MIS 5206
Protecting Information Assets
- Unit #1b -

Data Classification
Processes and Models

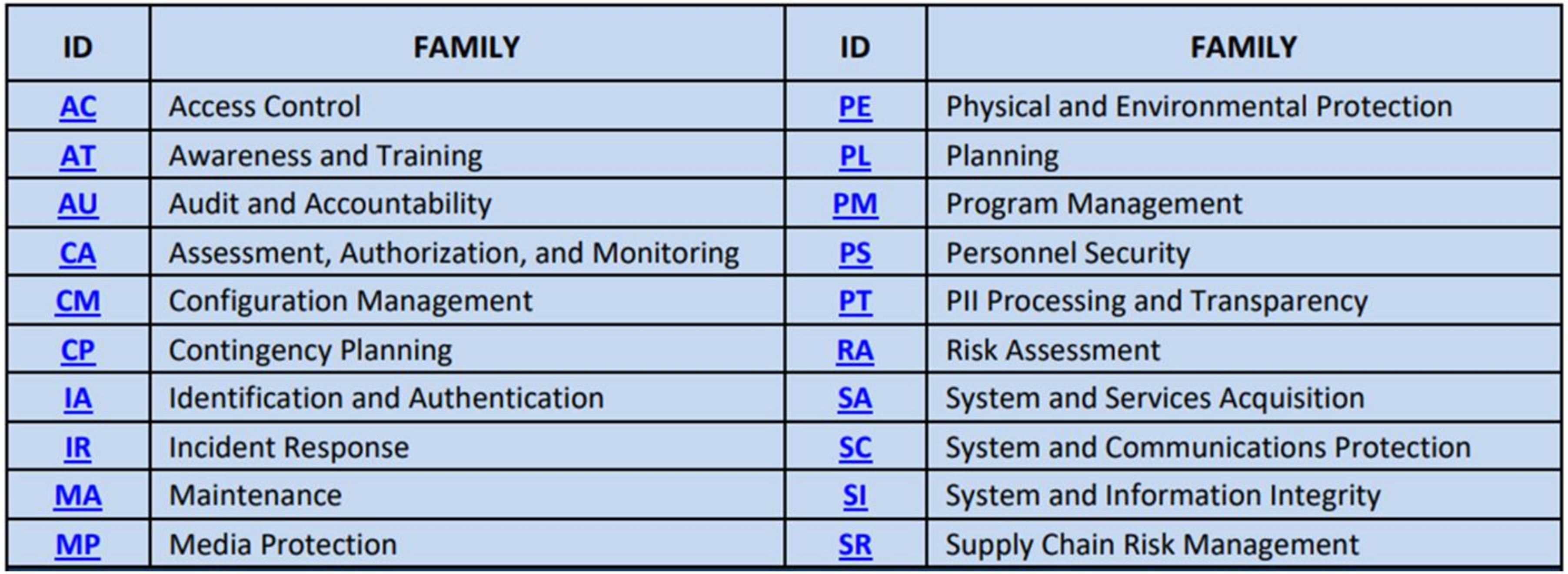
Agenda

- Vocabulary
- Data Classification Process and Models
- Test taking tip
- Quiz

Information Systems Security Controls

What do I mean when I say:

Information System security is a 20-dimensional problem ?



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

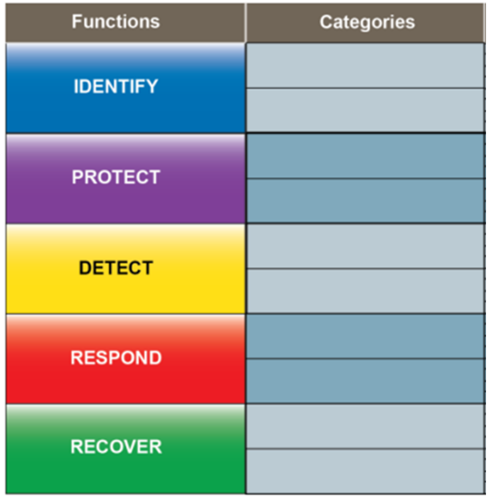
Taxonomies of Information System (InfoSys) Controls

By Function

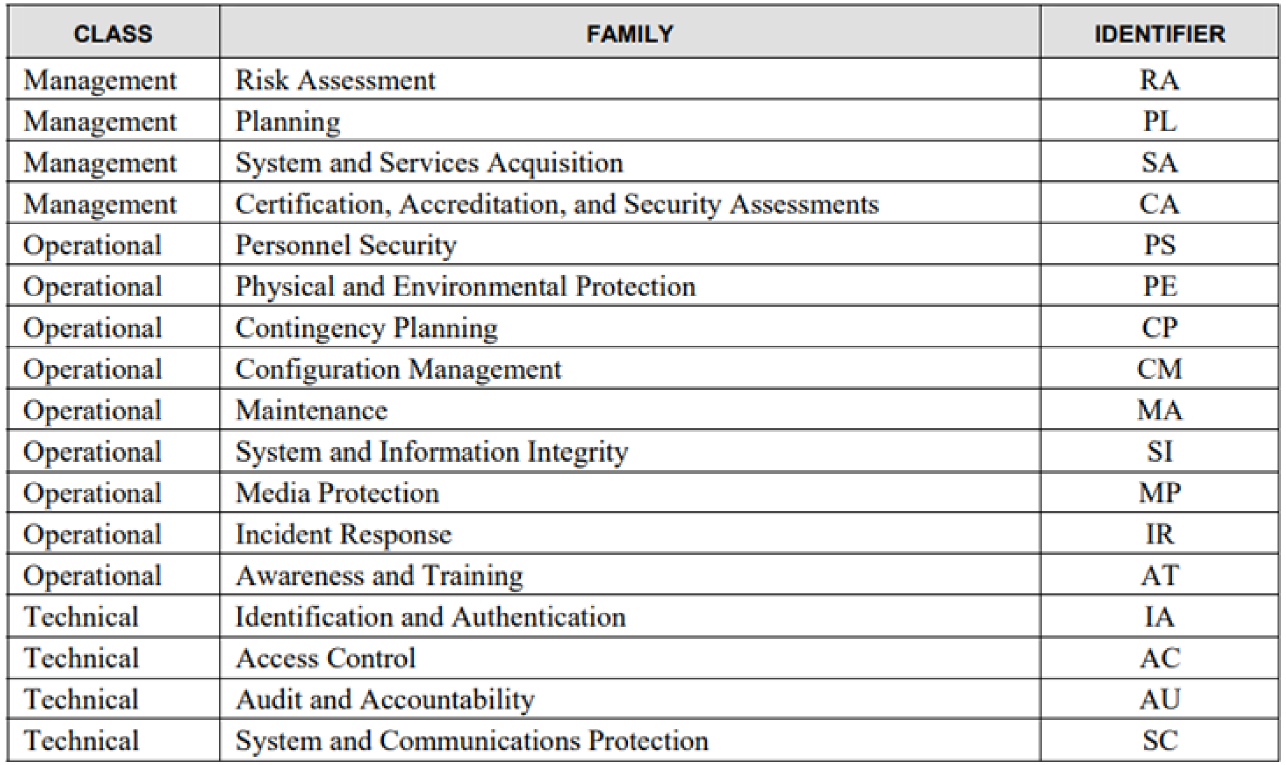
- Identify
- Protect
- Detect
- Respond
- Recover

By Class

- Management
- Operational
- Technical



Functions	Categories
IDENTIFY	
PROTECT	
DETECT	
RESPOND	
RECOVER	



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

Taxonomies of InfoSys Controls

By <u>Modality</u>

1. Physical
2. Technical
3. Administrative

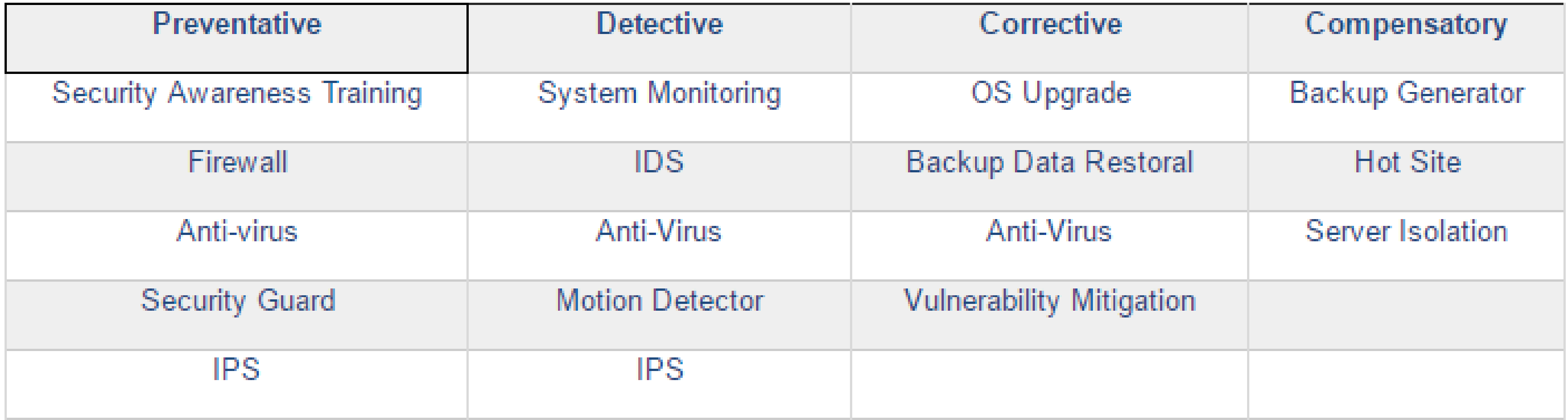
A modality is the way (or mode) in which something is done

http://www.sans.edu/research/security-laboratory/article/security-controls

Taxonomies of InfoSys Controls

By <u>Phase or Function</u>

1. Preventative
2. Detective
3. Corrective
4. Compensating



Preventative	Detective	Corrective	Compensatory
Security Awareness Training	System Monitoring	OS Upgrade	Backup Generator
Firewall	IDS	Backup Data Restoral	Hot Site
Anti-virus	Anti-Virus	Anti-Virus	Server Isolation
Security Guard	Motion Detector	Vulnerability Mitigation	
IPS	IPS		

These are sometimes referred to as “*phase controls*”

http://www.sans.edu/research/security-laboratory/article/security-controls

Taxonomies of Information System Controls

By phase or function

- Preventive
- Detective
- Corrective
- Compensating

By modality

- Physical
- Technical
- Administrative

Juxtaposing taxonomies to improve understanding…

		Modality		
	Controls	**Administrative**	**Technical**	**Physical**
Function	**Preventive**	*User registration*	*Passwords, Tokens*	*Fences*
	Detective	*Report reviews*	*Audit Logs*	*Sensors*
	Corrective	*Employee termination*	*Connection management*	*Fire extinguisher*
	Compensating	*Supervision*	*Keystroke logging*	*Layered defenses*

Question

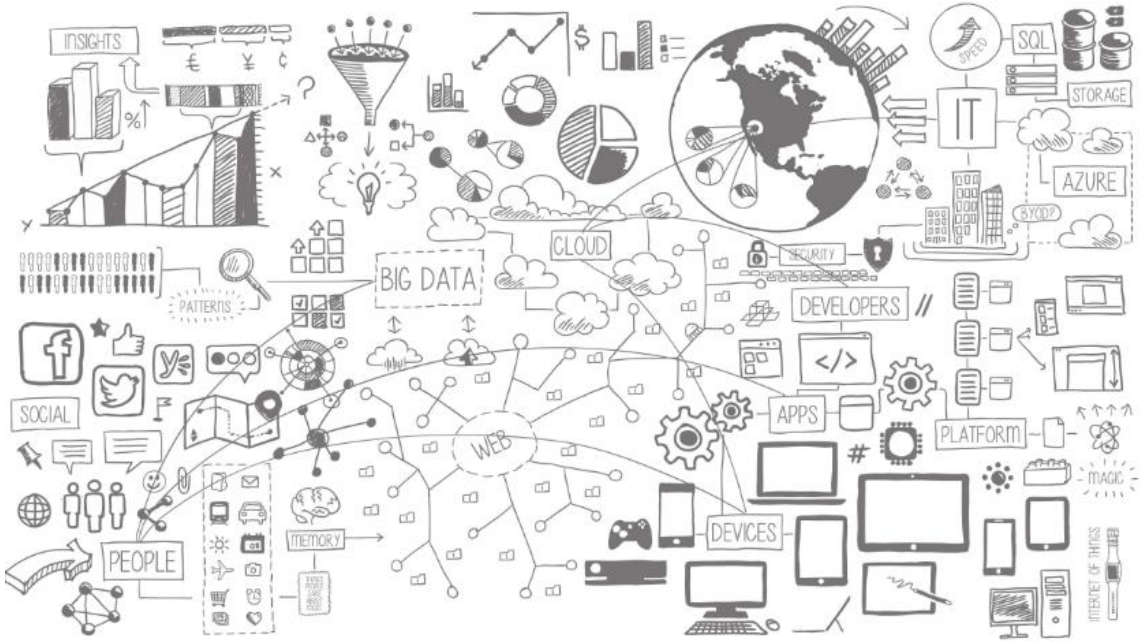
- What is data ?
- What is information ?
- How do data and information relate to each other?
- What is an information system?

What is data ?

http://researchdata.ox.ac.uk/

1. Known facts or things used as a basis for inference or reckoning
2. Quantities or characters operated on by a computer etc.

The Concise Oxford Dictionary



https://blogs.microsoft.com/blog/2014/04/15/a-data-culture-for-everyone/

What is the nature of data stored in the attributes comprising the entities within the information system's databases

What is information?

*An Entity's attribute values can be understood in terms of **"measurement levels"***

Stevens, S.S. 1946. On the theory of scales of measurement. Science 103:677-680.

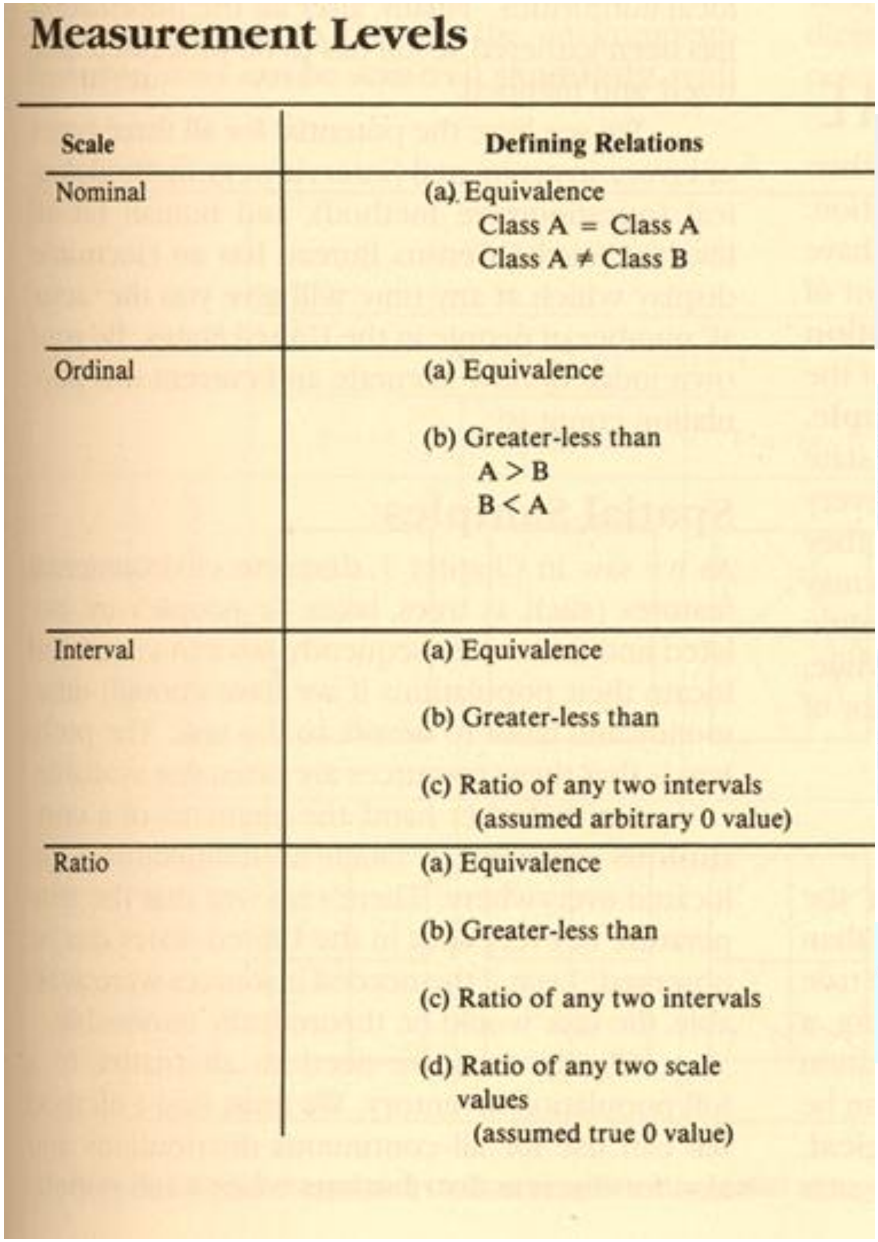
Measurements levels describe the inherent nature of information in the attribute data that make up entities

- Qualitative information tells what things exist
- Quantitative information orders and measures the magnitude of these things

Steven's 4 measurement levels

1. Nominal
2. Ordinal
3. Interval
4. Ratio

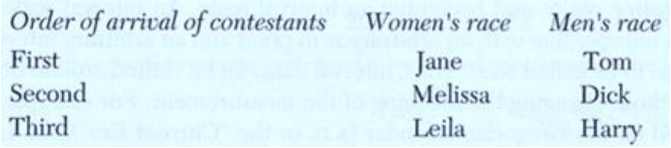
Increasing information content



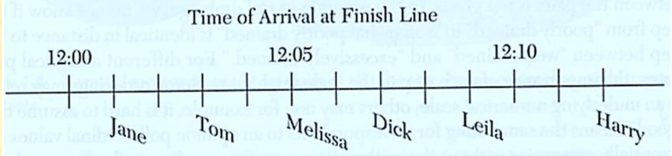
Measurement Levels

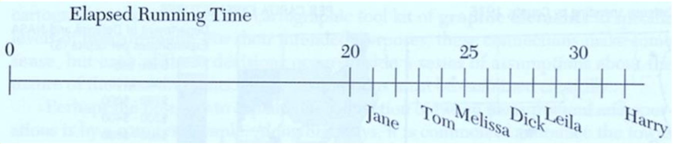
Scale	Defining Relations
Nominal	(a) Equivalence Class A = Class A Class A ≠ Class B
Ordinal	(a) Equivalence (b) Greater-less than A > B B < A
Interval	(a) Equivalence (b) Greater-less than (c) Ratio of any two intervals (assumed arbitrary 0 value)
Ratio	(a) Equivalence (b) Greater-less than (c) Ratio of any two intervals (d) Ratio of any two scale values (assumed true 0 value)

Polka dot
Solid Color



Order of arrival of contestants	*Women's race*	*Men's race*
First	Jane	Tom
Second	Melissa	Dick
Third	Leila	Harry

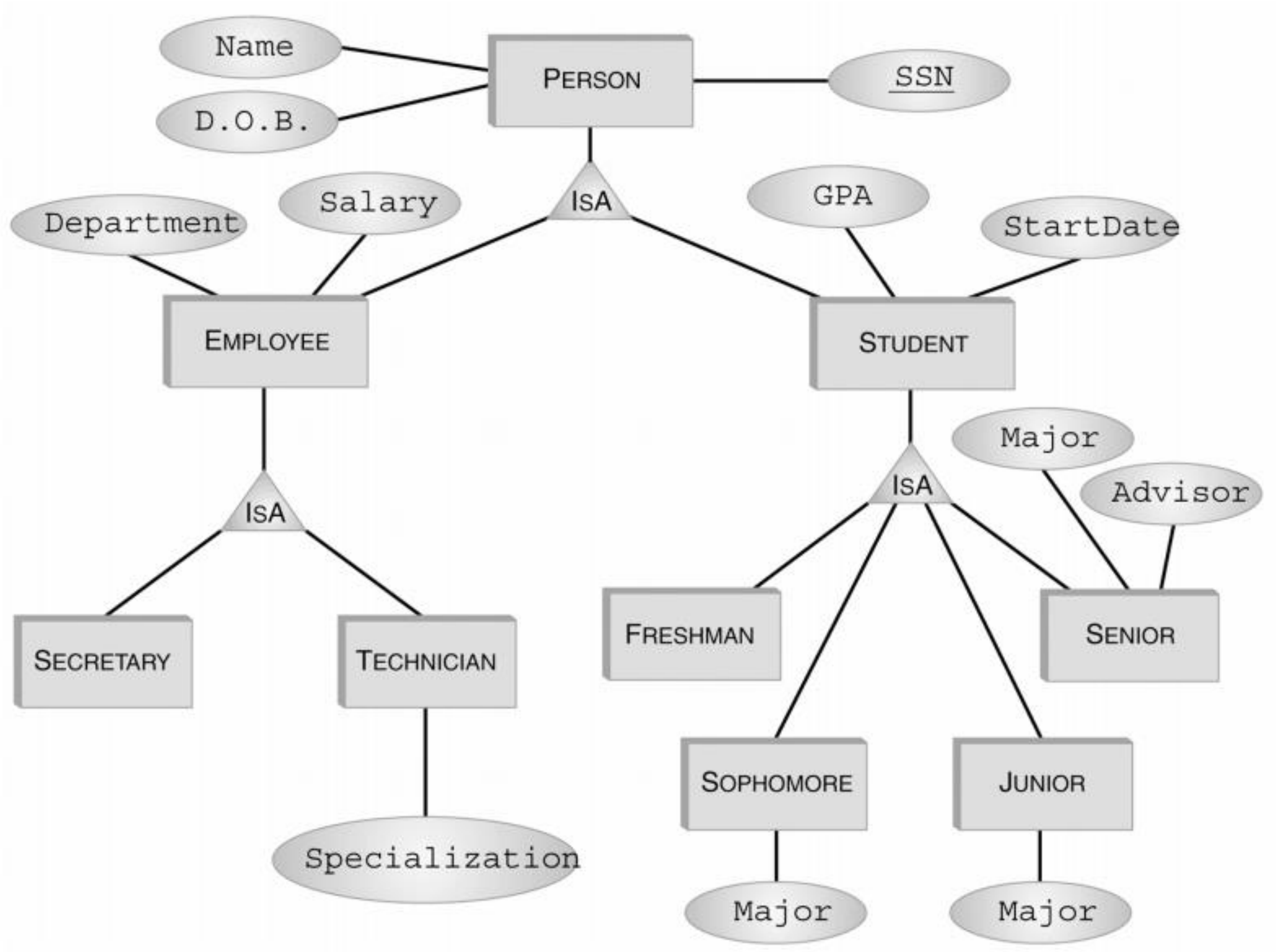




Entity Attribute Value Measurement Types

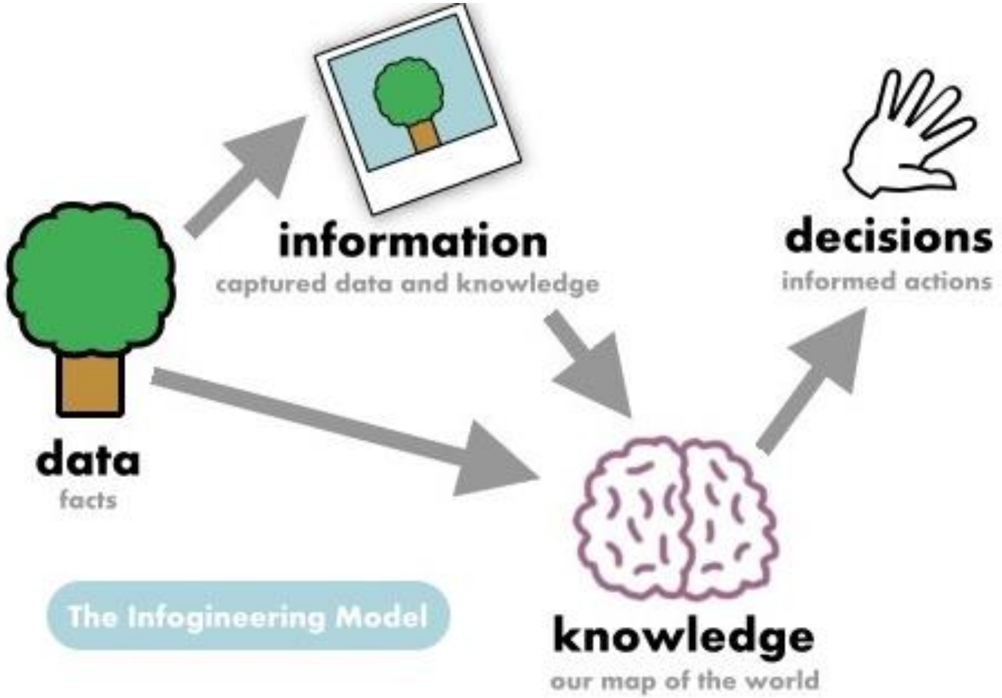
	Qualitative	**Quantitative**
Nominal	X	
Ordinal	X	
Interval		X
Ratio		X

How would you use Steven's measurements levels to categorize this information ?



How do data and information relate to each other ?

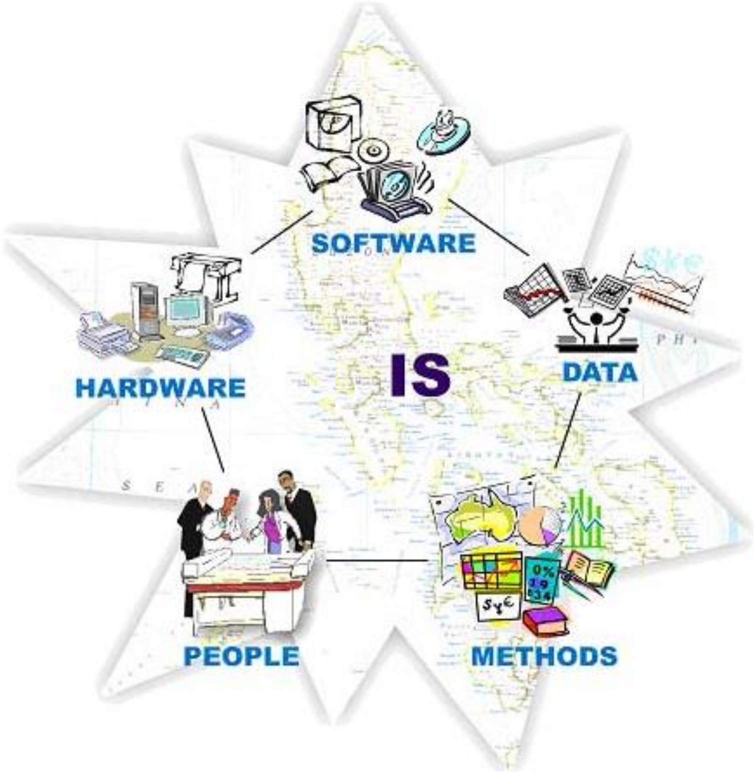
Information is data "put to work" in a decision-making context!

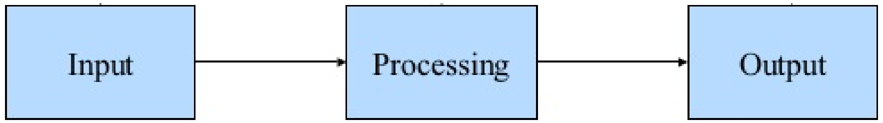


http://www.infogineering.net/data-information-knowledge.htm

What is an information system ?

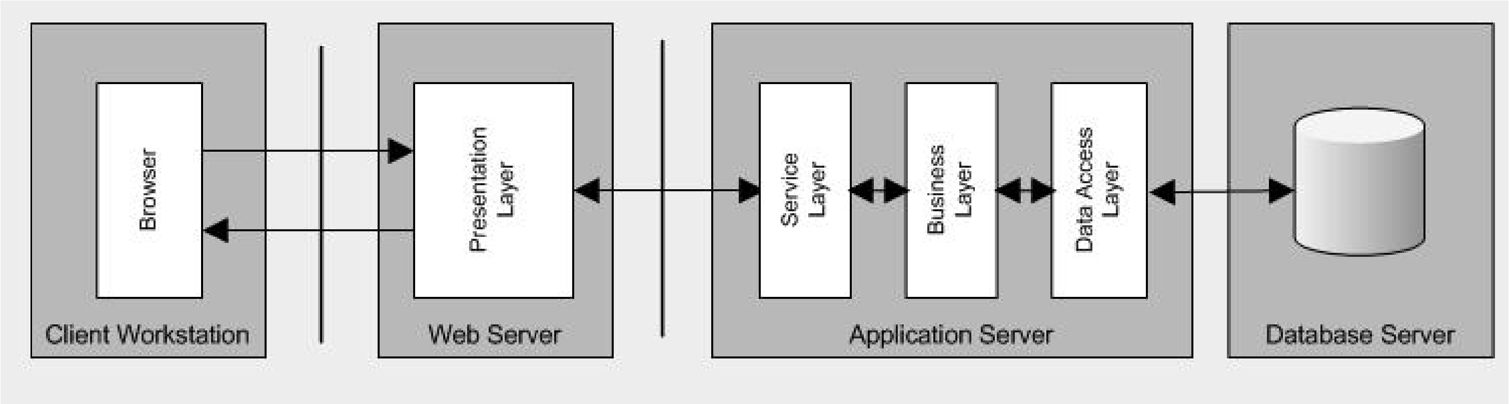
*“An **information system** (**IS**) is an organized system for the collection, organization, storage and communication of information. …complementary networks that people and organizations use to collect, filter (query), process, create and distribute data. Further, an information system (IS) is a group of components that interact to produce information.”* Wikipedia



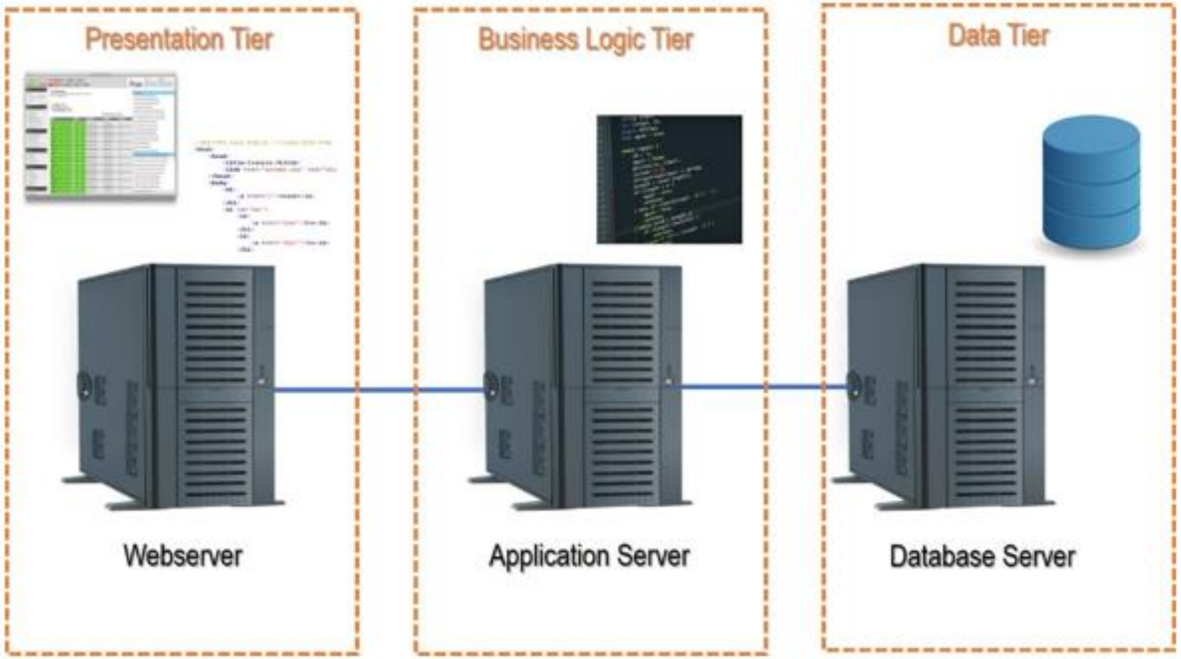


Input → Processing → Output

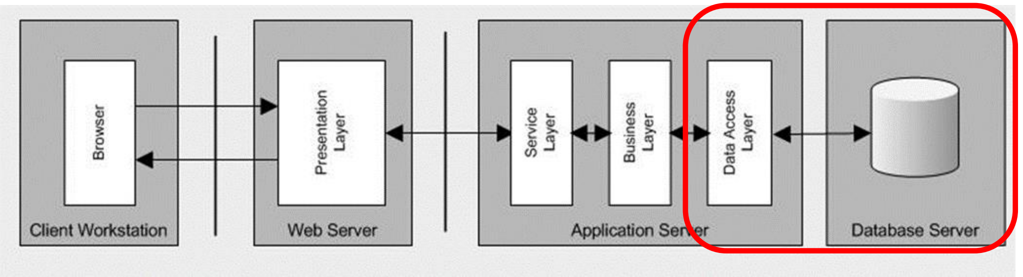
Information system (IS) architectures

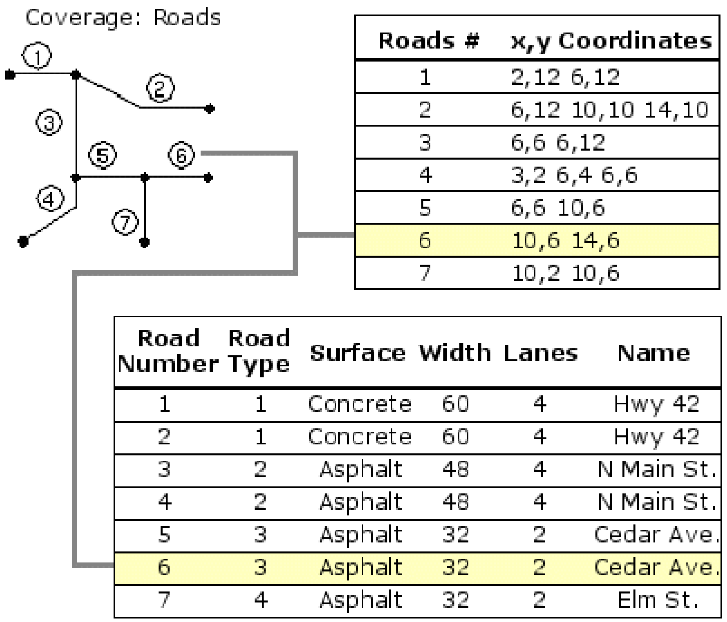


N-Tier Architecture examples



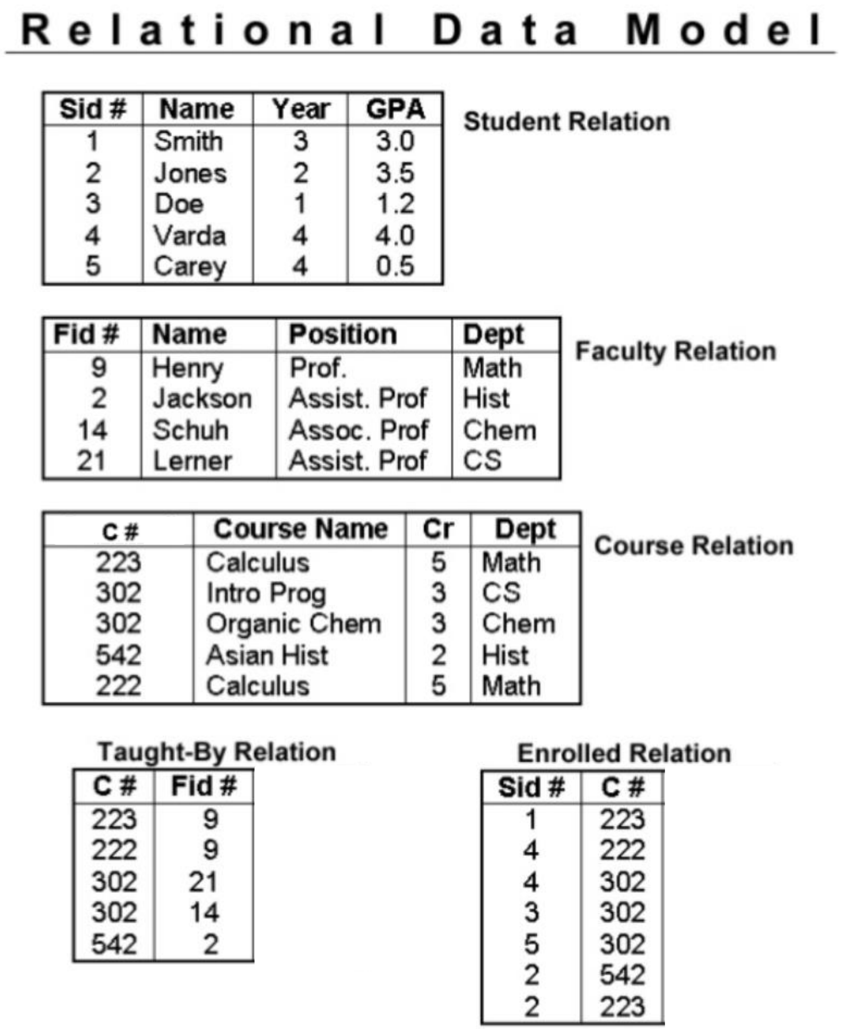
Information System Data





Roads #	x,y Coordinates
1	2,12 6,12
2	6,12 10,10 14,10
3	6,6 6,12
4	3,2 6,4 6,6
5	6,6 10,6
6	10,6 14,6
7	10,2 10,6

Road Number	Road Type	Surface	Width	Lanes	Name
1	1	Concrete	60	4	Hwy 42
2	1	Concrete	60	4	Hwy 42
3	2	Asphalt	48	4	N Main St.
4	2	Asphalt	48	4	N Main St.
5	3	Asphalt	32	2	Cedar Ave.
6	3	Asphalt	32	2	Cedar Ave.
7	4	Asphalt	32	2	Elm St.



Relational Data Model

Student Relation

Sid #	Name	Year	GPA
1	Smith	3	3.0
2	Jones	2	3.5
3	Doe	1	1.2
4	Varda	4	4.0
5	Carey	4	0.5

Faculty Relation

Fid #	Name	Position	Dept
9	Henry	Prof.	Math
2	Jackson	Assist. Prof	Hist
14	Schuh	Assoc. Prof	Chem
21	Lerner	Assist. Prof	CS

Course Relation

C #	Course Name	Cr	Dept
223	Calculus	5	Math
302	Intro Prog	3	CS
302	Organic Chem	3	Chem
542	Asian Hist	2	Hist
222	Calculus	5	Math

Taught-By Relation

C #	Fid #
223	9
222	9
302	21
302	14
542	2

Enrolled Relation

Sid #	C #
1	223
4	222
4	302
3	302
5	302
2	542
2	223

Concept

Classification Grouping of data according to pre-determined types

Why classify data ?

Data Classification Processes and Models

Data classification (“categorization”) is essential to ensuring that data is appropriately protected, and done so in the most cost-effective manner

The goal is to classify data according to risk associated with a breach to their confidentiality, integrity, and availability

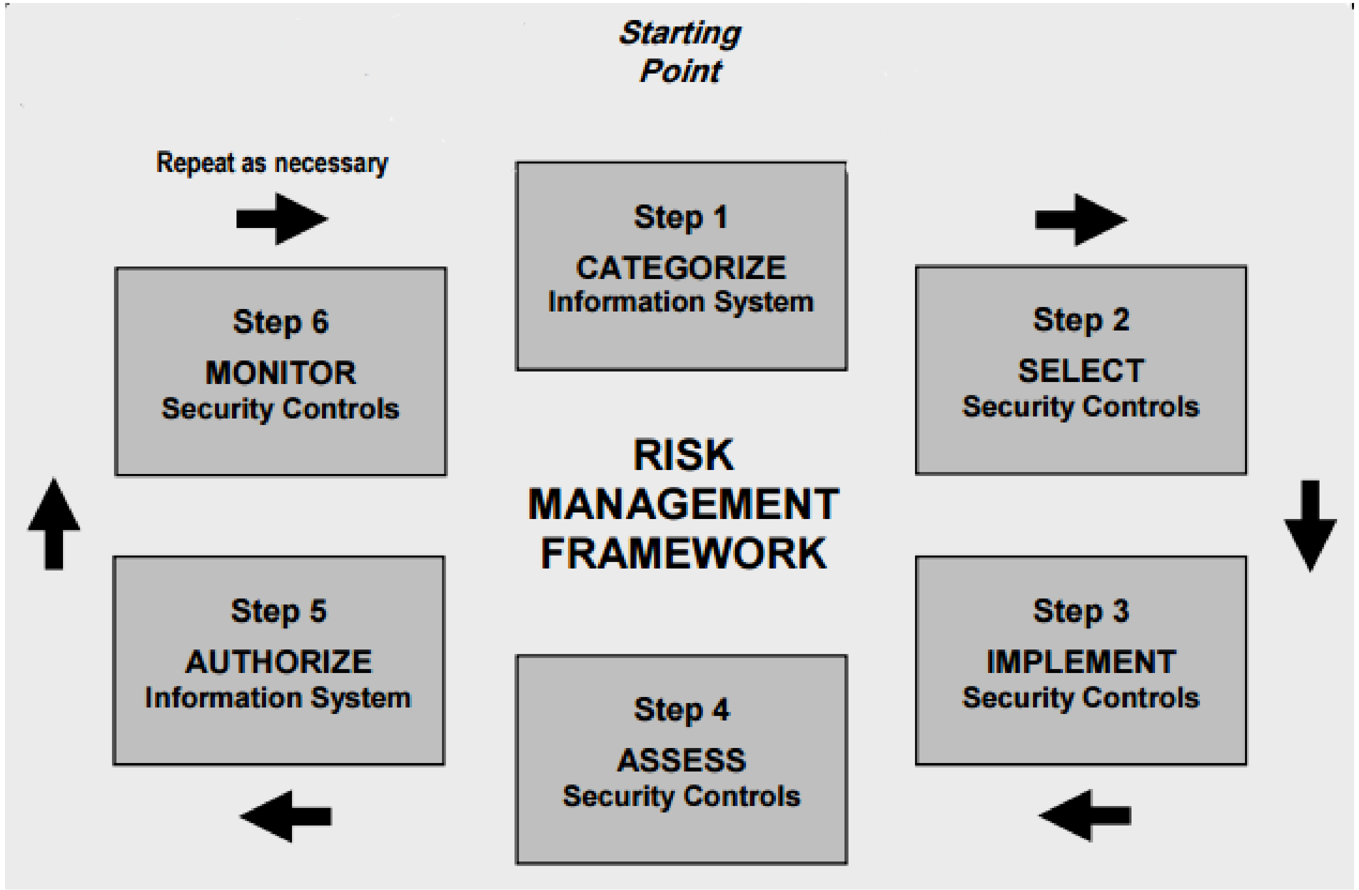
Enables determining the appropriate cost expenditure of security control mitigations required to protect the IT assets

Key Concepts

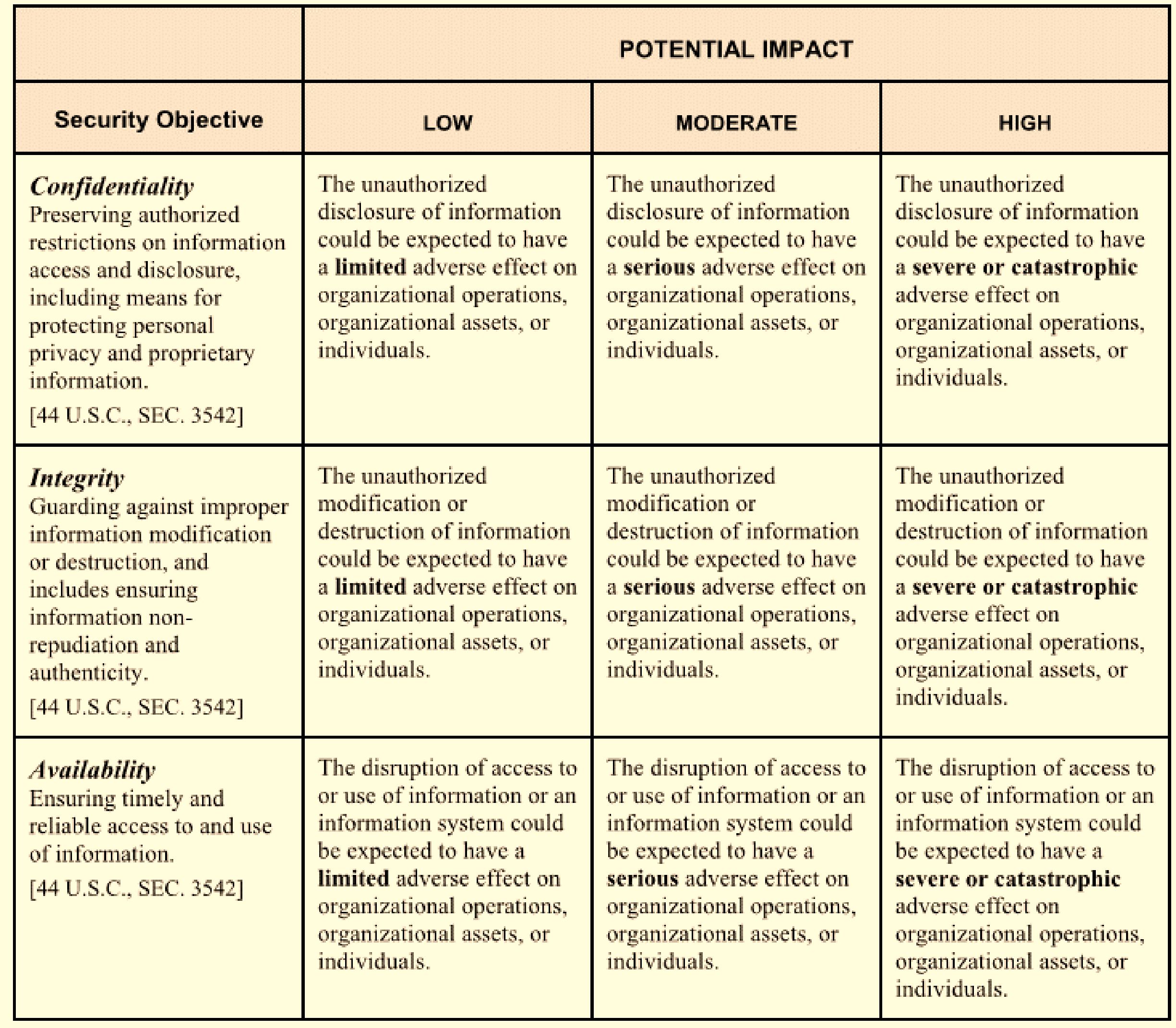
Classification	Grouping of data according to pre-determined types
Cost-Effectiveness	Appropriateness of the level of risk mitigation expenditure
Confidentiality	Restriction who may know about and/or have access to information
Integrity	Confidence that information is complete and unaltered
Availability	Access to information

Question:

How should we determine the information security categorization of an IT asset?

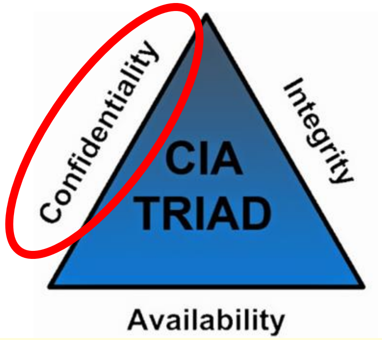


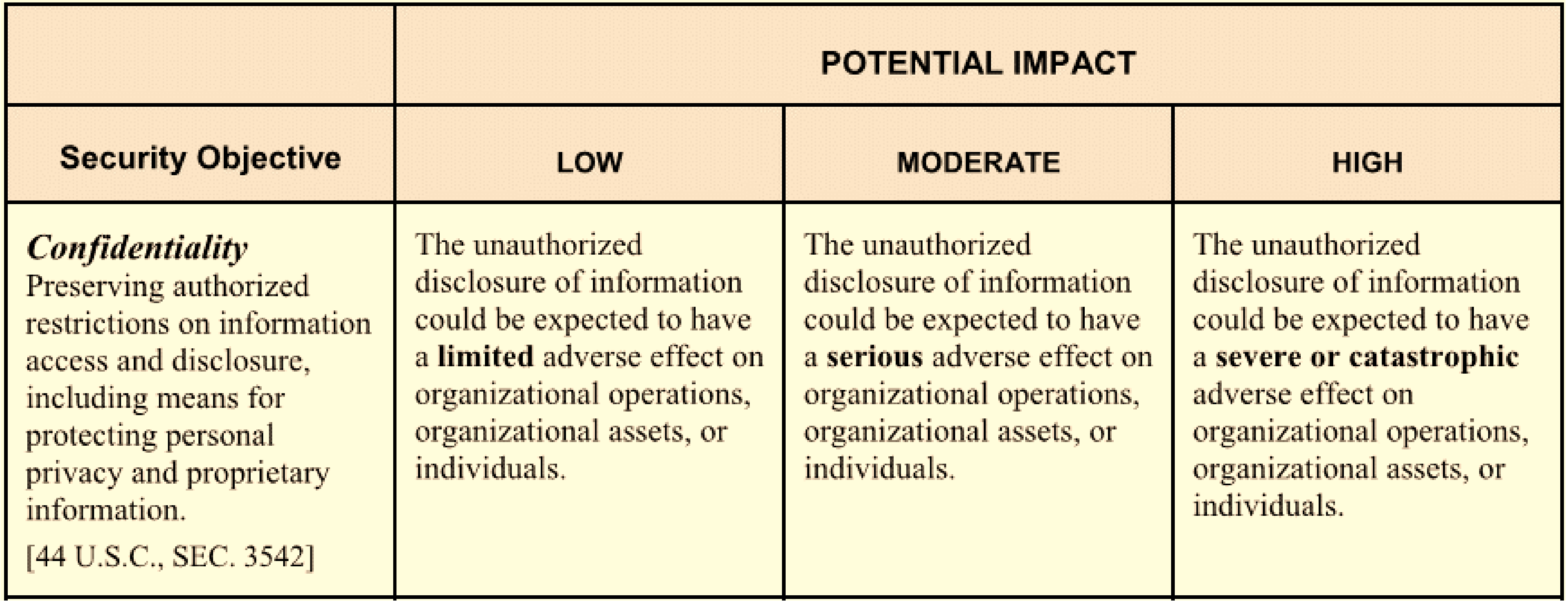
Security objectives and impact ratings



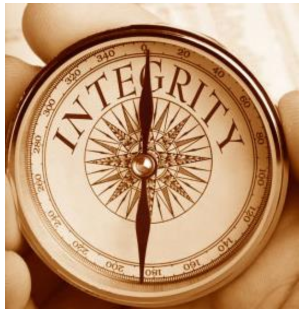
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could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

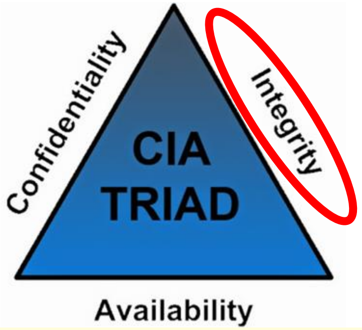
Confidentiality
Integrity
CIA
TRIAD
Availability

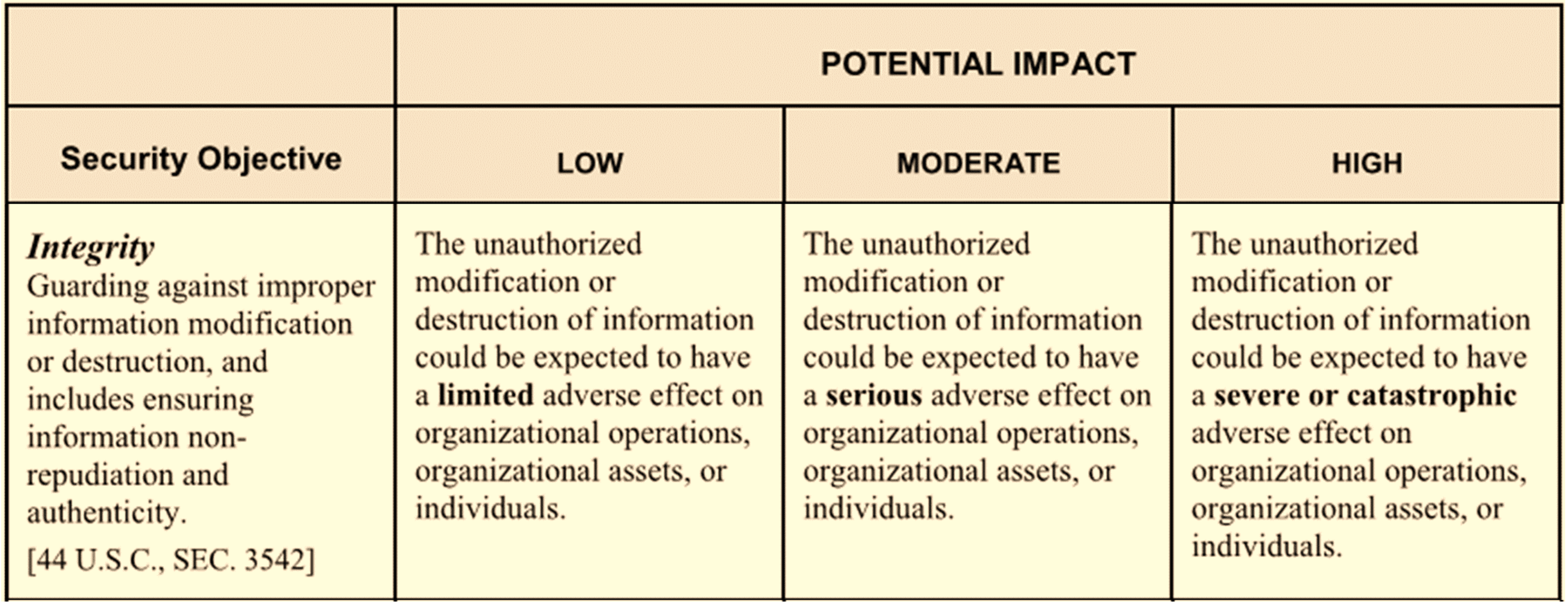




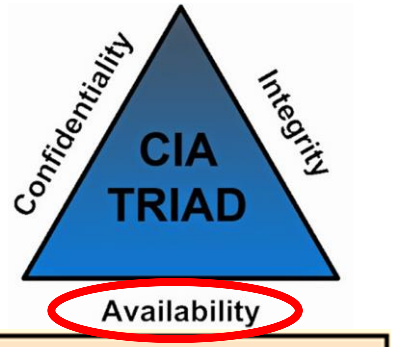
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

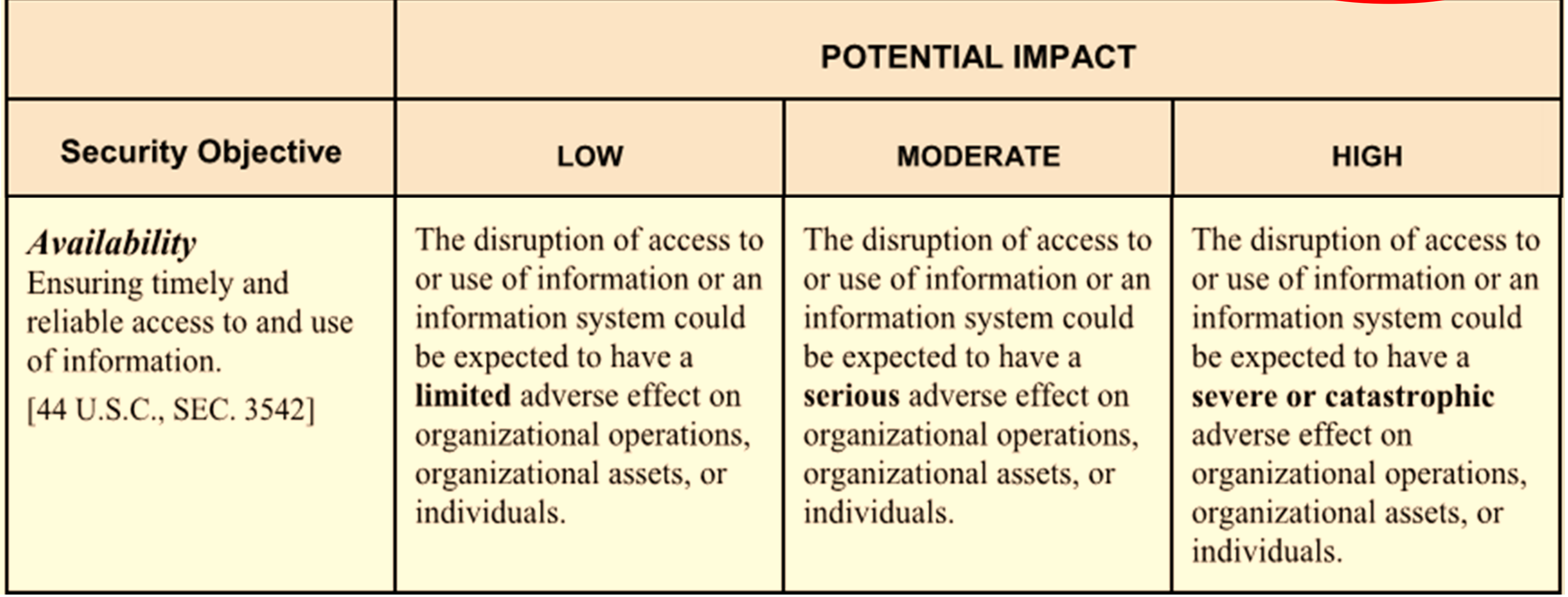






	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.





	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

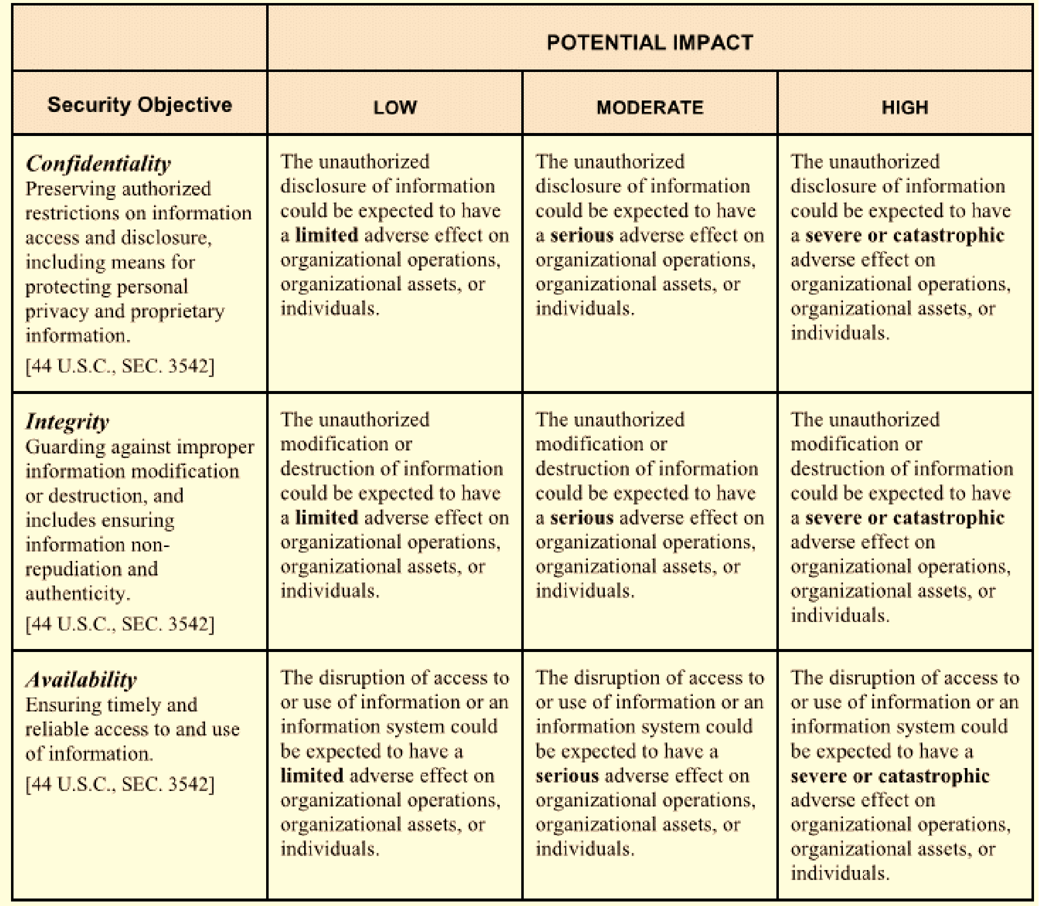
Security objectives and impact ratings

Low: *Limited adverse effect*

Moderate: *Serious adverse effect*

High: *Severe or catastrophic adverse effect*

What kind of Steven's measurement level is used by this Information Security Categorization standard?



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

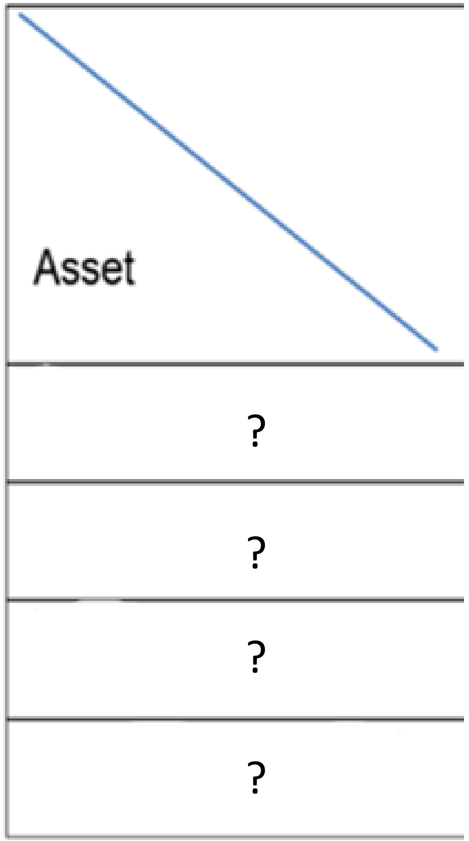
Question?

How would you determine the information security categorization of the Dean's computer

Steps:

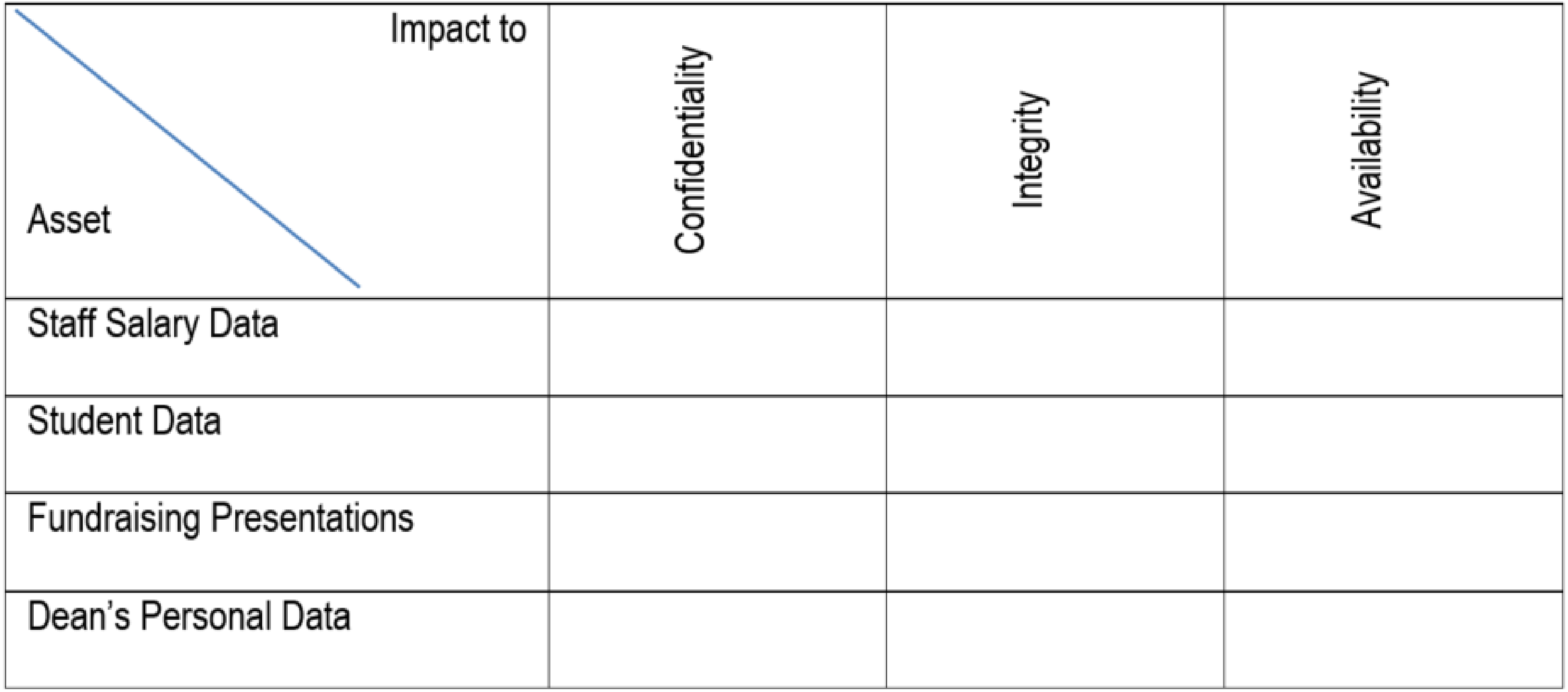
1. *Inventory the types of information that might be on the Dean's laptop*
2. *Assign confidentiality, integrity, and availability information security categorizations for each type of information contained on the Dean's laptop*
3. *Analyze the categorizations of the information, and determine the overall security categorization for the laptop*

1. Create an inventory of types of datasets possibly stored on the Dean’s laptop



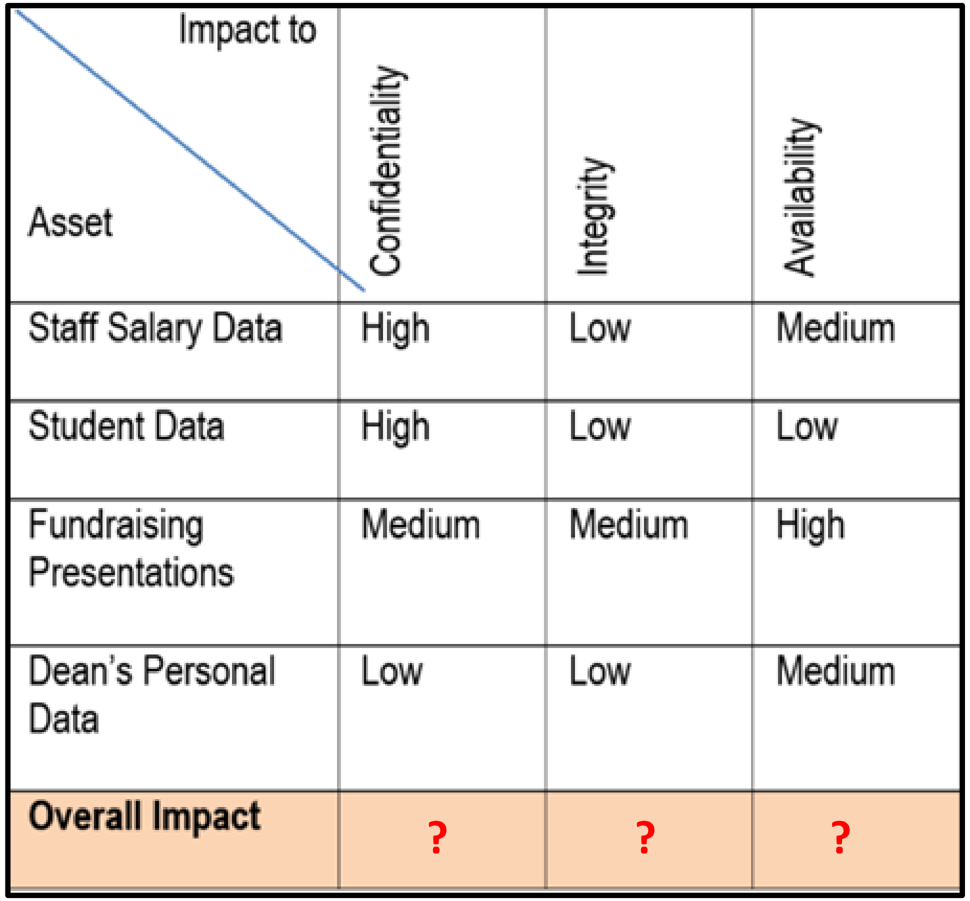
Asset
?
?
?
?

2. Assign information security categorization impact ratings to the data on the Dean’s laptop…



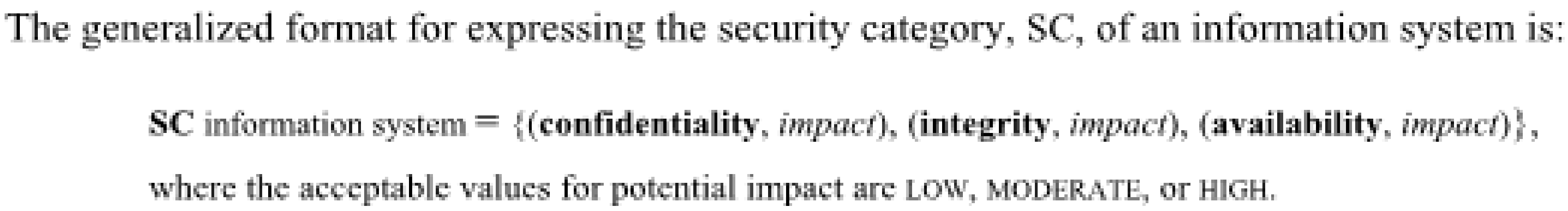
Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data			
Student Data			
Fundraising Presentations			
Dean’s Personal Data			

What is the information security categorization of the Dean’s laptop?



Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data	High	Low	Medium
Student Data	High	Low	Low
Fundraising Presentations	Medium	Medium	High
Dean’s Personal Data	Low	Low	Medium
Overall Impact	?	?	?

Determine the security categorization of an information system based on the security categorization of the multiple types of information that it contains or transports…

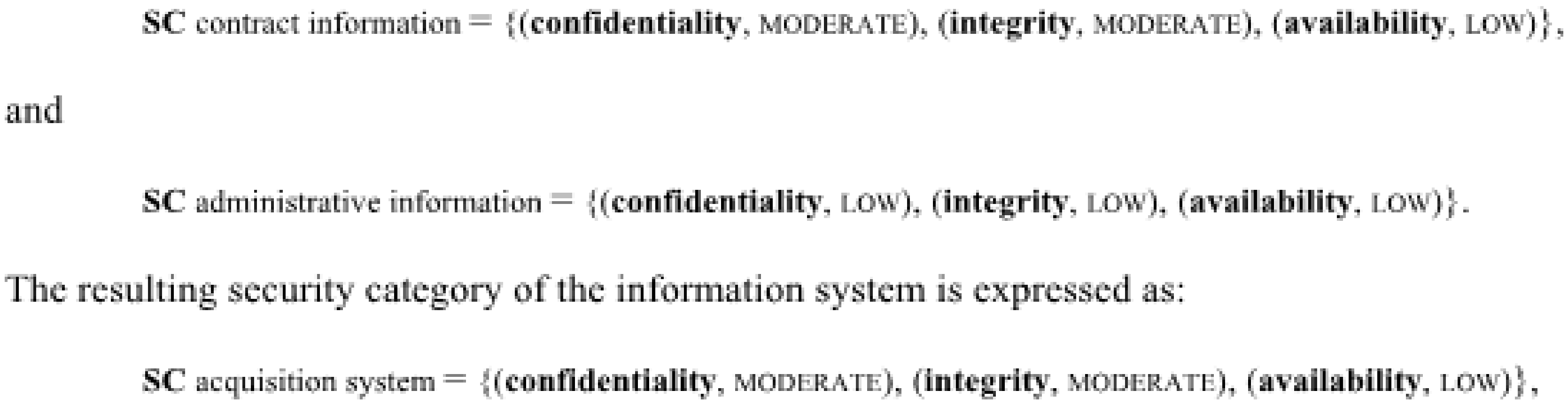


The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

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

Example with multiple information types:



SC contract information = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

and

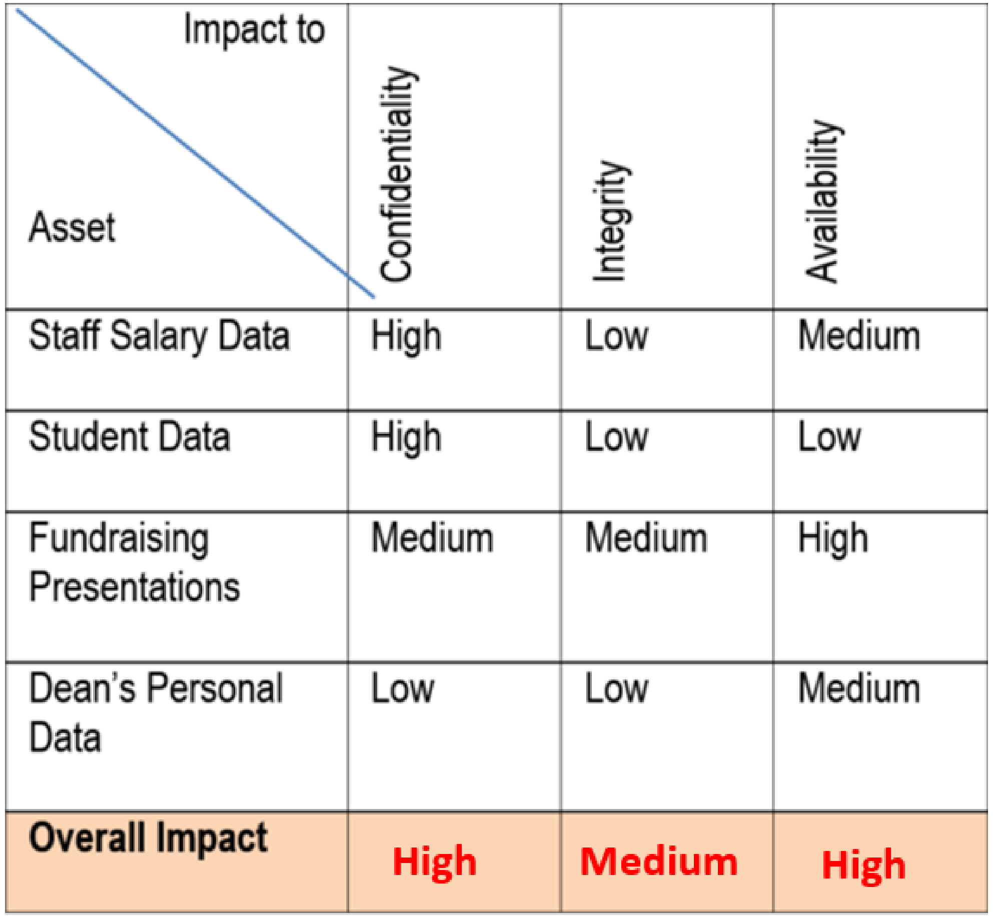
SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

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

SC acquisition system = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)},

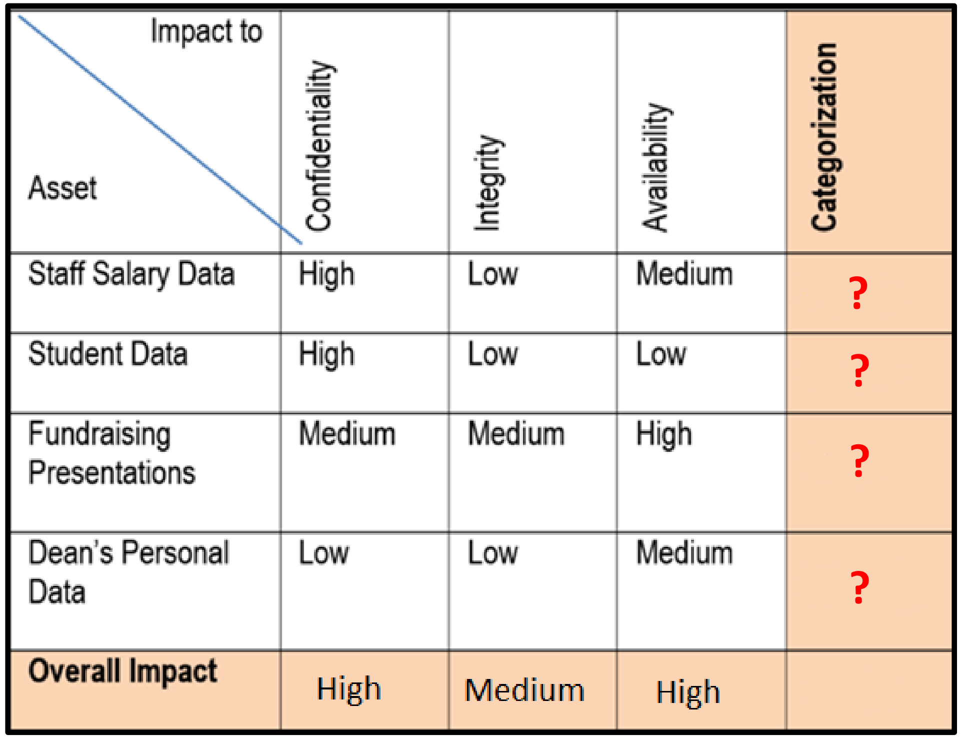
Low: Limited adverse effect
Moderate: Serious adverse effect
High: Severe or catastrophic adverse effect

Overall impact in each of the security objectives is based on the highest impact dataset for each of objective



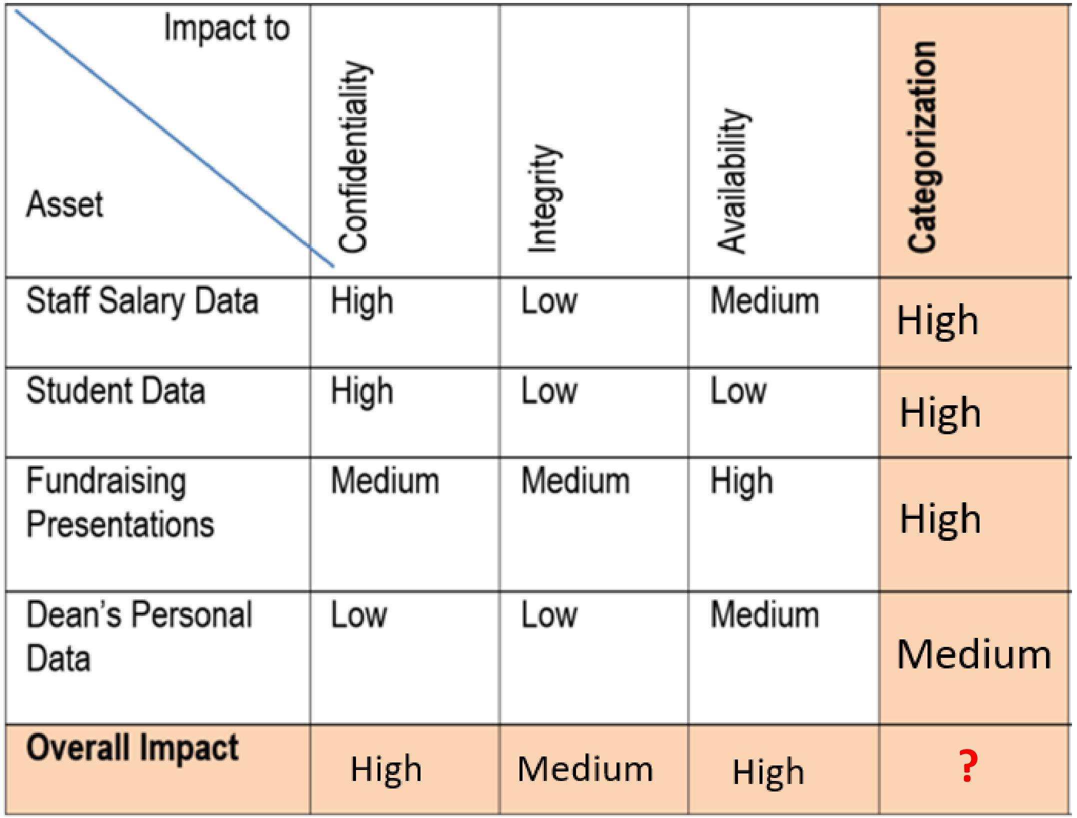
Impact to Asset	Confidentiality	Integrity	Availability
Staff Salary Data	High	Low	Medium
Student Data	High	Low	Low
Fundraising Presentations	Medium	Medium	High
Dean’s Personal Data	Low	Low	Medium
Overall Impact	**High**	**Medium**	**High**

What single overall information security categorization would you give each dataset on the Dean’s laptop?



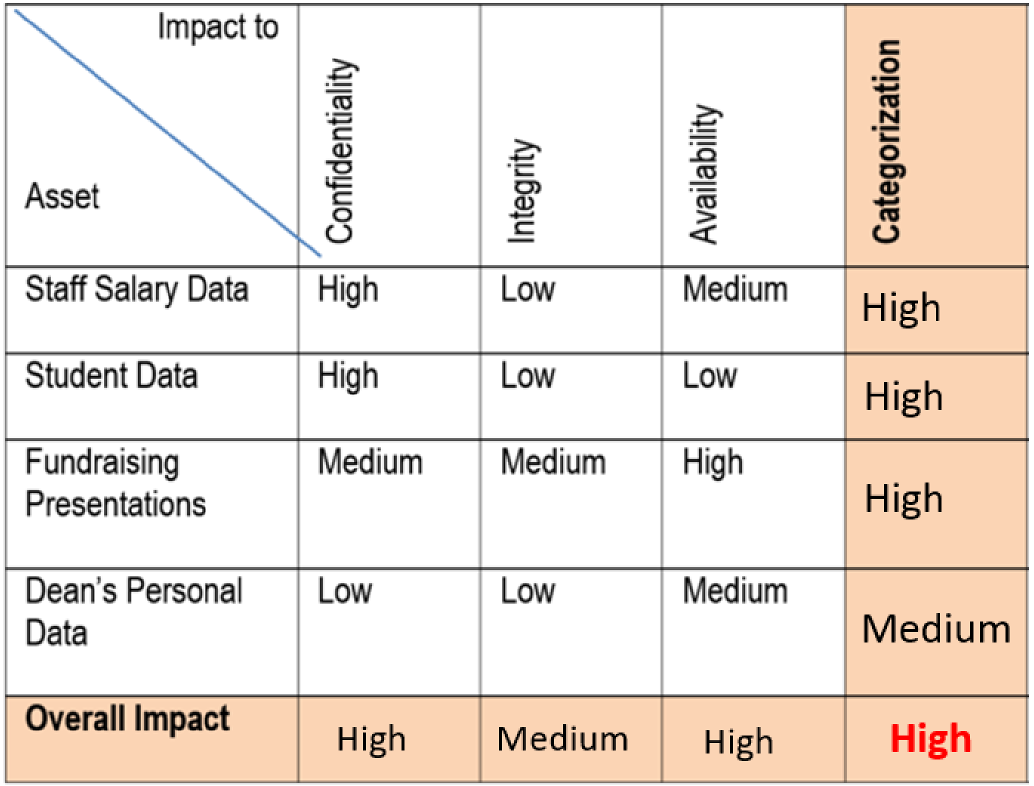
Impact to Asset	Confidentiality	Integrity	Availability	Categorization
Staff Salary Data	High	Low	Medium	?
Student Data	High	Low	Low	?
Fundraising Presentations	Medium	Medium	High	?
Dean’s Personal Data	Low	Low	Medium	?
Overall Impact	High	Medium	High	

What single value would you use to rate the information security requirements of the Dean’s laptop?



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

The single overall information security categorizations for each dataset on the Dean’s laptop



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

How do you define the following?

- Policy
- Standard
- Guideline
- Procedure

How do they relate to each other?

Policy, Standard, Guideline and Procedures

Policy:

- A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required actions and may include pointers to standards.
- Policy attributes include the following:
  - Requires compliance (mandatory)
  - Failure to comply results in disciplinary action
  - Focus on desired results, not on means of implementation
  - Further defined by standards and guidelines

Policy, Standard, Guideline and Procedures

Standard:

- A mandatory action or rule designed to support and conform to a policy
  - A standard should make a policy more meaningful and effective
  - A standard must include one or more accepted specifications for hardware, software, or behavior

Policy, Standard, Guideline and Procedures

Guideline:

- General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.
  - A guideline can change frequently based on the environment and should be reviewed more frequently than standards and policies.
  - A guideline is not mandatory, rather a suggestion of a best practice. Hence "guidelines" and "best practice" are interchangeable

Policy, Standard, Guideline and Procedures

Procedures:

- Procedures describe the process: who does what, when they do it, and under what criteria. They can be text- based or outlined in a process map
  - A series of steps taken to accomplish an end goal
  - Procedures define "how" to protect resources and are the mechanisms to enforce policy
  - Procedures provide a quick reference in times of crisis
  - Procedures help eliminate the problem of a single point of failure
  - Also known as a SOP (Standard Operating Procedure)

Policy, Standard, Guideline and Procedures

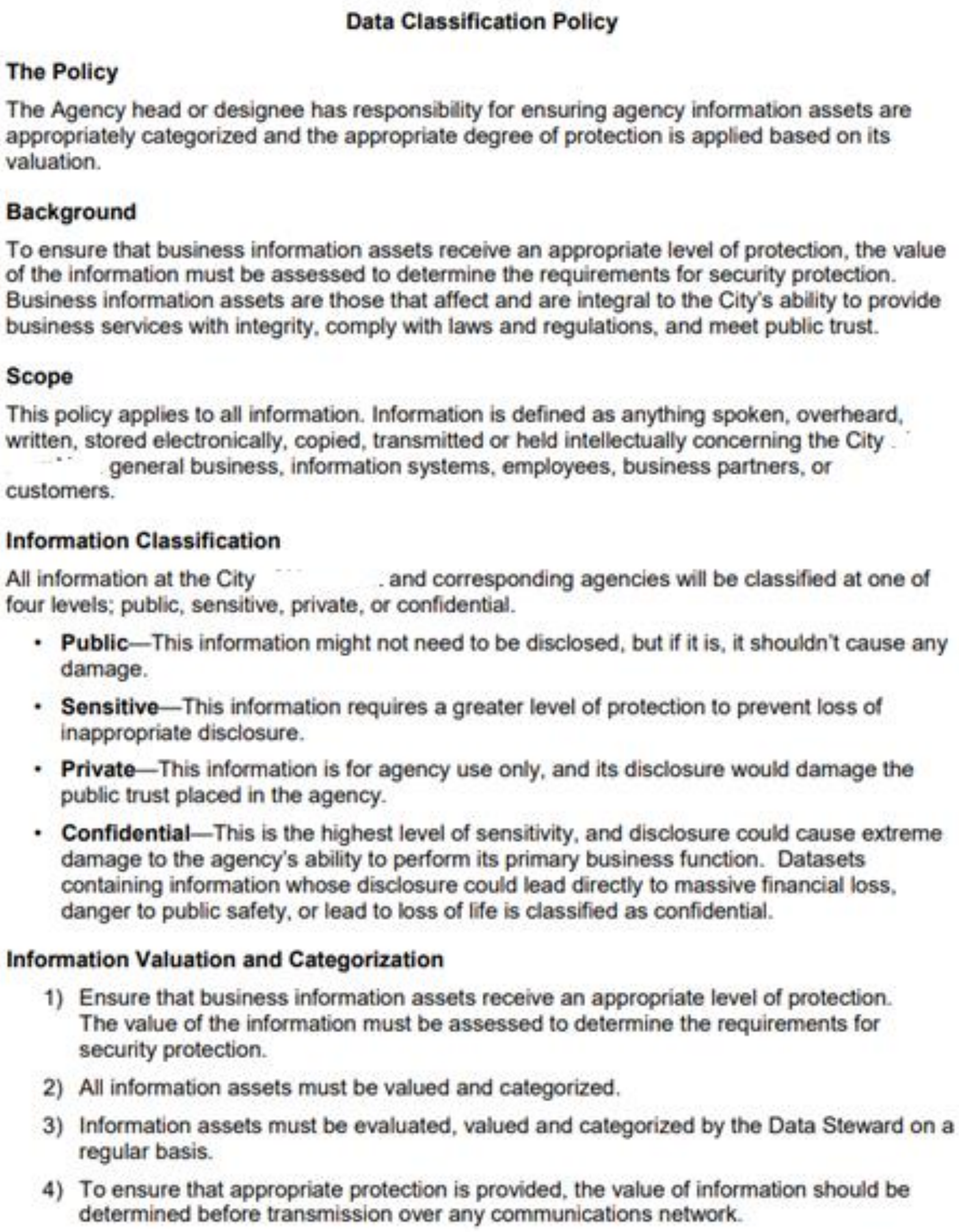
- **Policy:** A formal, brief, and high-level statement or plan that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required actions, and may include pointers to standards. Policy attributes include the following:
  - Requires compliance (mandatory)
  - Failure to comply results in disciplinary action
  - Focus on desired results, not on means of implementation
  - Further defined by standards and guidelines

- **Standard:** A mandatory action or rule designed to support and conform to a policy.
  - A standard should make a policy more meaningful and effective.
  - A standard must include one or more accepted specifications for hardware, software, or behavior.

- **Guideline:** General statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement procedures.
  - A guideline can change frequently based on the environment and should be reviewed more frequently than standards and policies.
  - A guideline is not mandatory, rather a suggestion of a best practice. Hence "guidelines" and "best practice" are interchangeable

- **Procedures:** Procedures describe the process: who does what, when they do it, and under what criteria. They can be text based or outlined in a process map.
  - A series of steps taken to accomplish an end goal.
  - Procedures define "how" to protect resources and are the mechanisms to enforce policy.
  - Procedures provide a quick reference in times of crisis.
  - Procedures help eliminate the problem of a single point of failure.
  - Also known as a SOP (Standard Operating Procedure)

Policy Example



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 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.

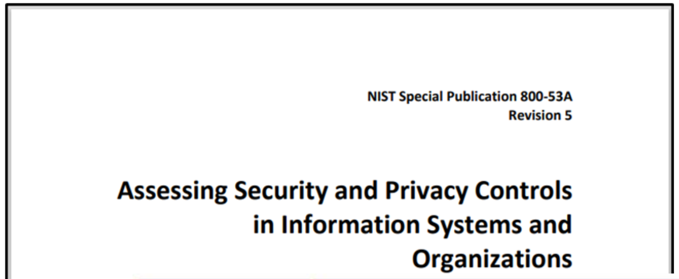
- **Public**—This information might not need to be disclosed, but if it is, it shouldn't cause any damage.
- **Sensitive**—This information requires a greater level of protection to prevent loss of inappropriate disclosure.
- **Private**—This information is for agency use only, and its disclosure would 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.

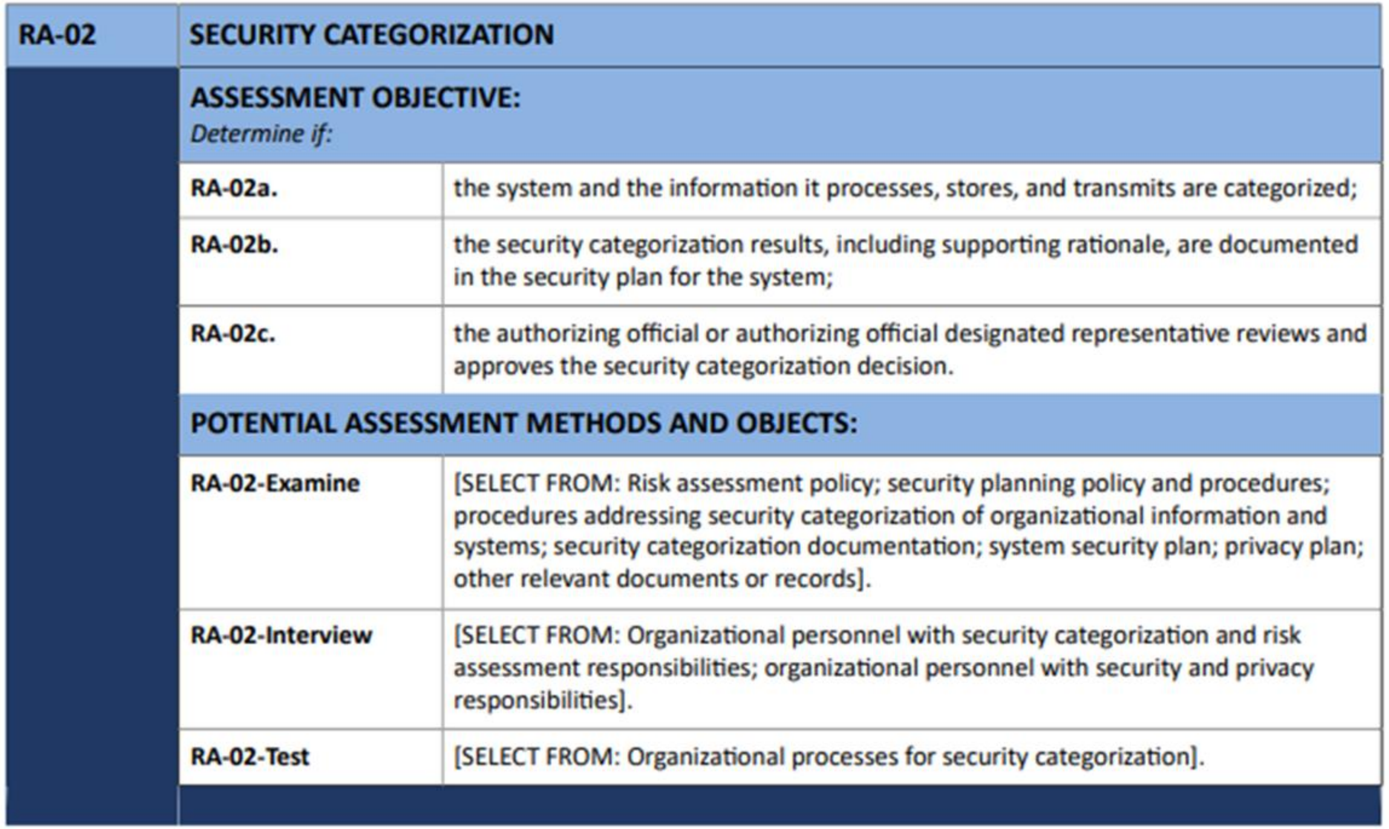
Question:

How would you audit the application of this policy?

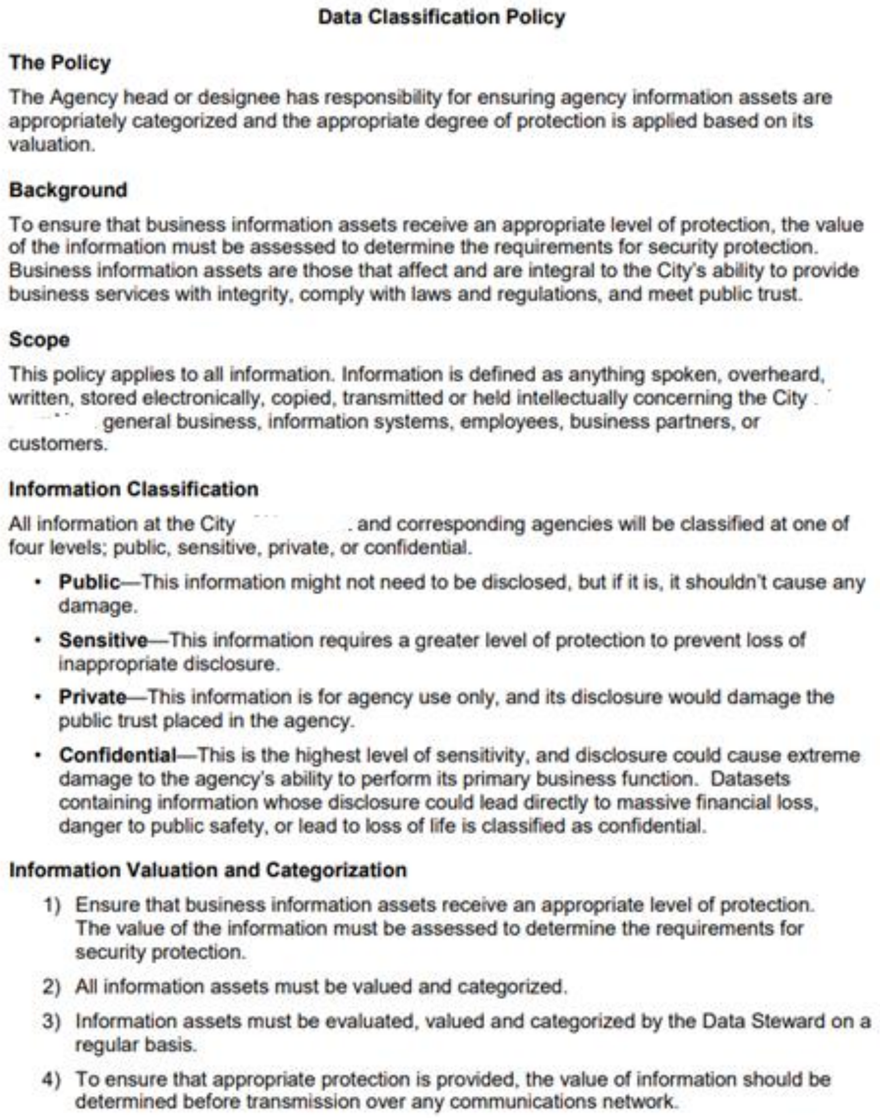


NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations



RA-02	**SECURITY CATEGORIZATION**
	ASSESSMENT OBJECTIVE: *Determine if:*
RA-02a.	the system and the information it processes, stores, and transmits are categorized;
RA-02b.	the security categorization results, including supporting rationale, are documented in the security plan for the system;
RA-02c.	the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
RA-02-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and systems; security categorization documentation; system security plan; privacy plan; other relevant documents or records].
RA-02-Interview	[SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with security and privacy responsibilities].
RA-02-Test	[SELECT FROM: Organizational processes for security categorization].



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

Information Classification

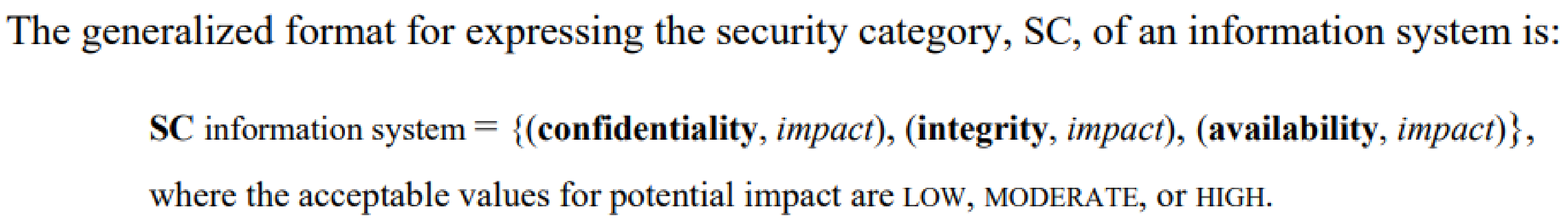
All information at the City . and corresponding agencies will be classified at one of four levels; public, sensitive, private, or confidential.

- **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.

Which do you prefer?

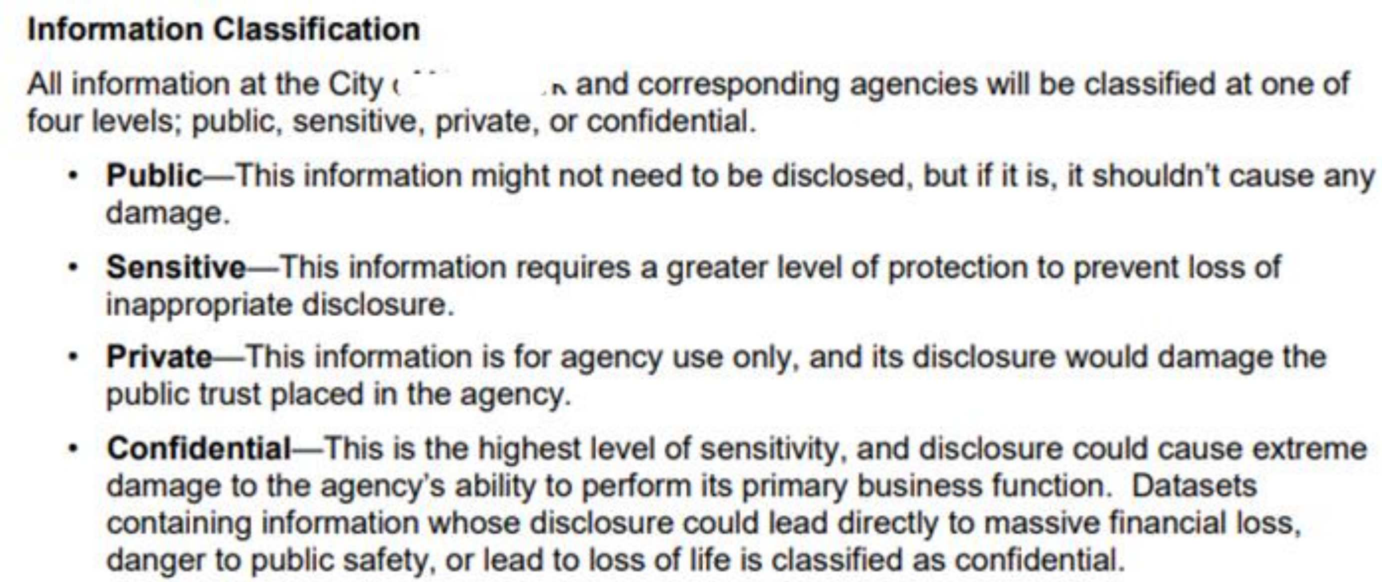


The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

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

…or…



Information Classification

All information at the City [redacted] 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.

Why?

Agenda

- ✓ Vocabulary
- ✓ Data Classification Process and Models
- CISA test taking tip
- Quiz

Test Taking Tip

- Look for “subset” questions -

Often you will encounter questions that ask you to chose the “Best” answer…

The idea is: At least two of the answers are correct in some sense, but one is “more correct” than the others

It can be useful to view these types of questions as having some possible answers that are actually subsets of the most correct answer

Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack
b) Surveillance attack
c) Social engineering attack
d) Man-in-the-middle attack

Test Taking Tip

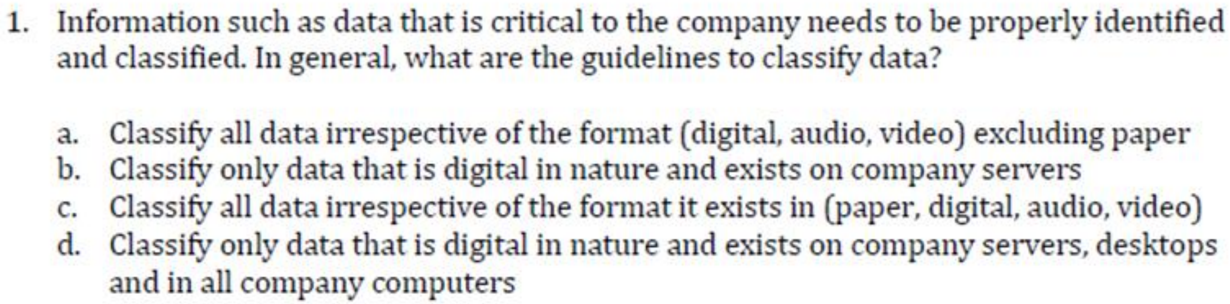
Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack
b) Surveillance attack
c) Social engineering attack
d) Man-in-the-middle attack

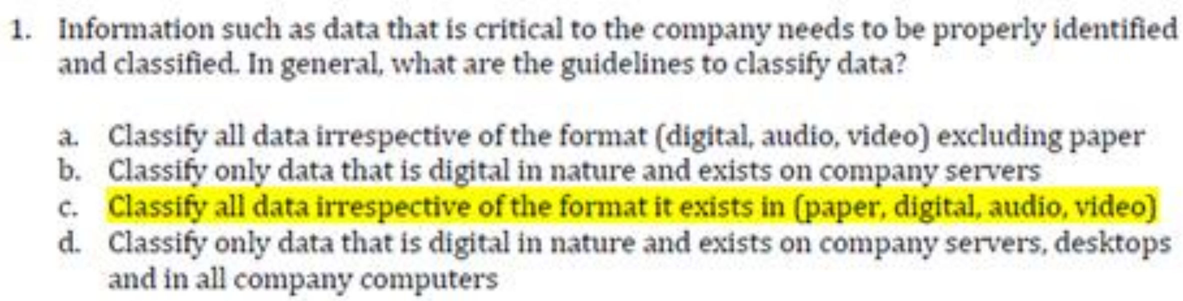
Answer: C

Quiz



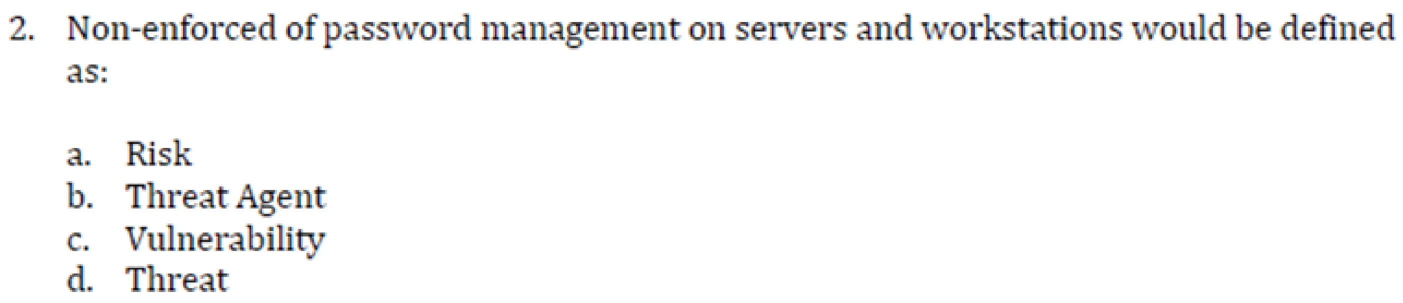
1. Information such as data that is critical to the company needs to be properly identified and classified. In general, what are the guidelines to classify data?

   a. Classify all data irrespective of the format (digital, audio, video) excluding paper
   b. Classify only data that is digital in nature and exists on company servers
   c. Classify all data irrespective of the format it exists in (paper, digital, audio, video)
   d. Classify only data that is digital in nature and exists on company servers, desktops and in all company computers



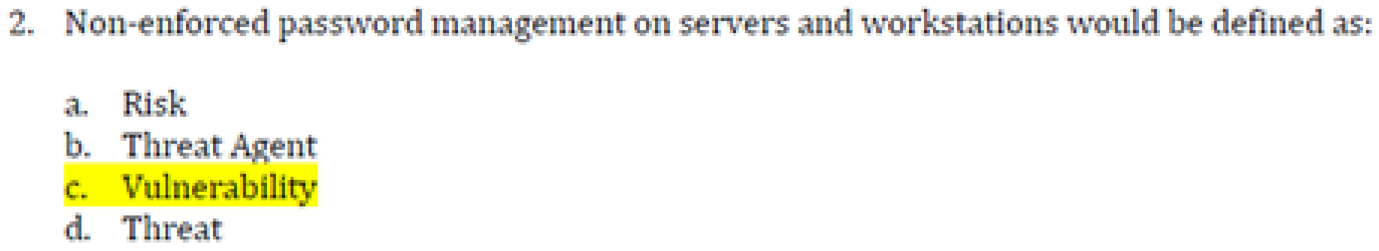
1. Information such as data that is critical to the company needs to be properly identified and classified. In general, what are the guidelines to classify data?

   a. Classify all data irrespective of the format (digital, audio, video) excluding paper
   b. Classify only data that is digital in nature and exists on company servers
   c. Classify all data irrespective of the format it exists in (paper, digital, audio, video)
   d. Classify only data that is digital in nature and exists on company servers, desktops and in all company computers



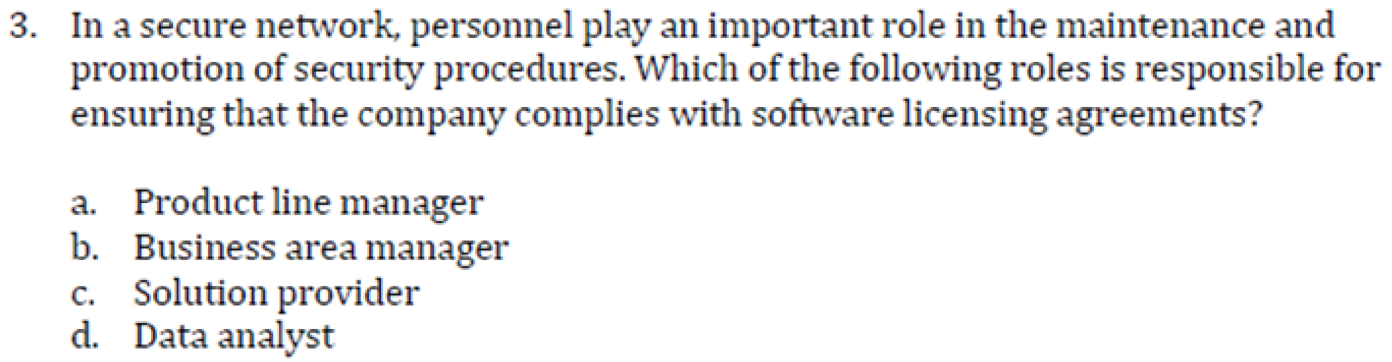
2. Non-enforced of password management on servers and workstations would be defined as:

    a. Risk
    b. Threat Agent
    c. Vulnerability
    d. Threat



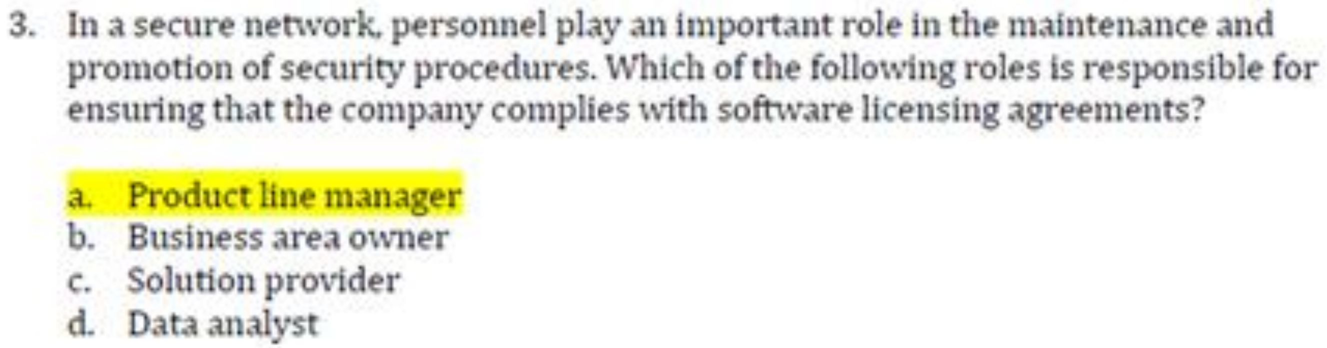
2. Non-enforced password management on servers and workstations would be defined as:

    a. Risk
    b. Threat Agent
    c. Vulnerability
    d. Threat



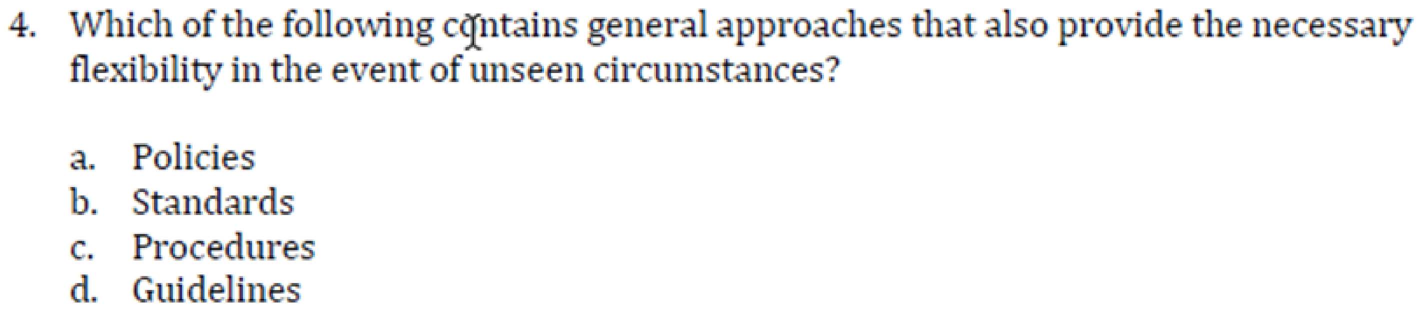
3. In a secure network, personnel play an important role in the maintenance and promotion of security procedures. Which of the following roles is responsible for ensuring that the company complies with software licensing agreements?

   a. Product line manager
   b. Business area manager
   c. Solution provider
   d. Data analyst



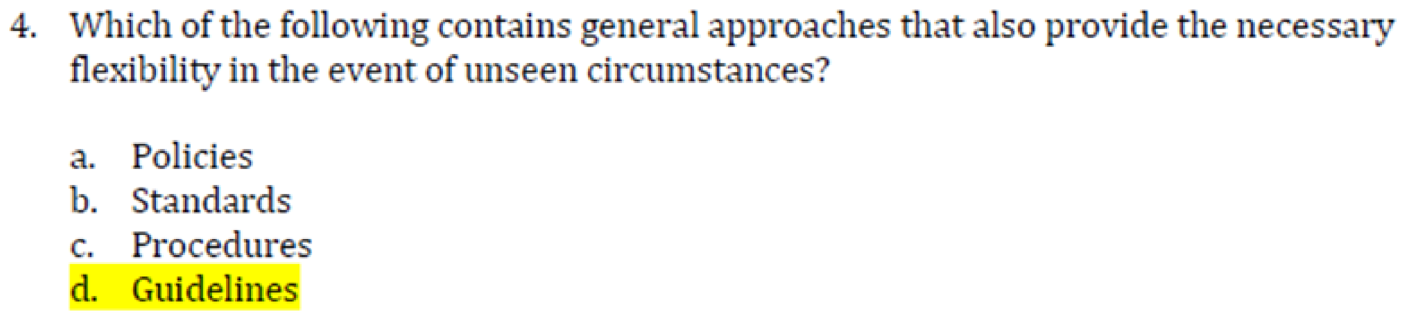
3. In a secure network, personnel play an important role in the maintenance and promotion of security procedures. Which of the following roles is responsible for ensuring that the company complies with software licensing agreements?

   a. Product line manager
   b. Business area owner
   c. Solution provider
   d. Data analyst



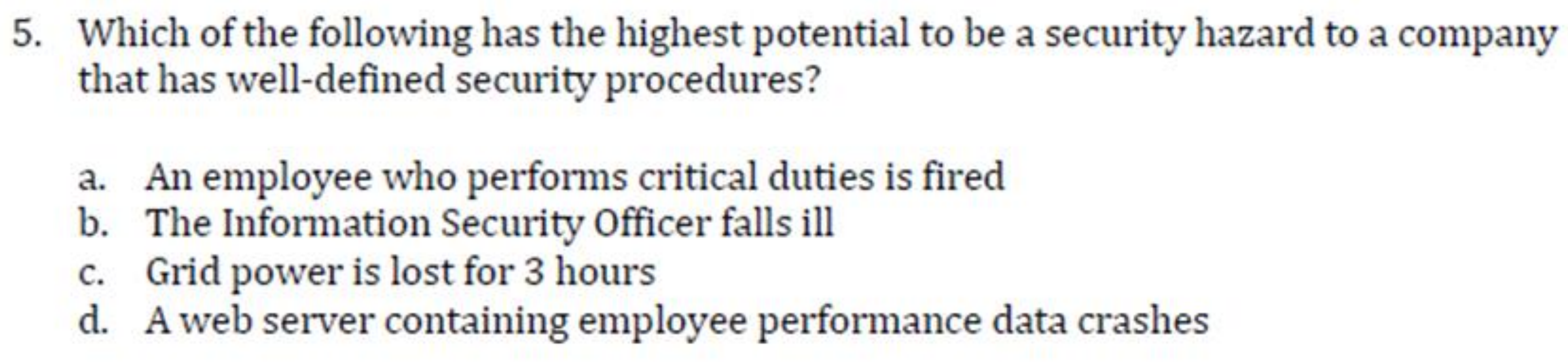
4. Which of the following contains general approaches that also provide the necessary flexibility in the event of unseen circumstances?

   a. Policies
   b. Standards
   c. Procedures
   d. Guidelines



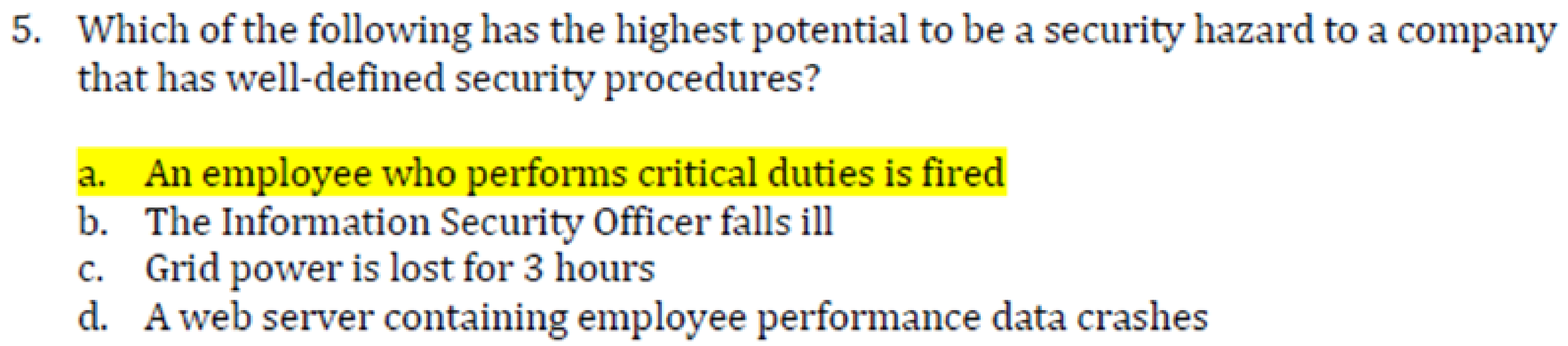
4. Which of the following contains general approaches that also provide the necessary flexibility in the event of unseen circumstances?

   a. Policies
   b. Standards
   c. Procedures
   d. Guidelines



5. Which of the following has the highest potential to be a security hazard to a company that has well-defined security procedures?

   a. An employee who performs critical duties is fired
   b. The Information Security Officer falls ill
   c. Grid power is lost for 3 hours
   d. A web server containing employee performance data crashes



5. Which of the following has the highest potential to be a security hazard to a company that has well-defined security procedures?

   a. An employee who performs critical duties is fired
   b. The Information Security Officer falls ill
   c. Grid power is lost for 3 hours
   d. A web server containing employee performance data crashes

Agenda

- ✓ Vocabulary
- ✓ Data Classification Process and Models
- ✓ Test taking tip
- ✓ Quiz