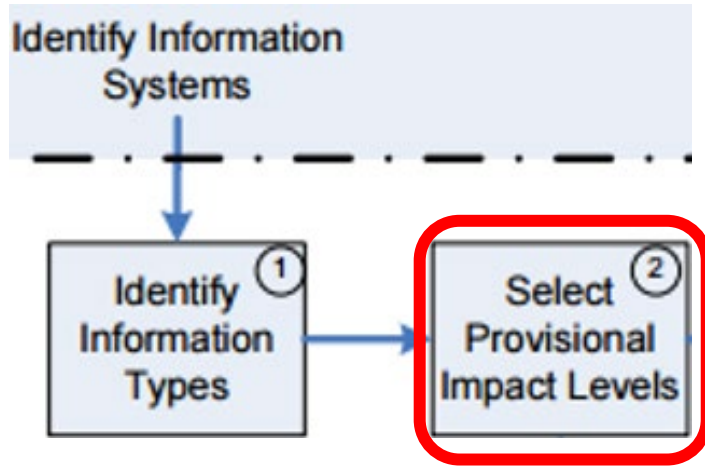
Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}

D.4.3 Disaster Repair and Restoration Information Type

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

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

Disaster Management Information Types



D.4.4 Emergency Response Information Type

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

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

Exercise

- *Determine the Summary Impact Levels for the Disaster Information Types*

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

Determine the Overall Impact Levels for the Disaster Information Types

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

Determine the overall security categorization of a Disaster Information System

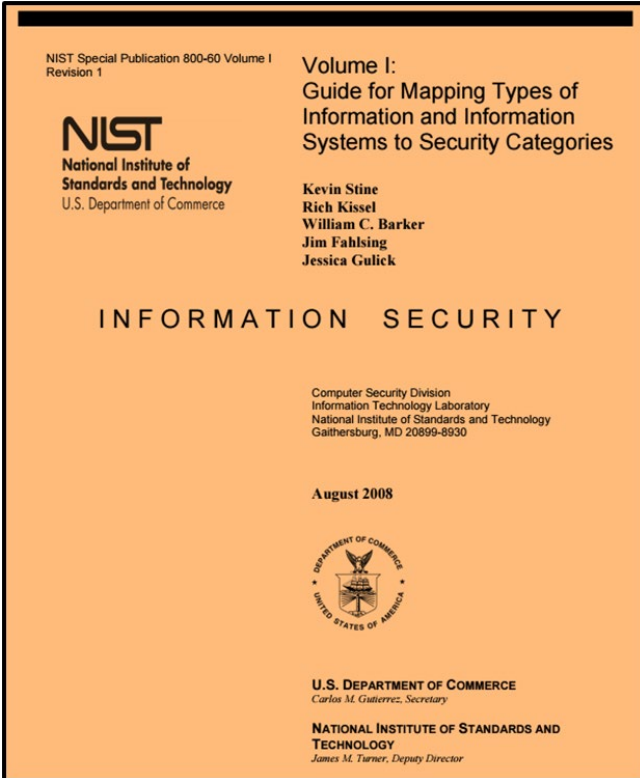
| Disaster Management Information Systems | | | | |
|--|-----------------|-----------|--------------|----------------------|
| Information Types | Confidentiality | Integrity | Availability | Summary Impact Level |
| Disaster Monitoring and Prediction | Low | High | High | High |
| Disaster Preparedness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

Determine the overall security categorization of a Disaster Information System

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

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

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



Once categorized, select security control baseline for the information system

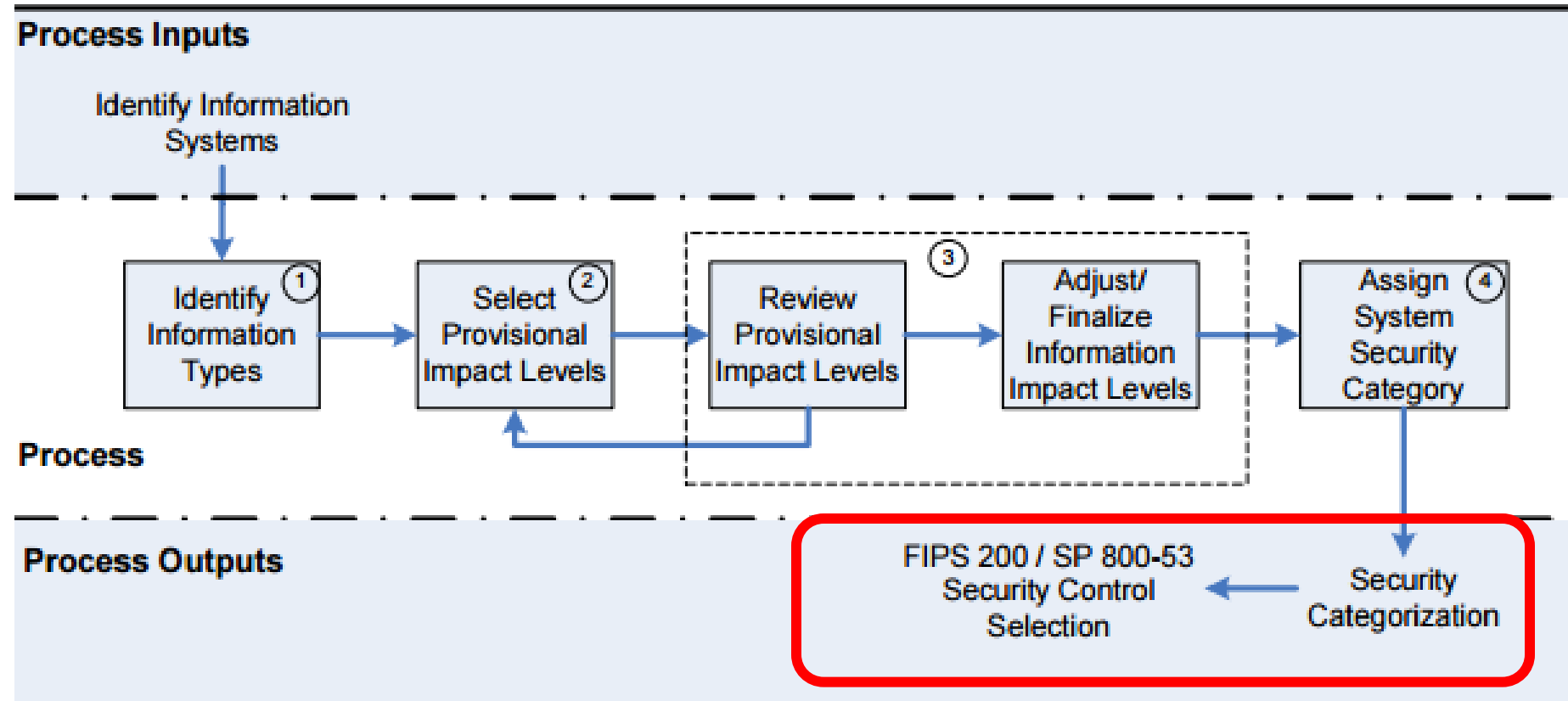
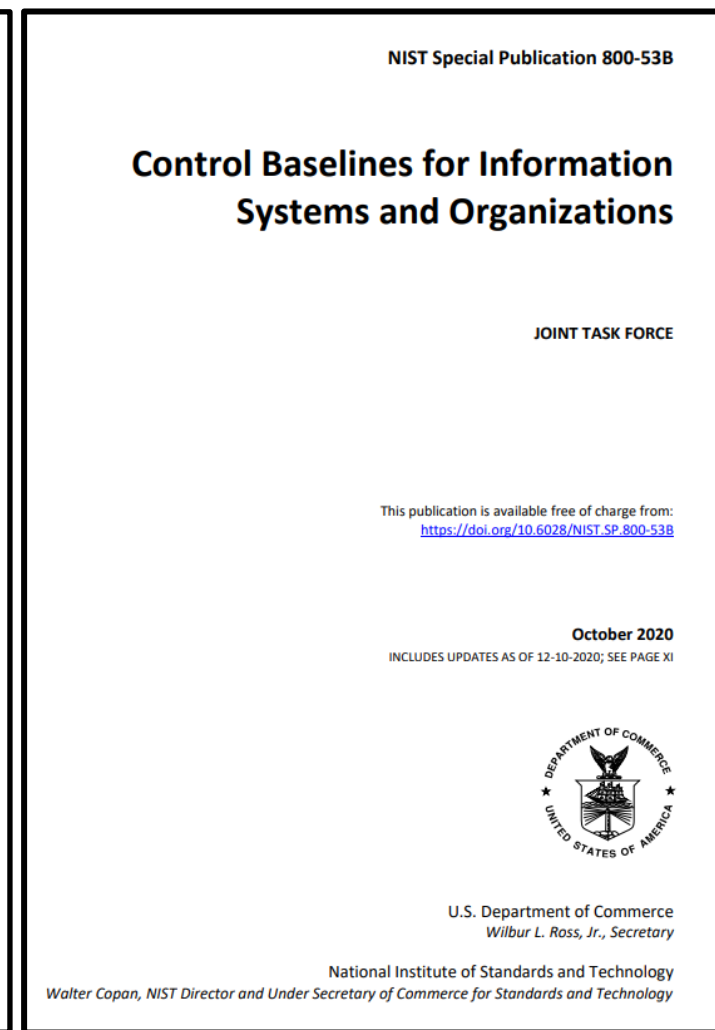
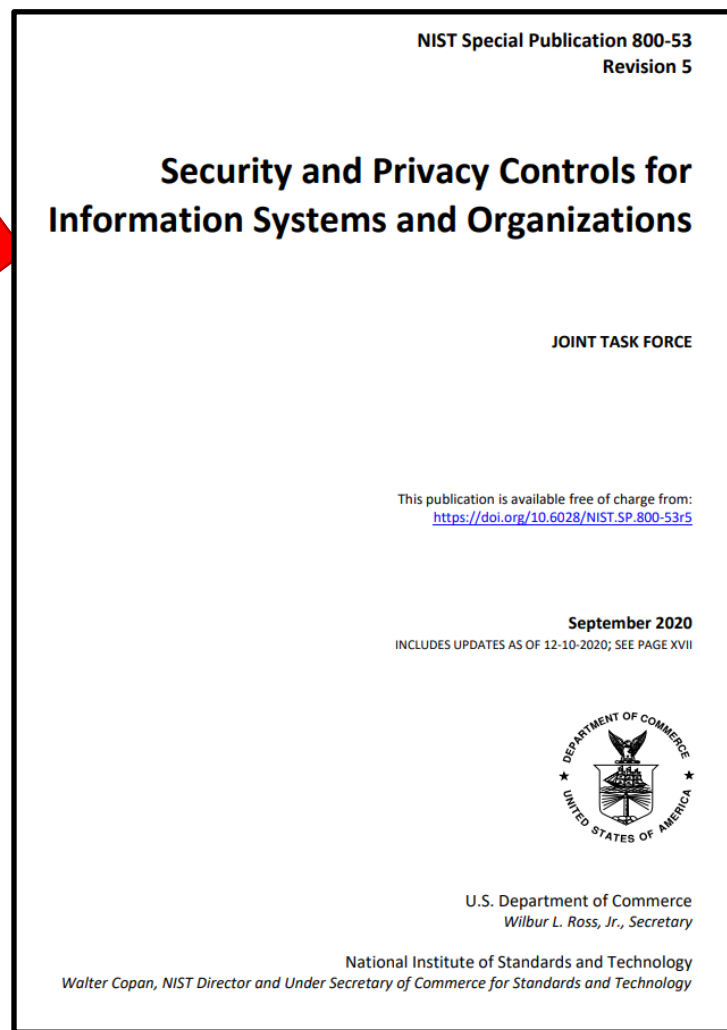
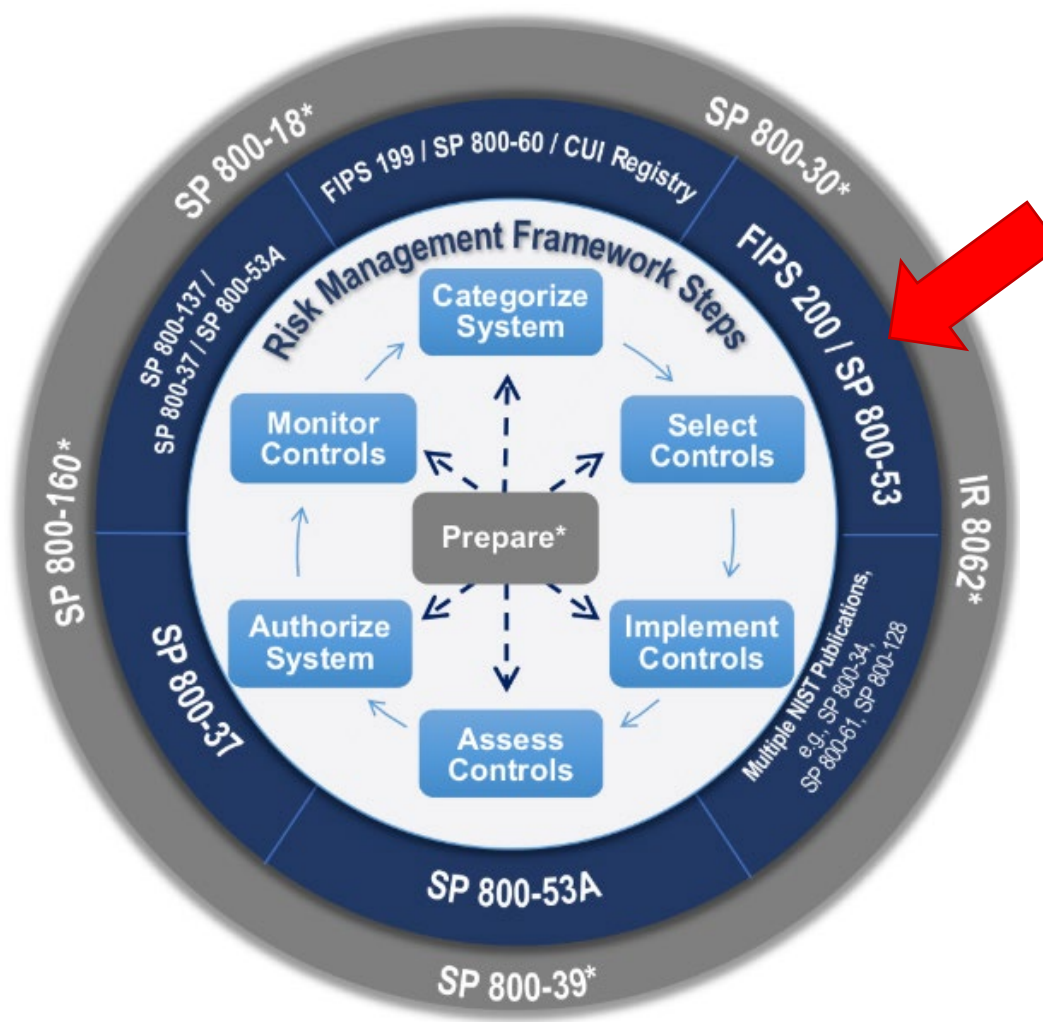
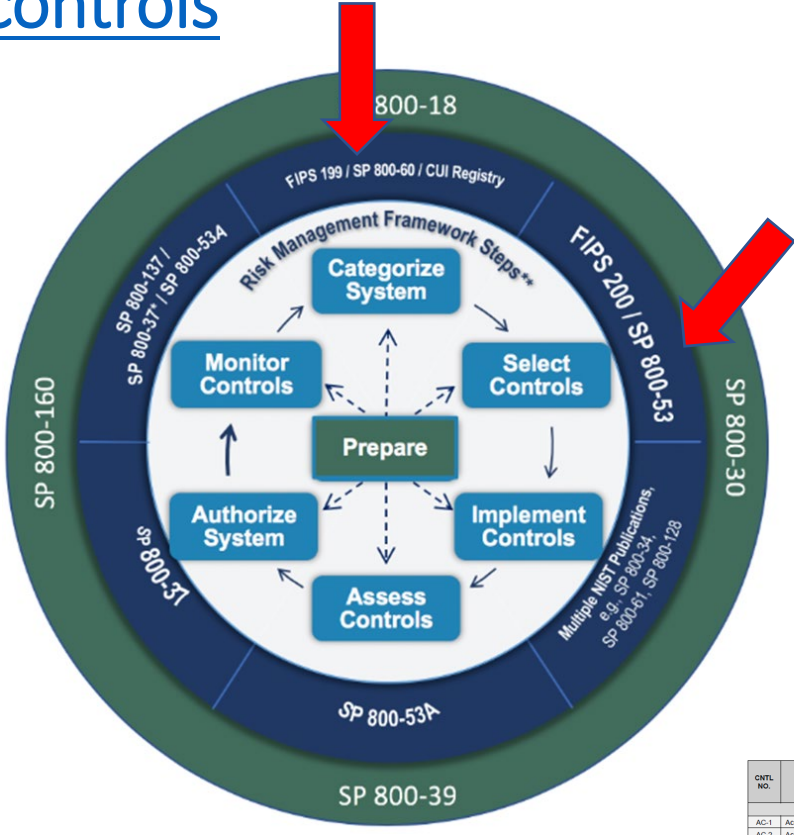


Figure 2: SP 800-60 Security Categorization Process Execution

Selecting cybersecurity risk controls



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



Disaster Management Information Systems

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

Table D-2: SECURITY CONTROL BASELINES

| 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 | AT-4 |
| AT-5 | Withdrawn | --- | --- | --- | --- |
| 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 |
| 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 |
| 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) |

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

Agenda

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

Milestone 1 – Risk Assessment Report

[Milestone 1 Assignment](#) is found in Canvas

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

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

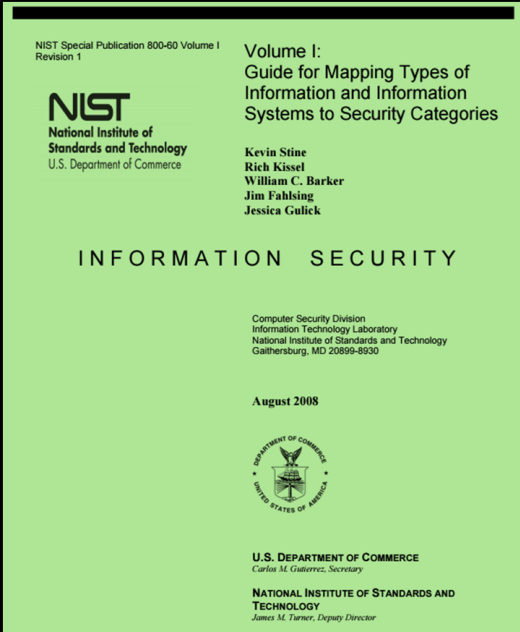
Your risk assessment assignment requires that you introduce and discuss:

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

How should you proceed in getting started with Milestone 1 ?

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

[NIST SP800-60V2R1: "Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories"](#)



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

[NIST SP800-60V1R1: “Guide for Mapping Types of Information and Information Systems to Security Categories”](#)

- 1. Mission-based Information & Information Systems**
- 2. Management and Support Information & Information Systems**
 - i. Services Delivery Support Functions**
 - ii. Resource Management Functions**

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

[NIST SP 800-60 Volume II Revision 1, Volume II: “Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories”](#)

Agenda

- ✓ National Institute of Standards and Technology (NIST)
 - ✓ Cybersecurity Framework
 - ✓ Risk Management Framework
- ✓ Applying the NIST Risk Management Framework
- ✓ Milestone 1 Assignment