

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

Risk Evaluation

Agenda

- Risk Evaluation
- Categorizing Information for IT Risk Management
- Using Categorization to Select a Baseline of Security Controls
- 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”

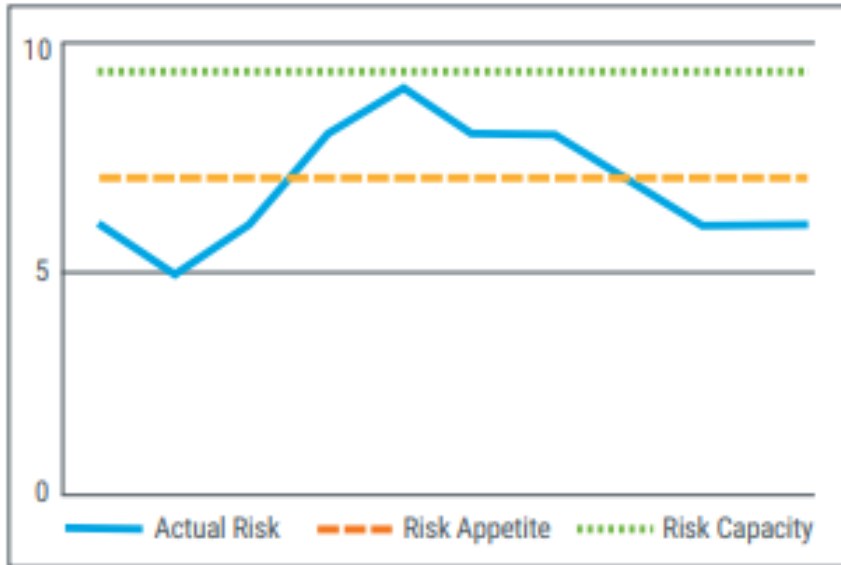


Diagram show a relatively sustainable situation

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

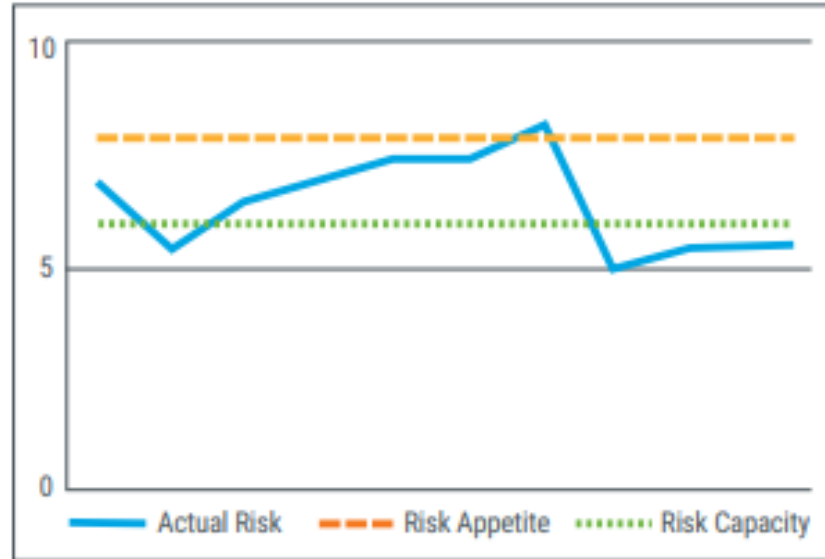
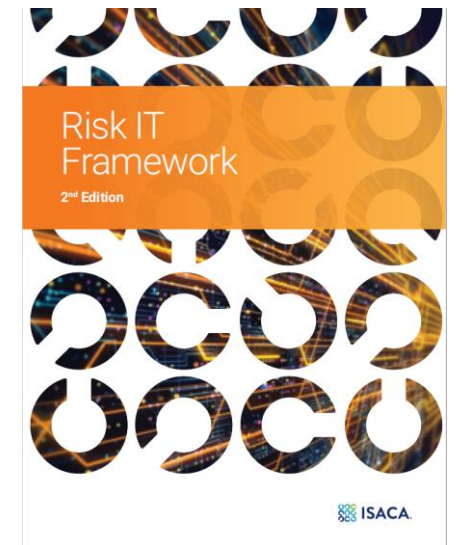


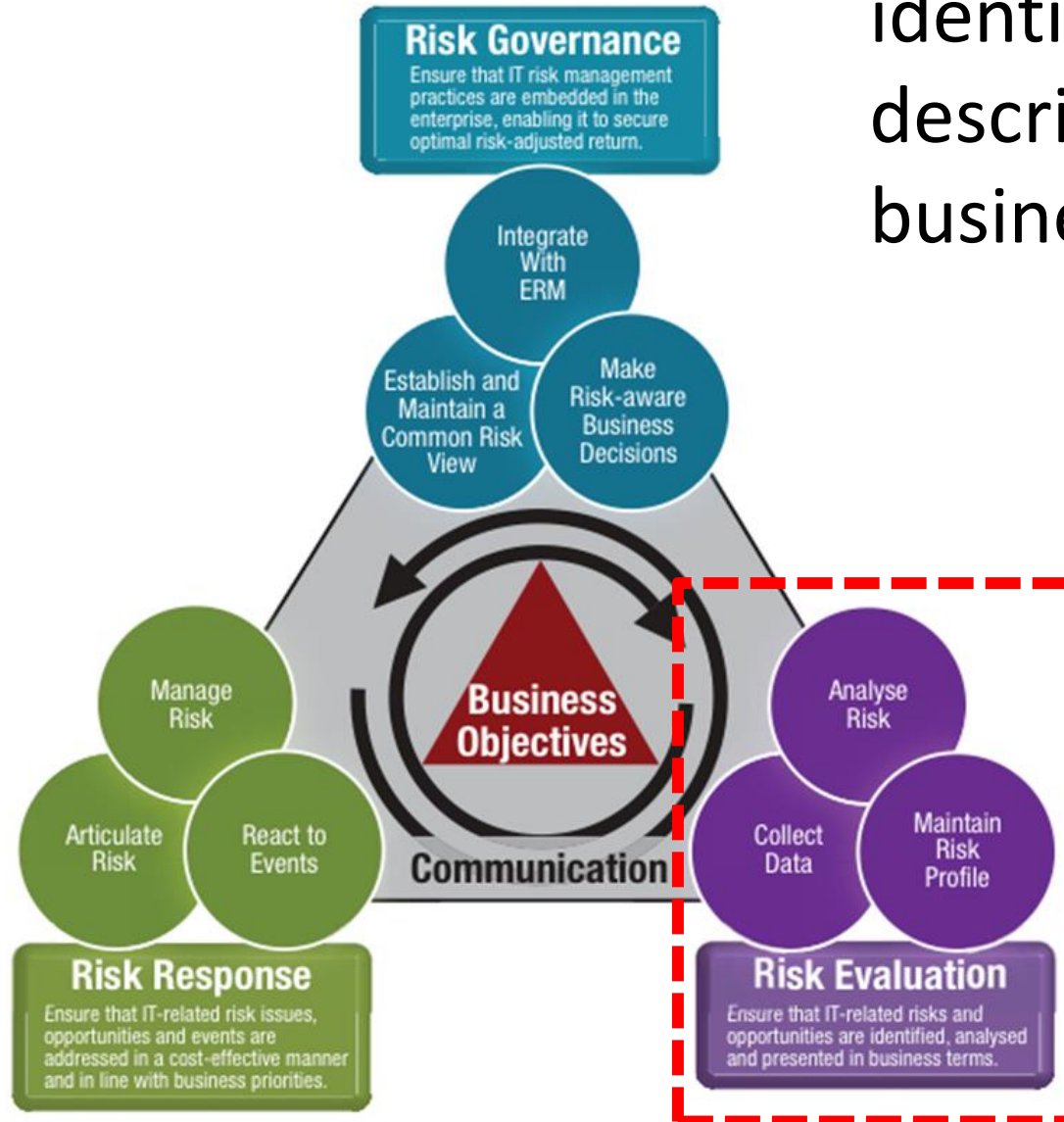
Diagram show an unsustainable situation

- 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



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

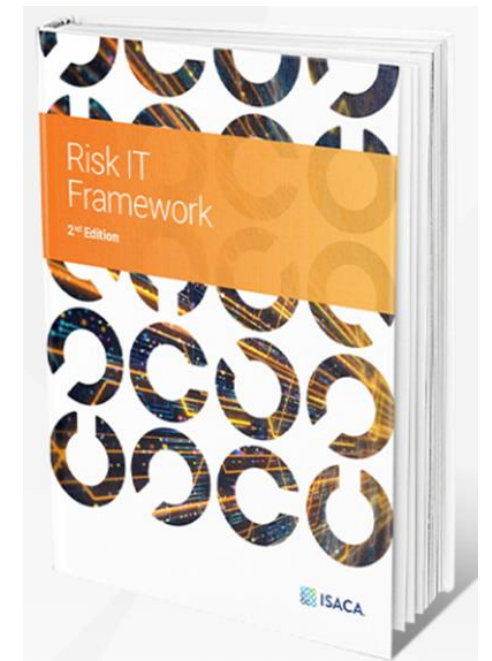
Maintain and up-to-date and complete inventory of known risks and attributes as understood in the context of IT controls and business processes

Risk Evaluation - Collect Data

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

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

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

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. In written, stored electronically, copied, transmitted, or otherwise disseminated to general business, information customers.

Information Classification

All information at the City is classified into four levels: public, sensitive, private, or confidential.

- **Public**—This information might not cause damage.
- **Sensitive**—This information requires protection to prevent inappropriate disclosure.
- **Private**—This information is for agency use and the public trust placed in the agency.
- **Confidential**—This is the highest level of protection. It is information whose disclosure could cause damage to the agency's ability to provide services, contain information whose disclosure could be a danger to public safety, or lead to the loss of a competitive advantage.

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.

Analyze Risk

MANAGEMENT GUIDELINES—RE2



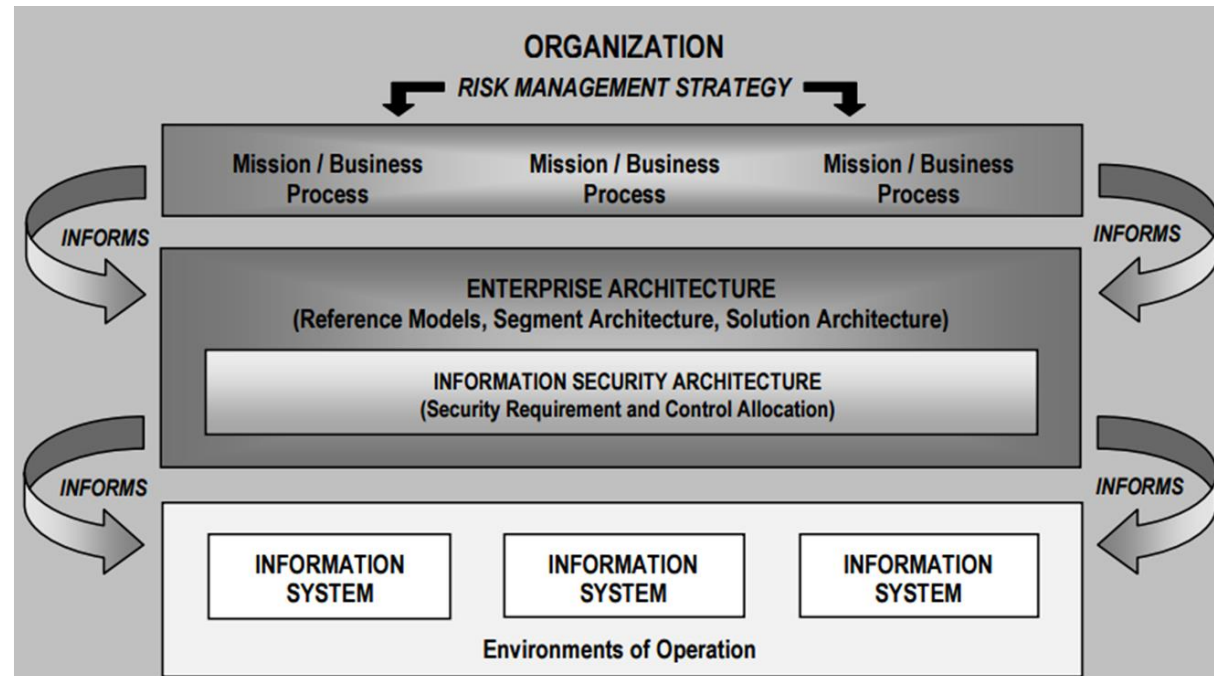
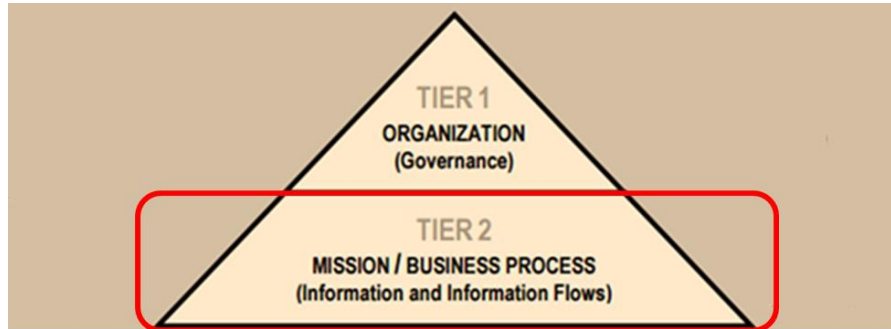
RACI Chart

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's general business, information systems, employees, business partners, or customers.

Information Classification

All information at the City and corresponding agencies will be classified at one of 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.

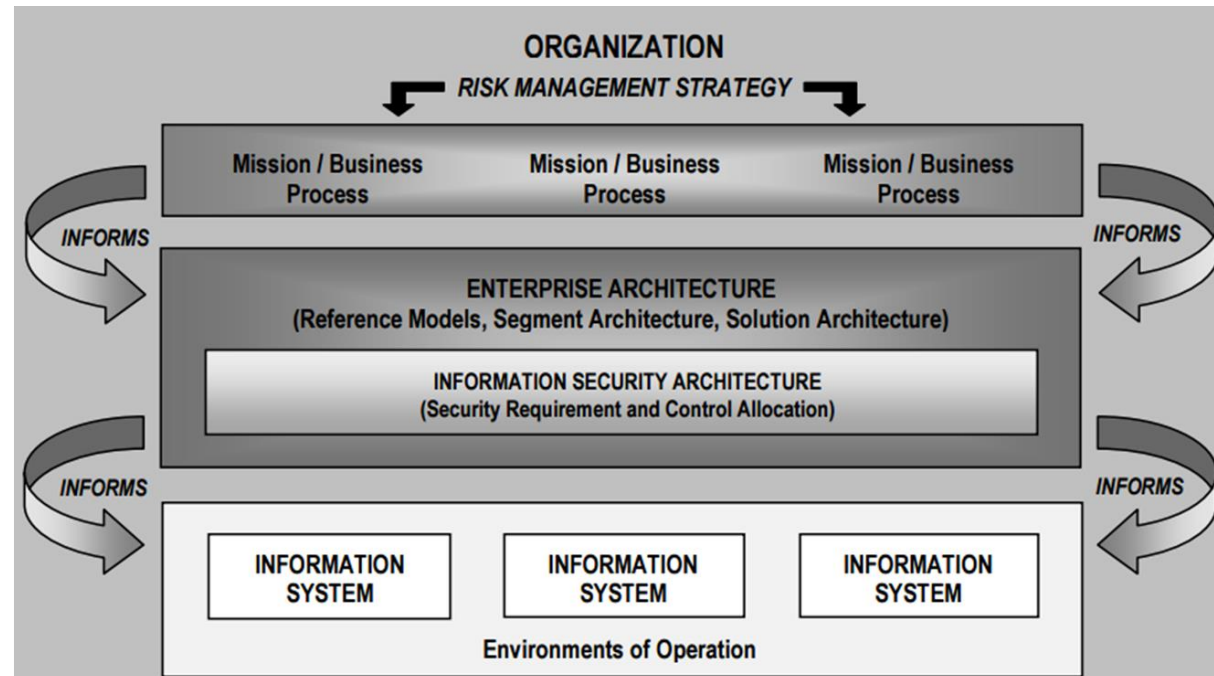
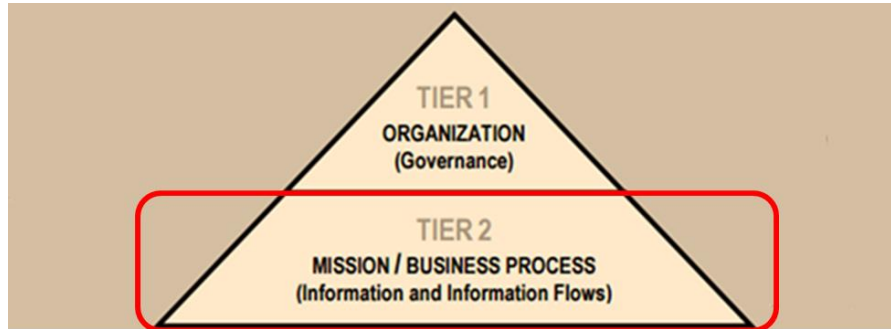
Information Valuation and Categorization

- 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.

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	Risk Control Functions	HR	Compliance and Audit
RE3.1 Map IT resources to business processes.			I	R			C	A/R	C		I
RE3.2 Determine business criticality of IT 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	C

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

Data Steward

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

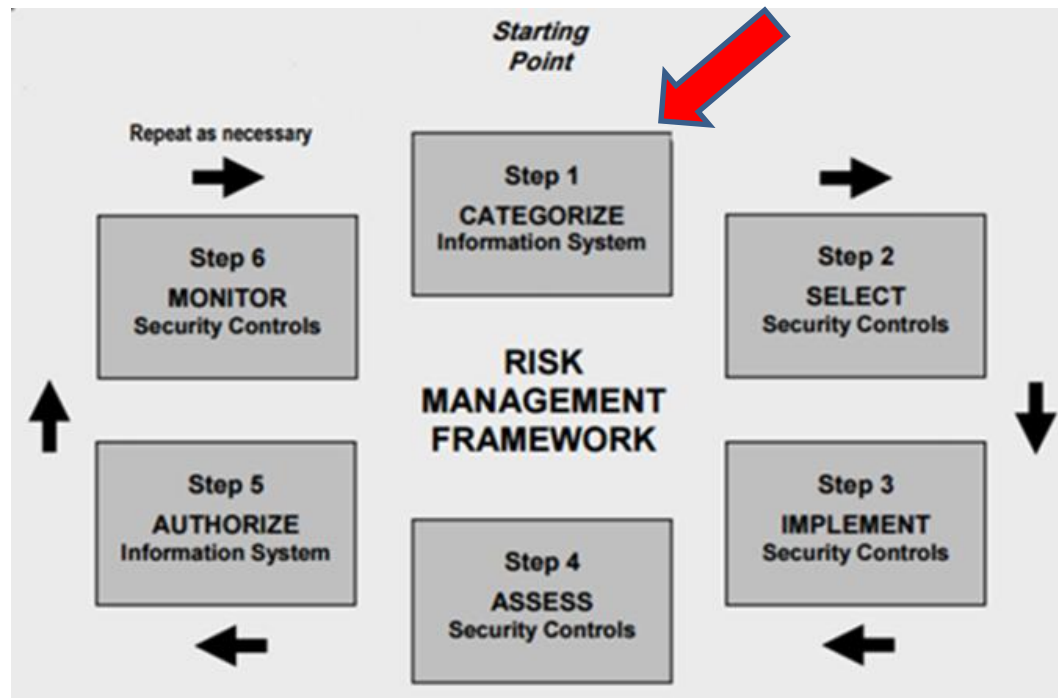
Information Categorization is part of Risk Evaluation



Why is data categorization important?

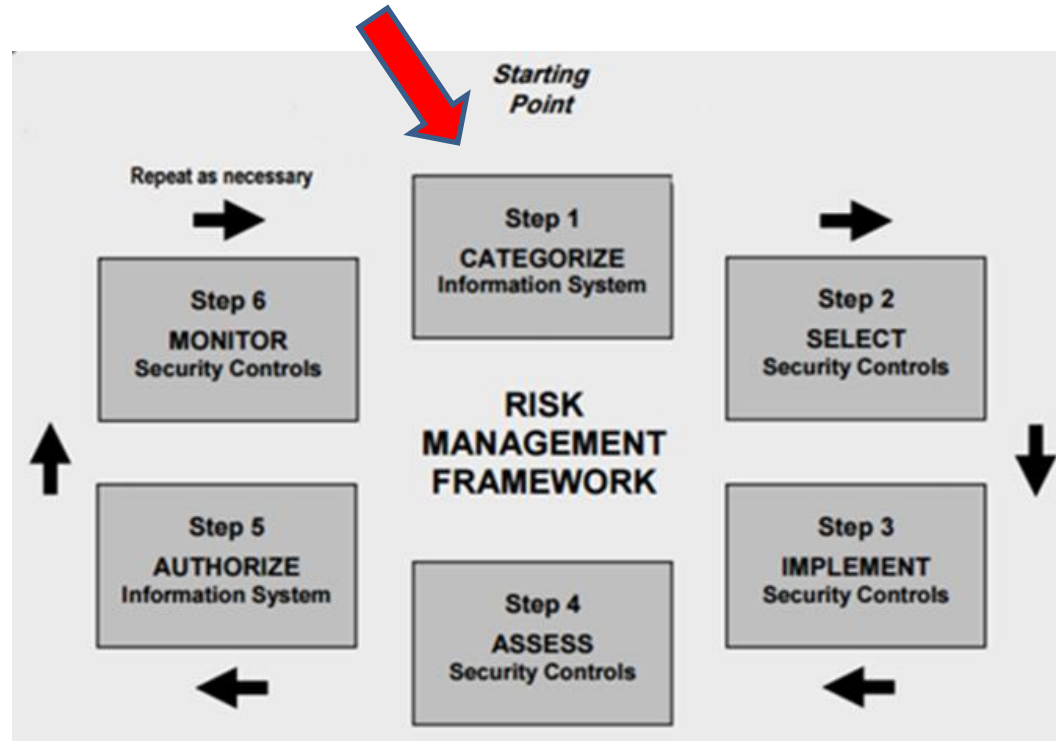
- It focuses attention on the identification and valuation of information assets
- It is the basis for access and other control policies and processes

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



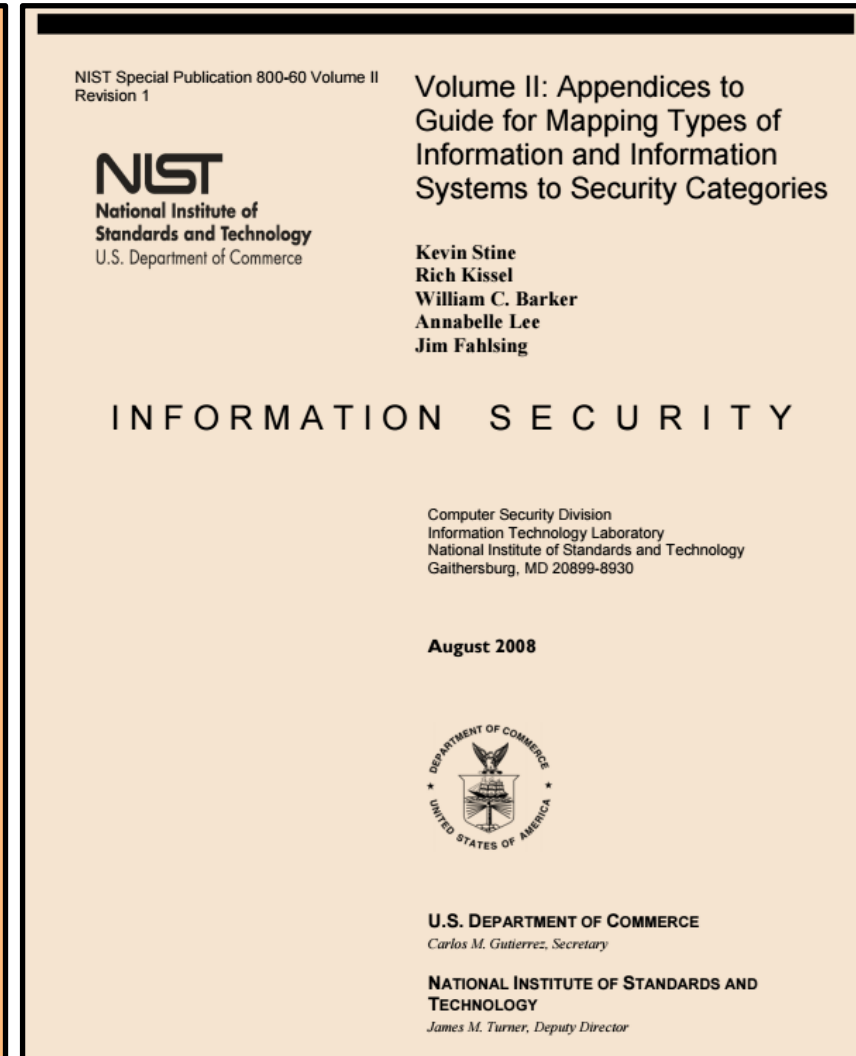
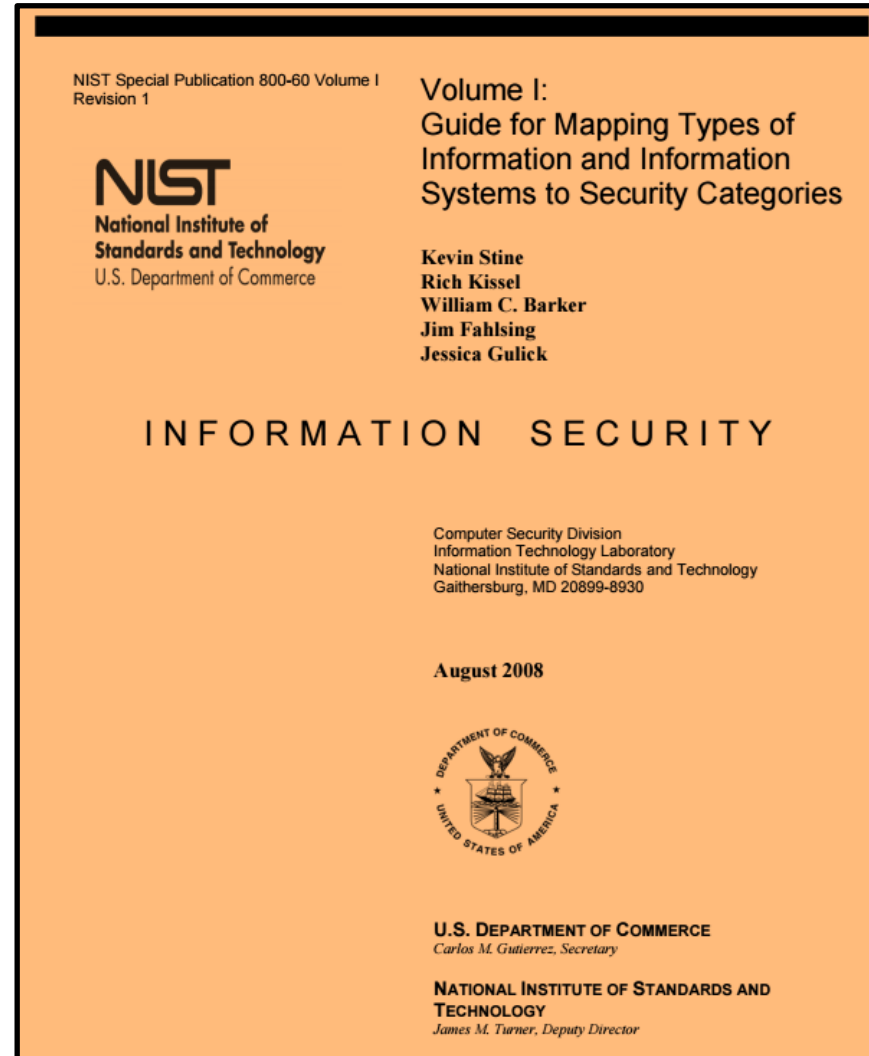
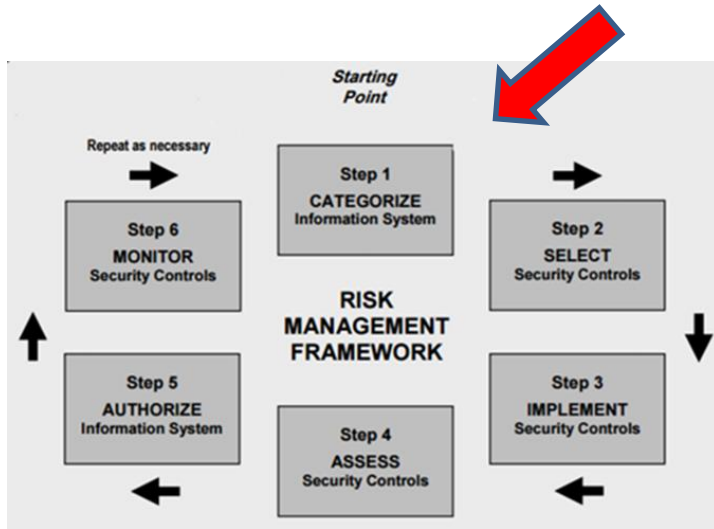
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		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.CO	Communications
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Categorizing Information and Information Systems

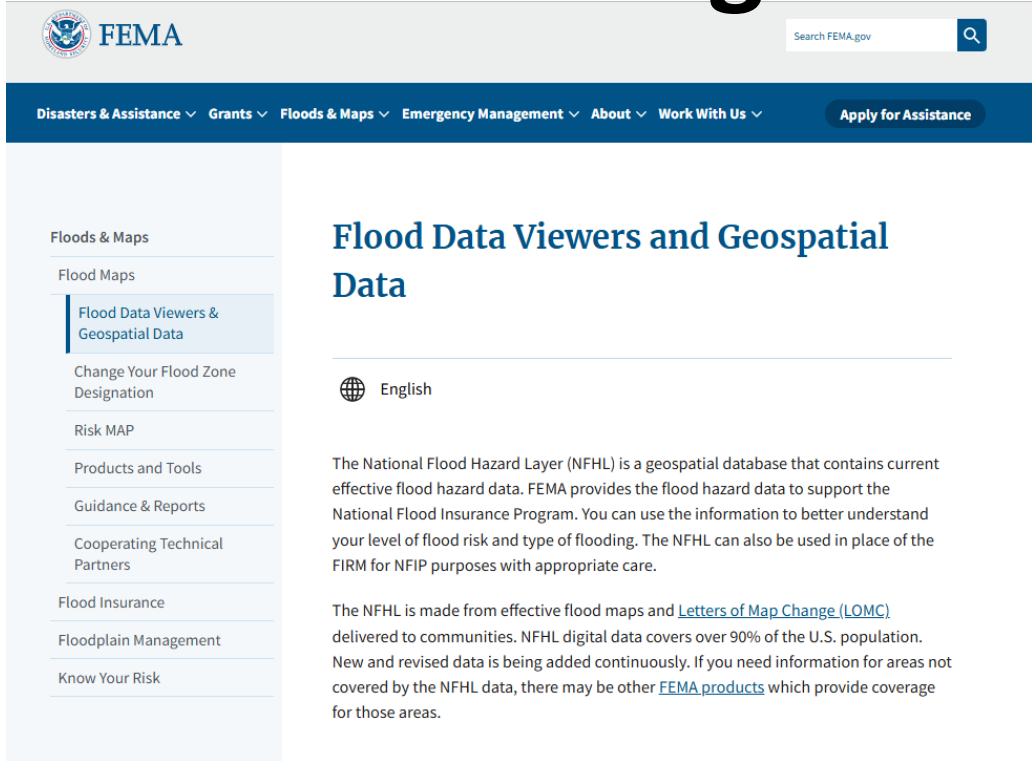


	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
<p>Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]</p>	The unauthorized disclosure of information could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

A guideline for helping categorize Information and Information Systems



Disaster Management Information System Example



The screenshot shows the FEMA website's navigation menu and a sidebar. The main content area is titled "Flood Data Viewers and Geospatial Data" and includes a language selector set to "English". Below this, there is a paragraph describing the National Flood Hazard Layer (NFHL) as a geospatial database containing current effective flood hazard data. A second paragraph explains that the NFHL is derived from effective flood maps and Letters of Map Change (LOMC) and covers over 90% of the U.S. population. A sidebar on the left lists various categories under "Floods & Maps", with "Flood Data Viewers & Geospatial Data" highlighted.

Accessing the National Flood Hazard Layer

Map Service Center

Access localized National Flood Hazard Layer data by searching FEMA's Map Service Center.

[FEMA's Map Service Center](#)

NFHL Interactive Viewer

Or you may view, download, and print current local digital effective flood hazard data in an interactive map.

[NFHL Viewer](#)

In the [NFHL Viewer](#), you can use the address search or map navigation to locate an area of interest and the NFHL Print Tool to download and print a full Flood Insurance Rate Map (FIRM) or FIRMette (a smaller, printable version of a FIRM) where NFHL data exists. Technical GIS users can also utilize a series of dedicated GIS web services that allow the NFHL database to be incorporated into websites and GIS applications. For more information on available services, go to the [NFHL GIS Services User Guide](#).



[NFHL Viewer](#)

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

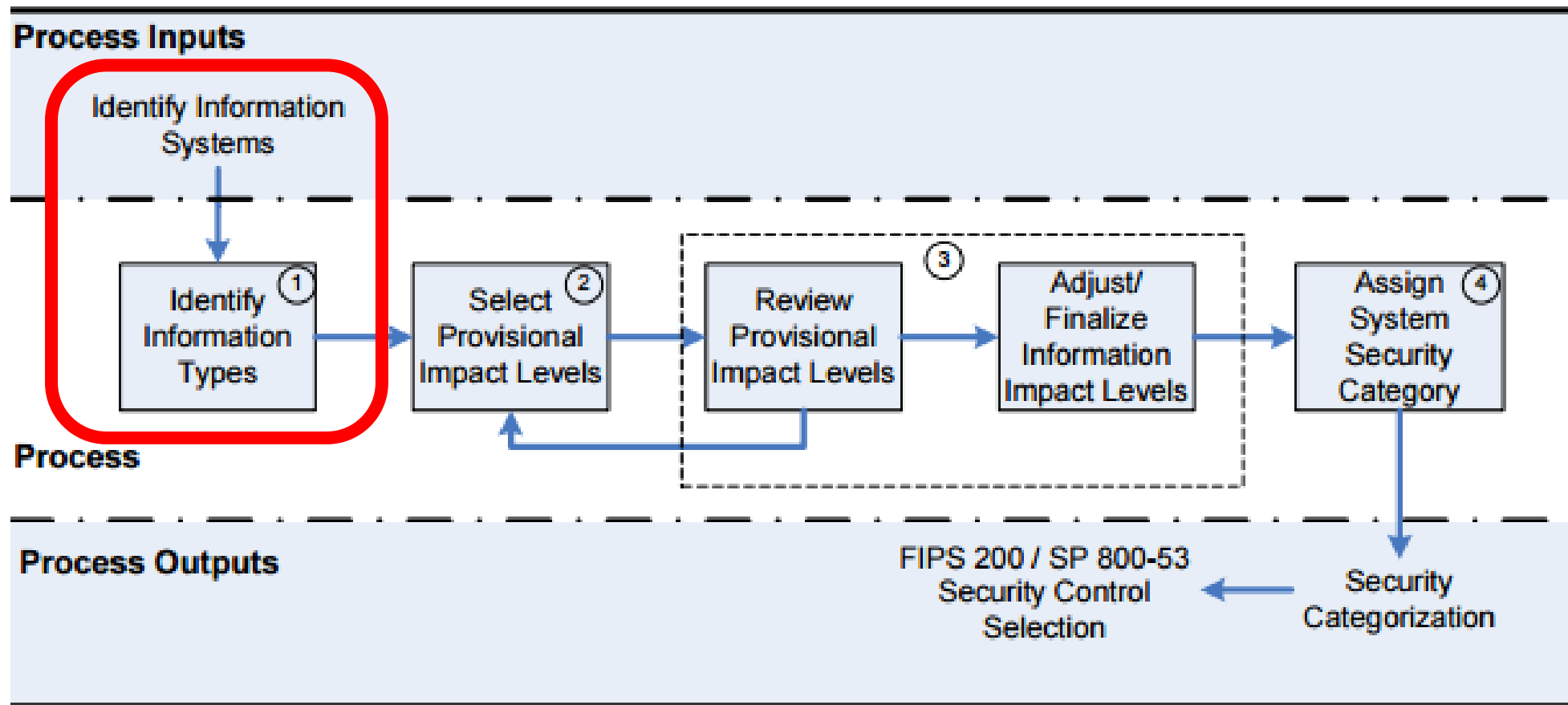
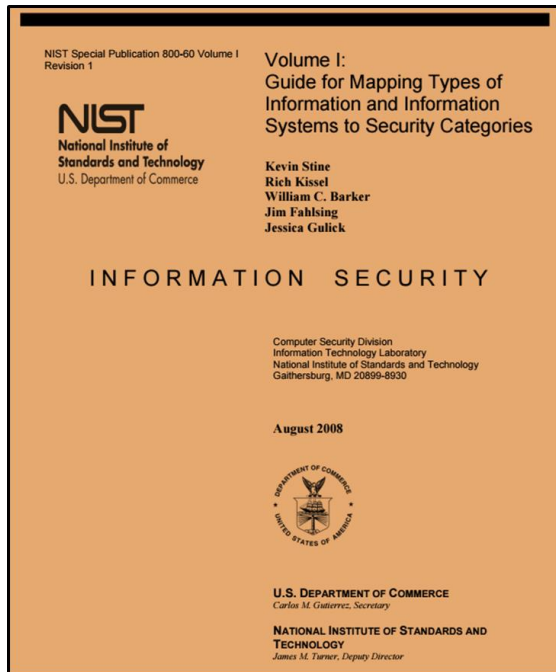


Figure 2: SP 800-60 Security Categorization Process Execution

Table 4: Mission-Based Information Types and Delivery Mechanisms¹⁴

Mission Areas and Information Types [Services for Citizens]		
<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 Preparedness Energy Resource Management Energy Production</p> <p>D.8 Environmental Management Environmental Monitoring and Forecasting Environmental Remediation Pollution Prevention and Control</p> <p>D.9 Economic Development Business and Industry Development Intellectual Property Protection 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.14 Health Access to Care Population Health Mgmt & Consumer Safety Health Care Administration Health Care Delivery Services Health Care Research and Practitioner Education</p> <p>D.15 Income Security General Retirement and Disability Unemployment Compensation Housing Assistance Food and Nutrition Assistance Survivor Compensation</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>



2. Select Provisional Impact Levels for the identified information system

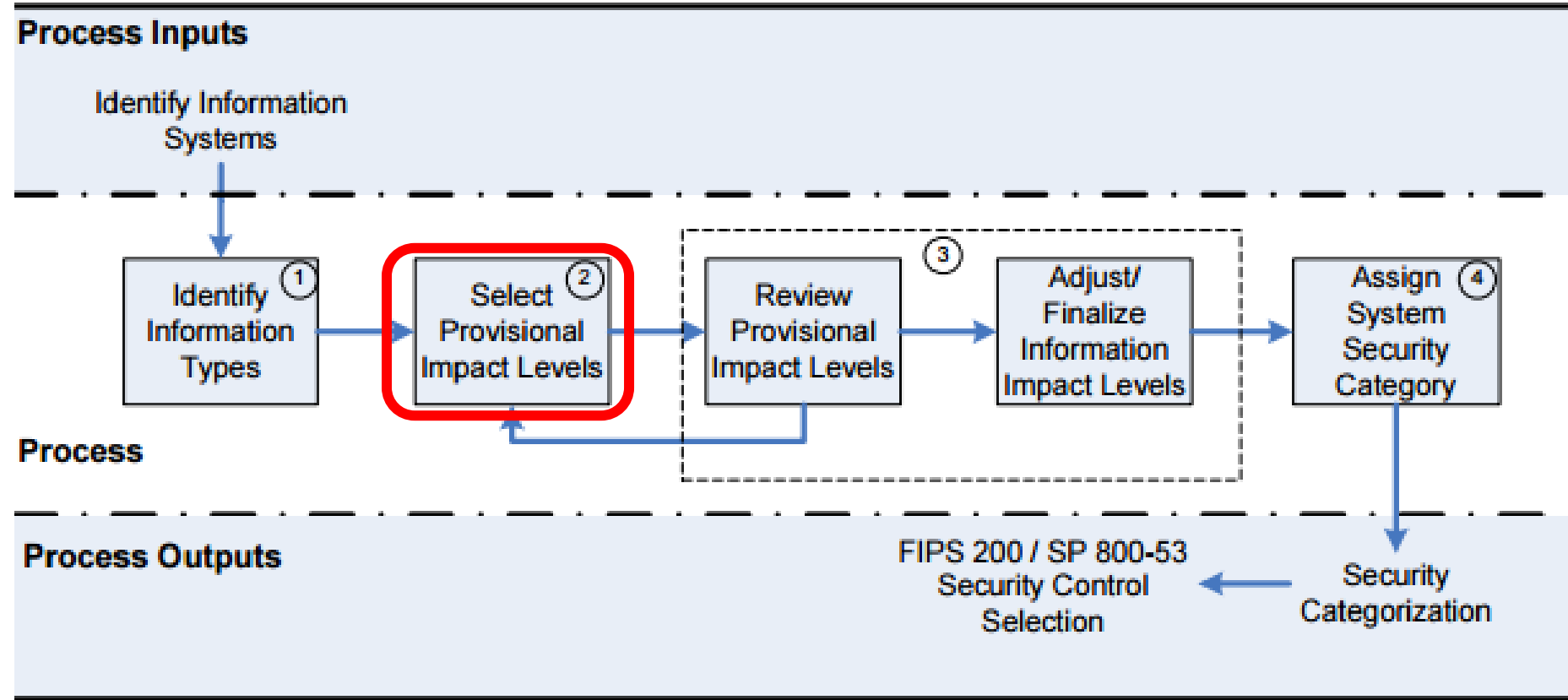


Figure 2: SP 800-60 Security Categorization Process Execution



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.4 Disaster Management115
D.4.1 Disaster Monitoring and Prediction Information Type.....116
D.4.2 Disaster Preparedness and Planning Information Type117
D.4.3 Disaster Repair and Restoration Information Type118
D.4.4 Emergency Response Information Type.....119

<https://community.mis.temple.edu/mis5206sec951summer2024/category/1c-risk-evaluation/>

Guideline for help in security categorization

Preliminary security categorizations for disaster information types and an information system that contains them...

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

<https://community.mis.temple.edu/mis5206sec951summer2024/category/1c-risk-evaluation/>

Determine the Security Categorizations of the Disaster Information System

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

Determine the Overall Security Categorization of the Disaster Information System

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

Overall Security Categorization of the Disaster Information System

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

Exercise

Using the Security Categorization Workbook create a preliminary risk assessment to discuss with managers of a company that own and depend on financial information contained in a financial management system

Financial management involves accounting practices and procedures that allow for accurate and effective handling of a business' revenues, funding, and expenditures.

A financial management information system supports the following 7 business functions and associated datasets:

- Accounting, Funds Control, Payments, Collections and Receivables, Asset and Liability Management, Reporting and Information, Cost Accounting/ Performance

Your risk assessment will be based on:

- Security objectives and potential impacts defined in FIPS 199: “Standards for Security Categorization of Federal Information and Information Systems”
- Provisional security categorizations for the financial management information types using NIST Special Publication 800-60 Volume II (see Wrap-Up post for this lesson in the course Website)
- Determination of an overall security categorization for the financial management information system based on the provisional security categorization of the 7 information types (from 3 above)

Agenda

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

Question:

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

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



Determine the overall information security categorization of the different datasets



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

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

Asset	Impact to			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	?

NIST SP 800-100 Information Security Handbook: A Guide for Managers (Chapter 10, page 90)

<https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-100.pdf>

Analyze risk to prioritize protection

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



The diagram shows three ovals: 'Likelihood' (green), 'Threat' (pink), and 'Impact' (blue). Arrows point from 'Likelihood' and 'Threat' to a central 'RISK' oval (pink), and from 'Vulnerability' (yellow) to 'RISK'. 'Impact' also has an arrow pointing to 'RISK'.

	Impact		
Threat Likelihood	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

NIST SP 800-100 Information Security Handbook: A Guide for Managers

<https://community.mis.temple.edu/mis5206sec951summer2023/files/2023/06/nistspecialpublication800-100.pdf>

Analyze risk to prioritize protection

Threat Likelihood	Impact		
	Low (10)	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

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 of the information must be assessed to Business information assets are those business services with integrity, comp

Scope

This policy applies to all information. It is written, stored electronically, copied, transmitted, or otherwise disseminated to general business, information, or customers.

Information Classification

All information at the City is classified into four levels: public, sensitive, private, or confidential.

- **Public**—This information might cause 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:

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

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
IT investigation:		\$ 200
Single Loss Expectancy:		\$22,200
Annualized Rate of Occurrence:	0.05	
Annual Loss Expectancy:		\$ 1,100

Risk management decision

Decision:

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

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

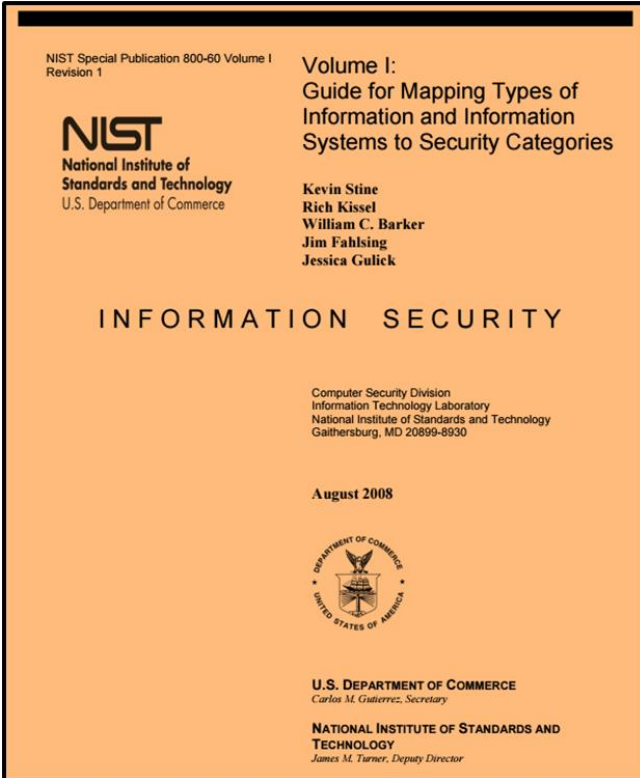
Annual Loss Expectancy Calculation

Credit Monitoring Service (1000 records):	\$15,000
Dean's Lost Productivity (assume \$300,000 salary):	
10 hours restoring data from various sources	\$ 3,000
10 hours re-doing lost work	\$ 3,000
Replacement Device:	\$ 1,000
<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



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

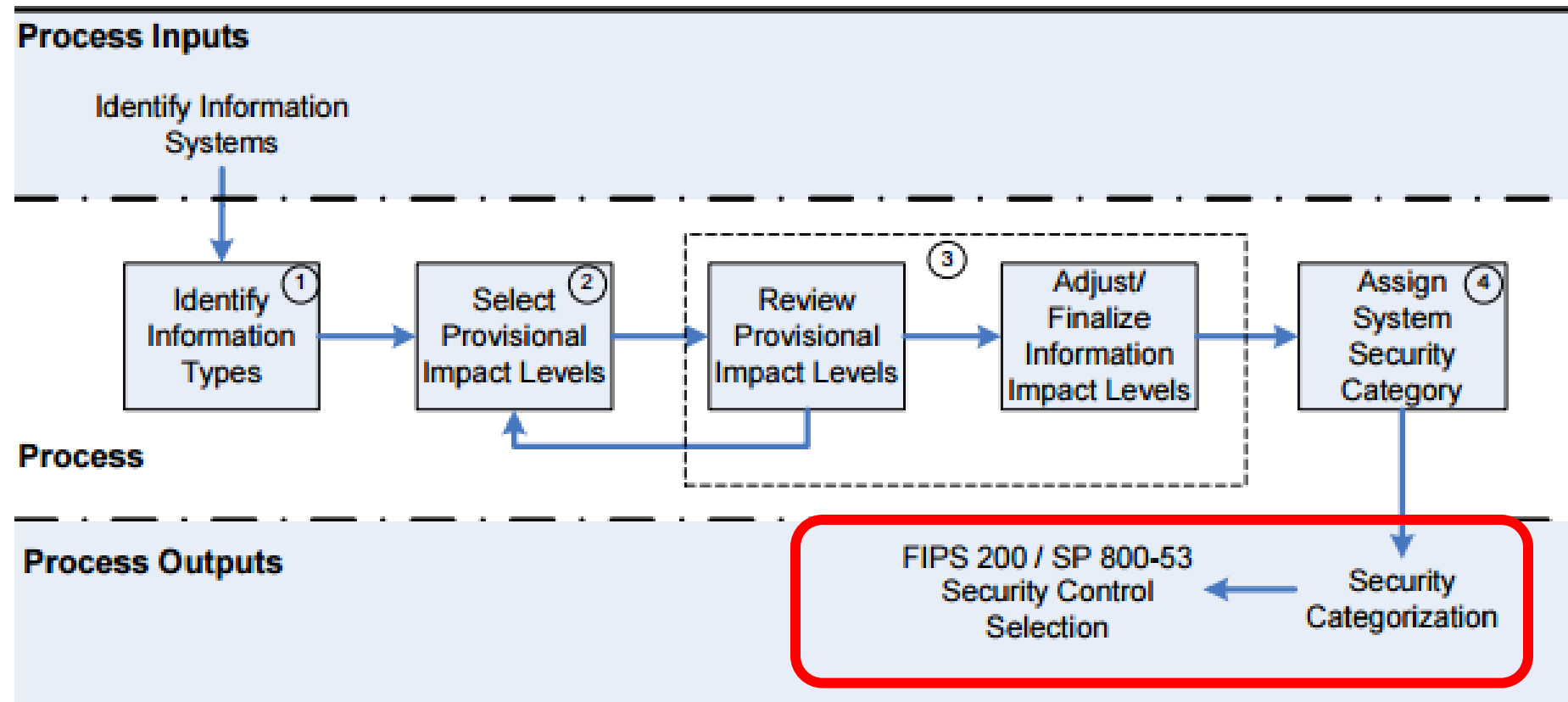
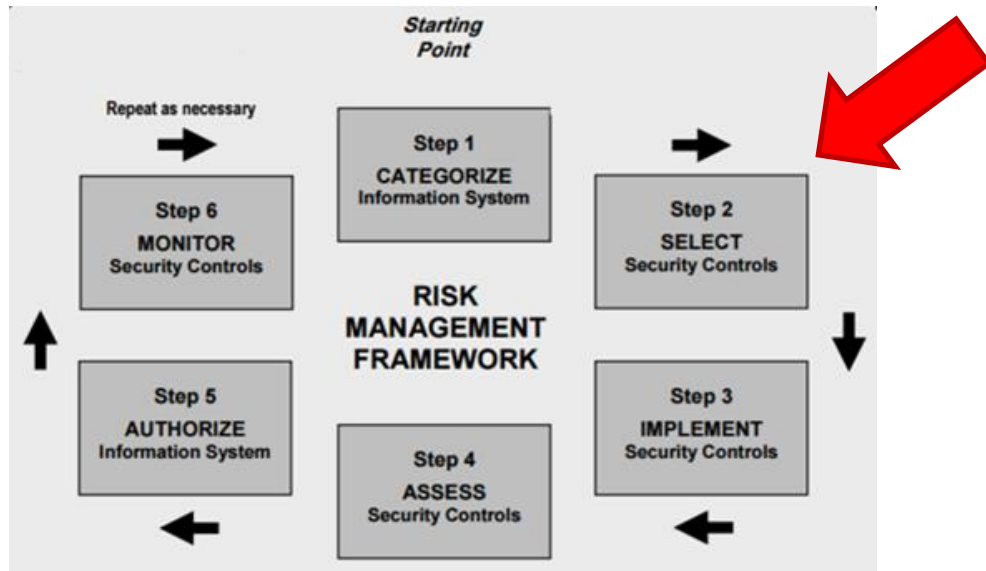


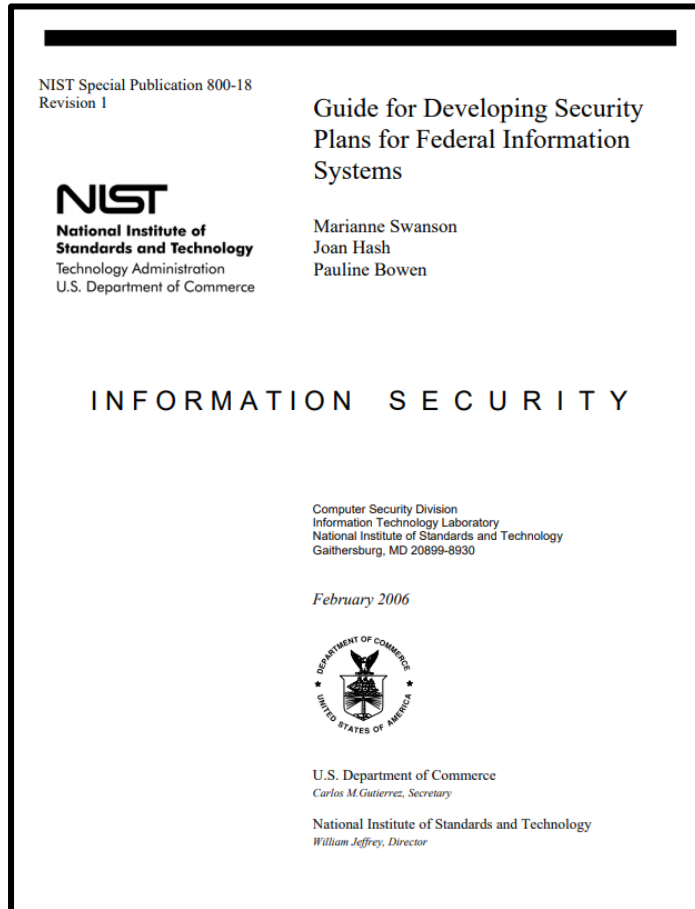
Figure 2: SP 800-60 Security Categorization Process Execution

Selecting cybersecurity risk controls



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

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



CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Management controls focus on management of the information system and management of risk for a system

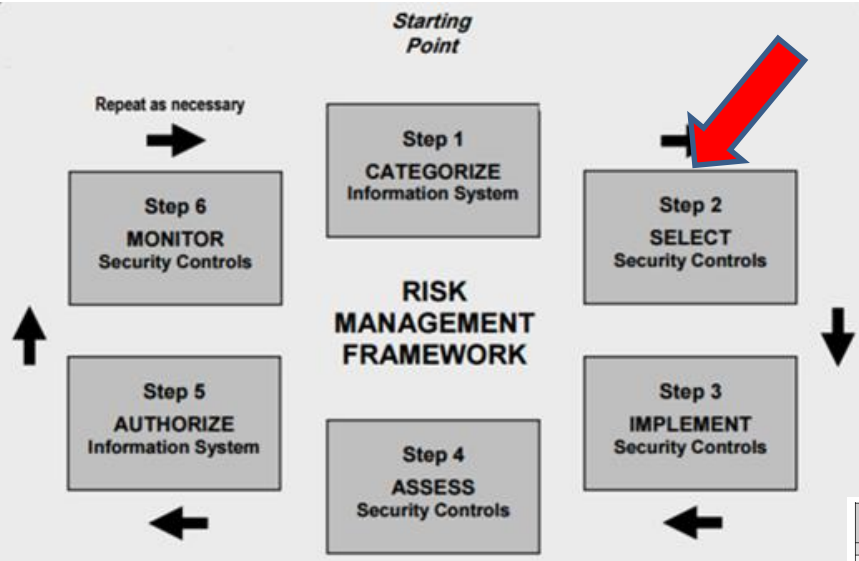
Operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems) with technical expertise and/or management expertise

Technical controls focus on automated security controls that the computer system(s) executes

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



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



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	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	Not Selected
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 (1)	IR-4 (1) (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-7	Least Privilege	P1	CM-7 (1) (2)	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (2) (3)	CM-8 (1) (2) (3)

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

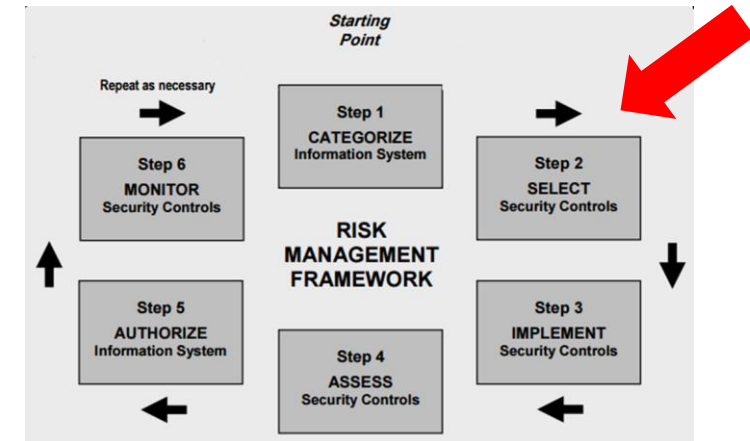
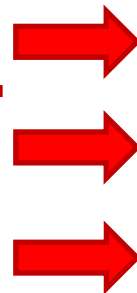
CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	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) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Login Attempts	P0	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Login (Session) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Access 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	P1	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

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

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

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