MIS 5206
Protecting Information Assets
- Unit #2b -

Data Classification Processes and Models

Agenda

- Vocabulary: Taxonomies of Information Security Controls
- Data Classification Process and Models
- Vocabulary: Policy, Standard, Guideline, Procedure
- 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

Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

By Class

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 Phase

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		

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

Taxonomies of Information System Controls

By phase

- Preventive
- Detective
- Corrective
- Compensating

By modality

- Physical
- Technical
- Administrative

Juxtaposing taxonomies to improve understanding…

Modality

Phase / Controls	Administrative	Technical	Physical
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*

Agenda

- ✓Vocabulary: Taxonomies of Information Security Controls
- Data Classification Process and Models
- Vocabulary: Policy, Standard, Guideline, Procedure
- Test taking tip
- Quiz

Questions:

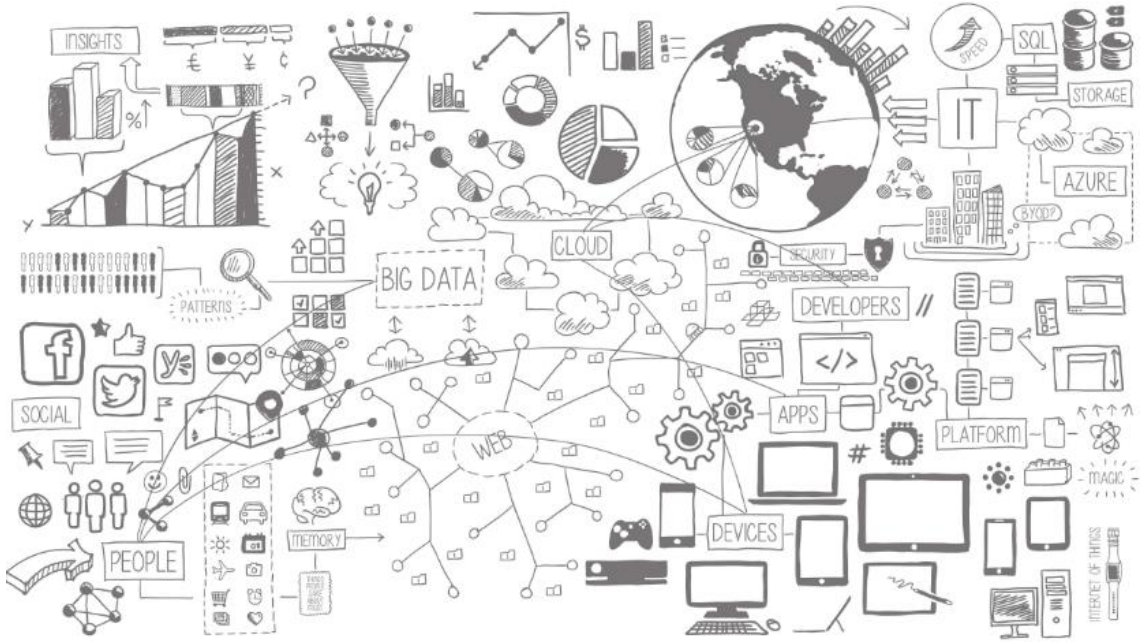
- What is data ?
- What is information ?
- How do data and information relate to each other?
- What is an information system?

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

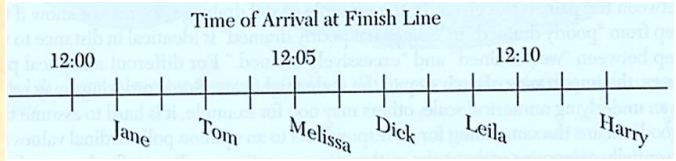
1. Nominal
2. Ordinal
3. Interval
4. Ratio

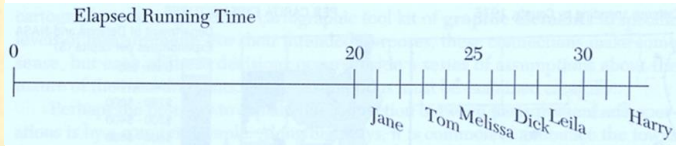
Increasing information content

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)

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

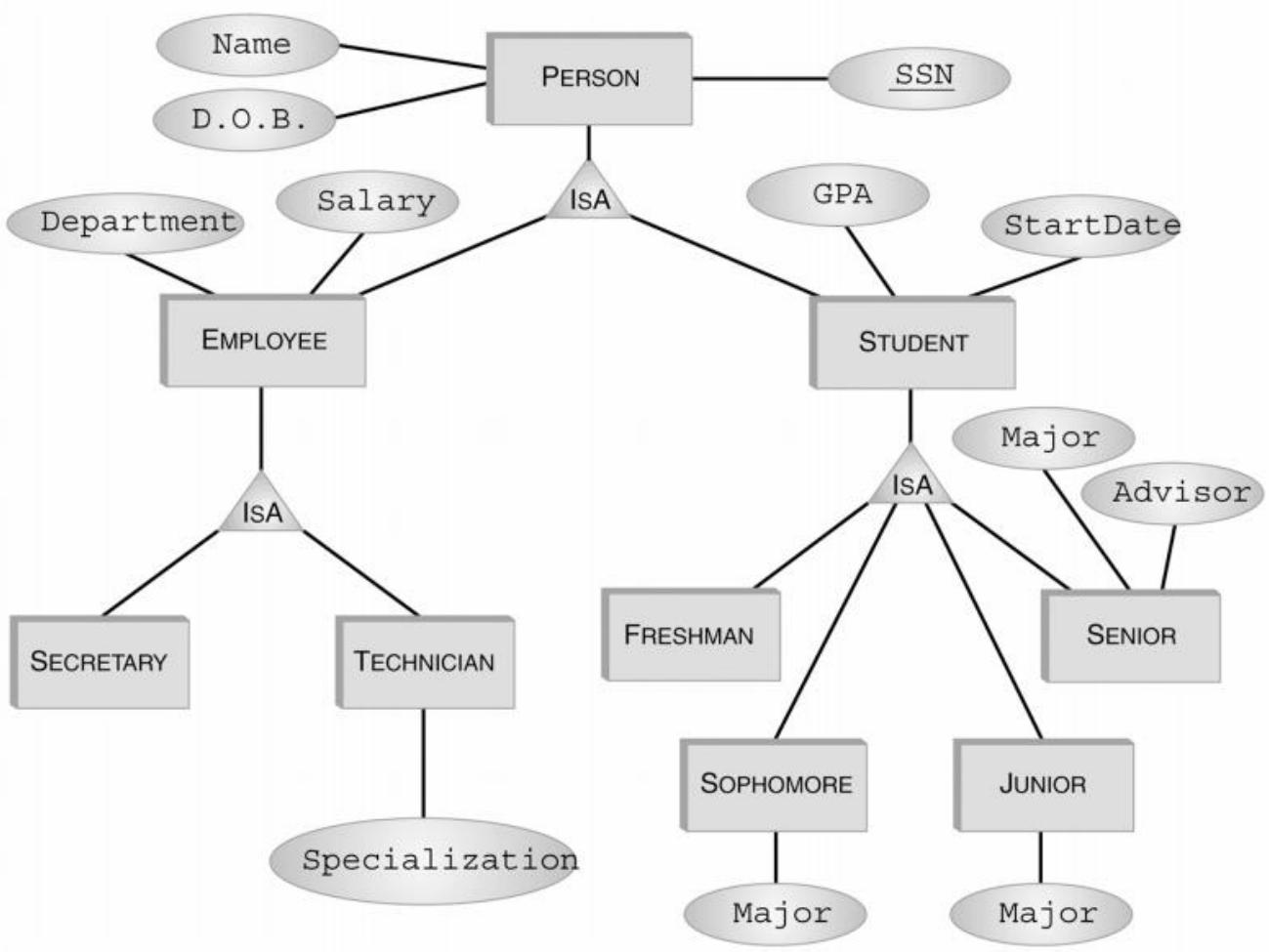




Entity Attribute Value Measurement Types

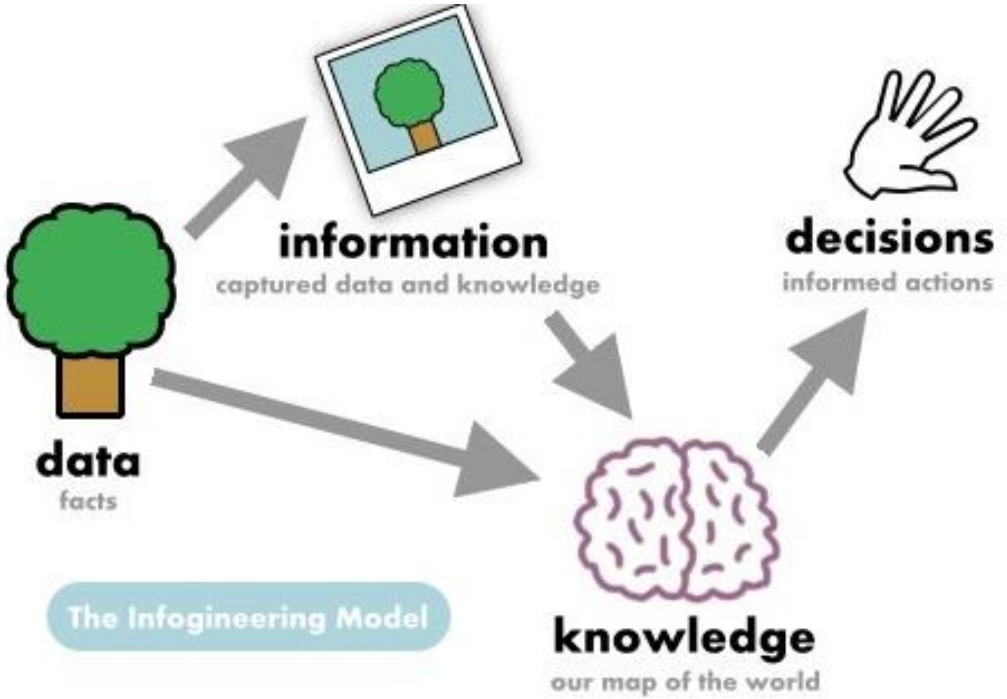
	Qualitative	**Quantitative**
Nominal	X	
Ordinal	X	
Interval		X
Ratio		X

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



How do data and information relate to each other ?

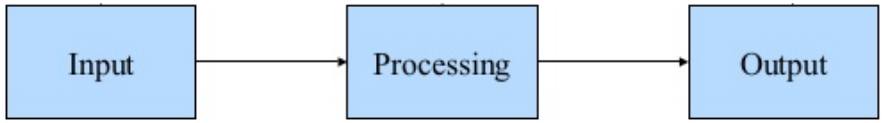
Information is data "put to work" in a decision-making context!



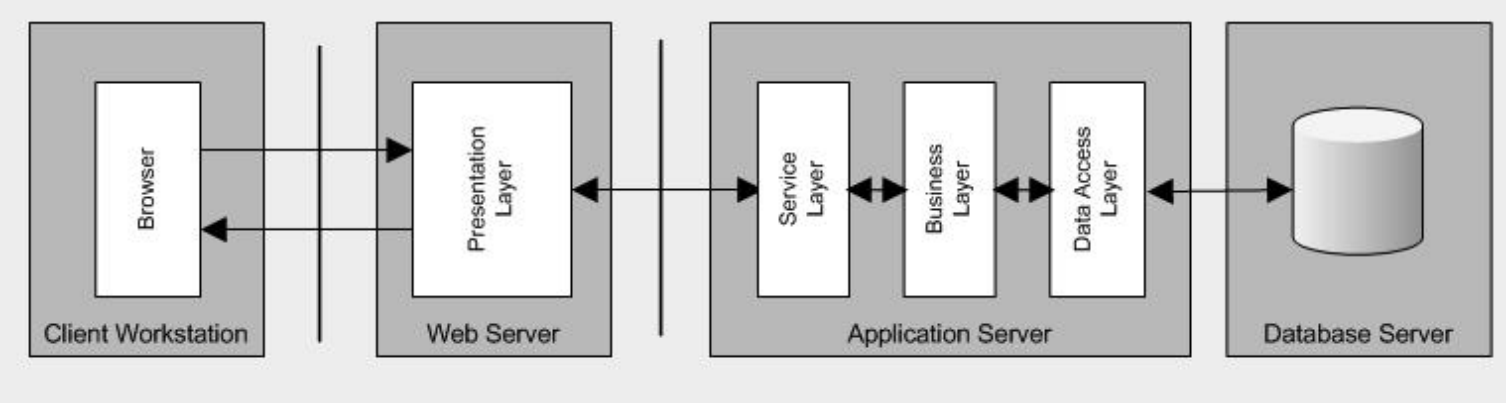
http://www.infogineering.net/data-information-knowledge.htm

What is an information system ?

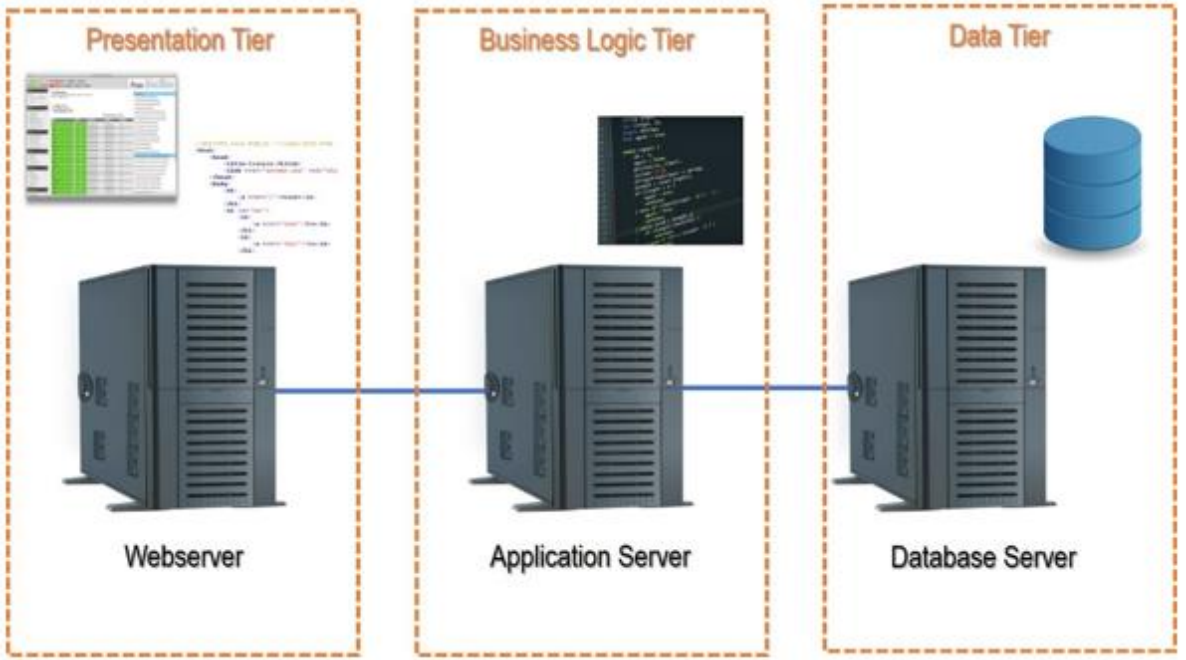
*"An **information system** (**IS**) is an organized system for the collection, organization, storage and communication of information. … Further, an information system (IS) is a group of components that interact to produce information."* Wikipedia



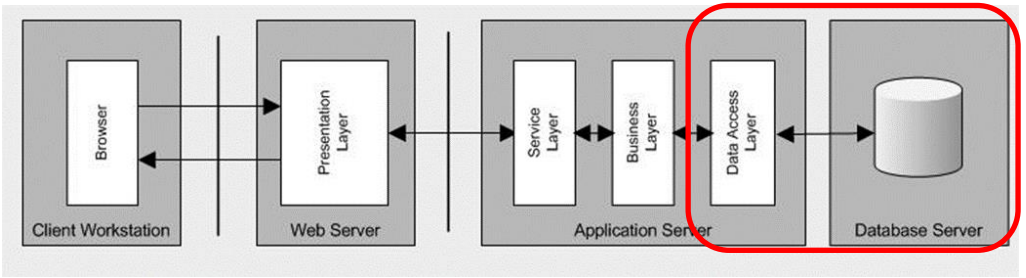
Information system (IS) architectures



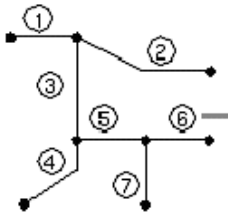
N-Tier Architecture examples



Information System Data



Coverage: Roads



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

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

Student Relation

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

Faculty 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

Course Relation

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

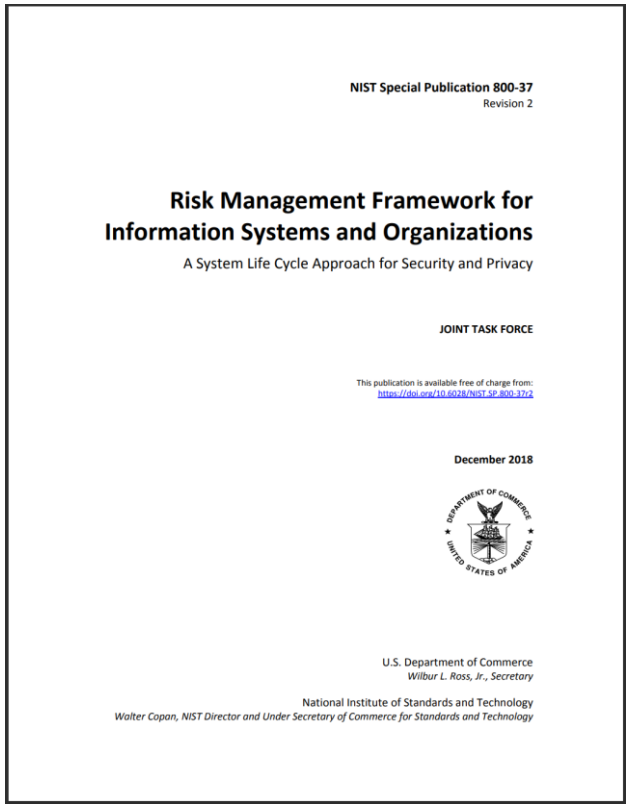
Enables determining the appropriate cost expenditure of security control mitigations required to protect the IT assets

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?


NIST Special Publication 800-37
Revision 2

Risk Management Framework for Information Systems and Organizations

A System Life Cycle Approach for Security and Privacy

JOINT TASK FORCE

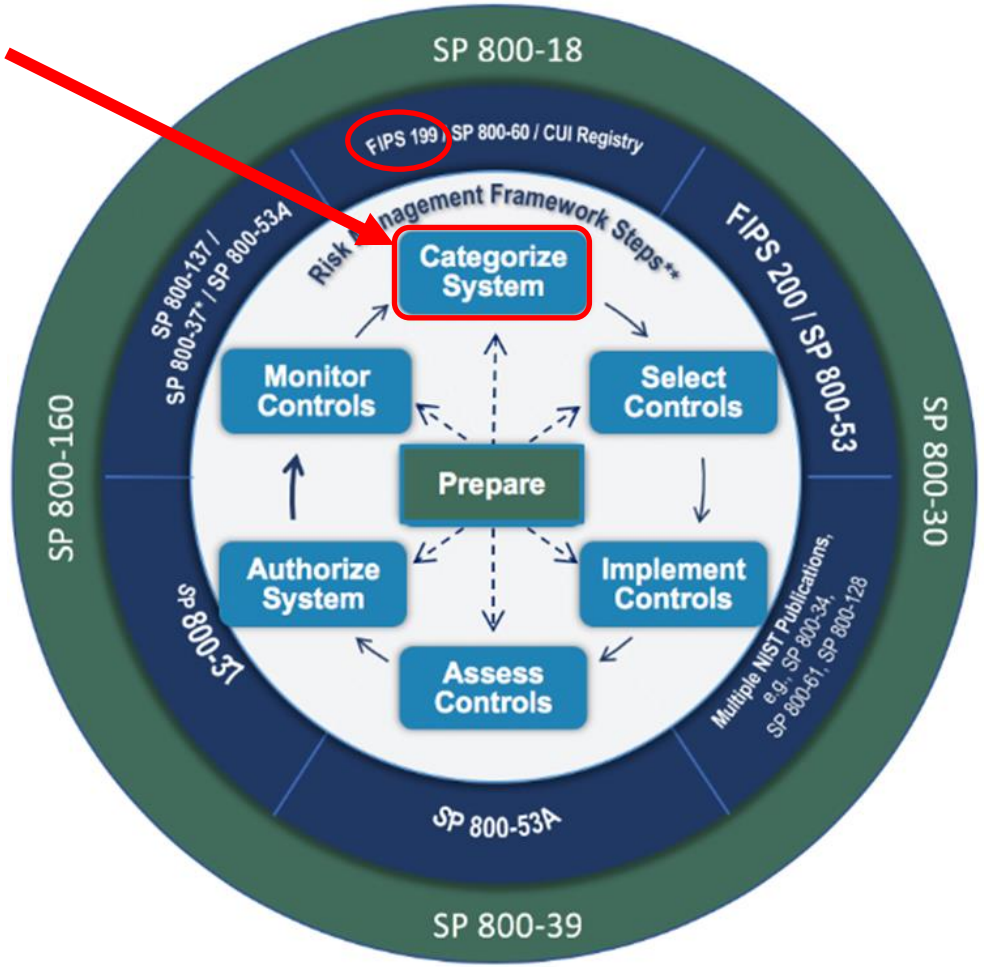
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-37r2

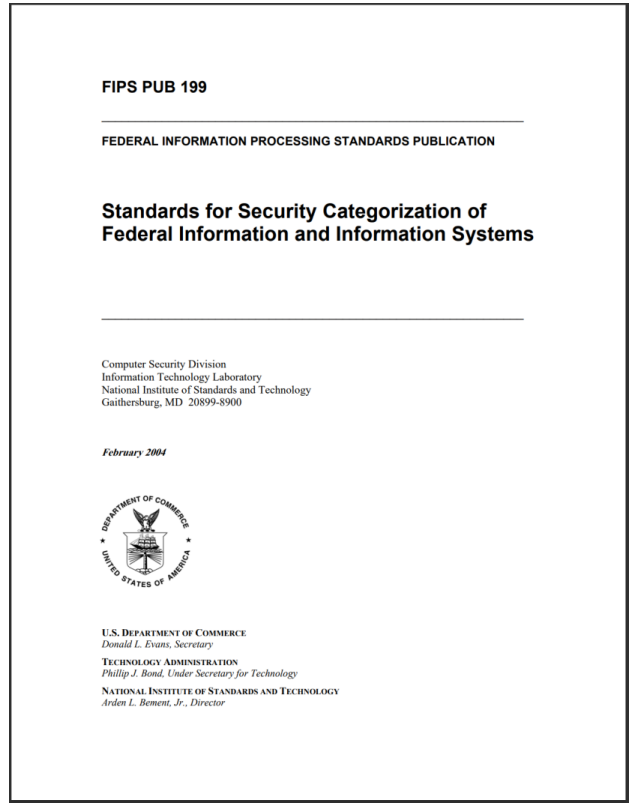
December 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Start here




FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

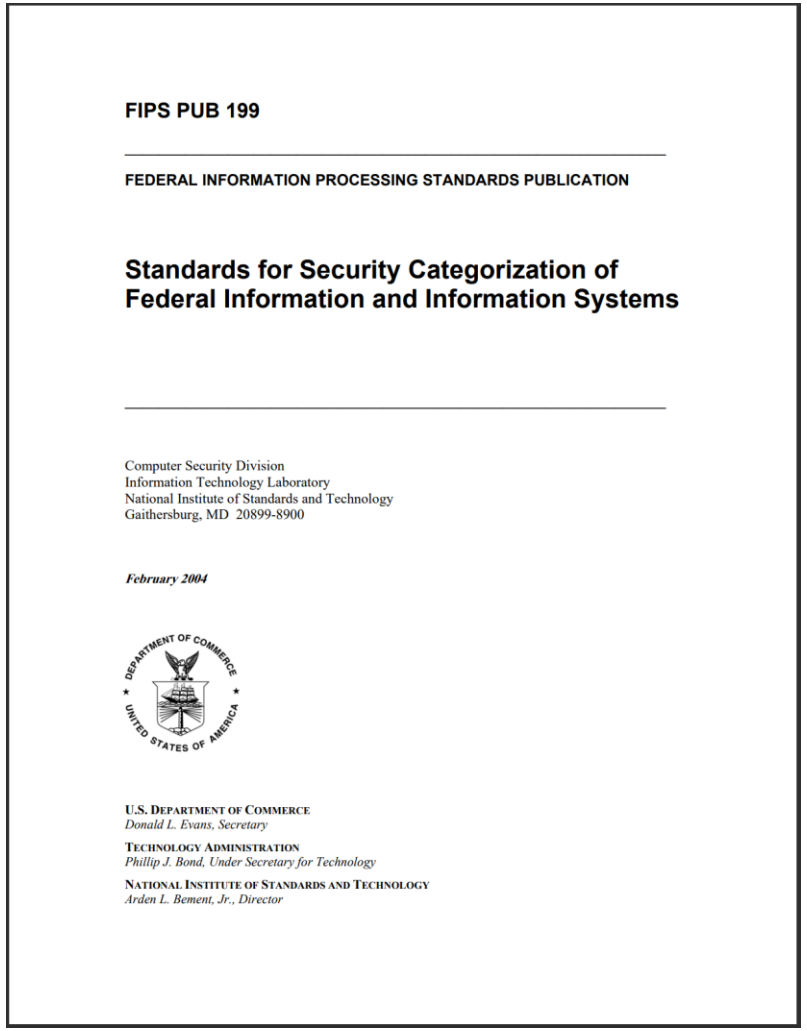
February 2004

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

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Security Categorization is based on 3 security objectives



FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

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

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

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

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.

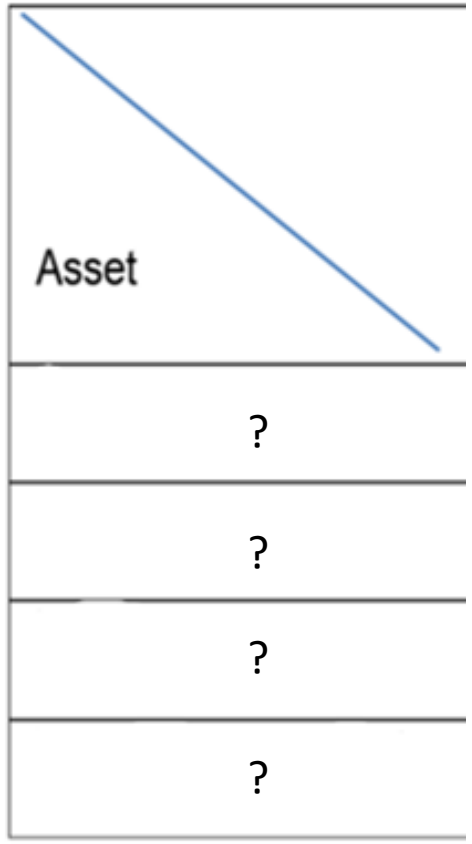
Question:

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 a confidentiality breach impact rating, an integrity breach impact rating, and an availability breach impact rating to each type of information contained on the Dean's laptop*
3. *Analyze the breach impact ratings to determine the overall security categorization for the laptop*

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



Asset
Staff Salary Data
Student Data
Fundraising Presentations
Dean's Personal Data

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

	Security Objective		
Asset	***Confidentiality***	***Integrity***	***Availability***
Staff Salary Data	Moderate	Moderate	Low
Student Data	Moderate	Moderate	Low
Fundraising Presentations	Low	Low	Low
Dean's Personal Data	High	Low	Low

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

Determination of security categorization of an information system is based on the security categorization of the types of information it contains…

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)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

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

	Security Objective		
Asset	***Confidentiality***	***Integrity***	***Availability***
Staff Salary Data	Moderate	Moderate	Low
Student Data	Moderate	Moderate	Low
Fundraising Presentations	Low	Low	Low
Dean's Personal Data	High	Low	Low
Overall Impact:	?	?	?

	Security Objective		
Asset	***Confidentiality***	***Integrity***	***Availability***
Staff Salary Data	Moderate	Moderate	Low
Student Data	Moderate	Moderate	Low
Fundraising Presentations	Low	Low	Low
Dean's Personal Data	High	Low	Low
Overall Impact:	High	Moderate	Low

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

	Security Objective			Security Categorization
Asset	***Confidentiality***	***Integrity***	***Availability***	
Staff Salary Data	Moderate	Moderate	Low	Moderate
Student Data	Moderate	Moderate	Low	Moderate
Fundraising Presentations	Low	Low	Low	Low
Dean's Personal Data	High	Low	Low	High
Overall Impact	**High**	**Moderate**	**Low**	

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

	Security Objective			Security Categorization
Asset	***Confidentiality***	***Integrity***	***Availability***	
Staff Salary Data	Moderate	Moderate	Low	Moderate
Student Data	Moderate	Moderate	Low	Moderate
Fundraising Presentations	Low	Low	Low	Low
Dean's Personal Data	High	Low	Low	High
Overall Impact:	High	Moderate	Low	**High**

Agenda

- ✓Vocabulary: Taxonomies of Information Security Controls
- ✓Data Classification Process and Models
- Vocabulary: Policy, Standard, Guideline, Procedure
- Test taking tip
- Quiz

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 if applied based on its valuation.

Background
To ensure that business 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 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.

How would you audit the application of this information security 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 if applied based on its valuation.

Background
To ensure that business 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 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.

Which security classification do you prefer?

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

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

…or…

- **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 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?

Evolution of a Security Classification Policy

Data Classification Policy

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

Background
To ensure that business 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 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.

[NYC Citywide Information Classification Policy]

5.0 Requirements

5.1 Information must be classified according to the following criteria:

5.1.1 Restricted Information: Information shall be designated as "Restricted" if the unauthorized disclosure, alteration or destruction of such information could be expected to have a **severe or catastrophic** adverse effect on the City's operations, organizational assets, or individuals.

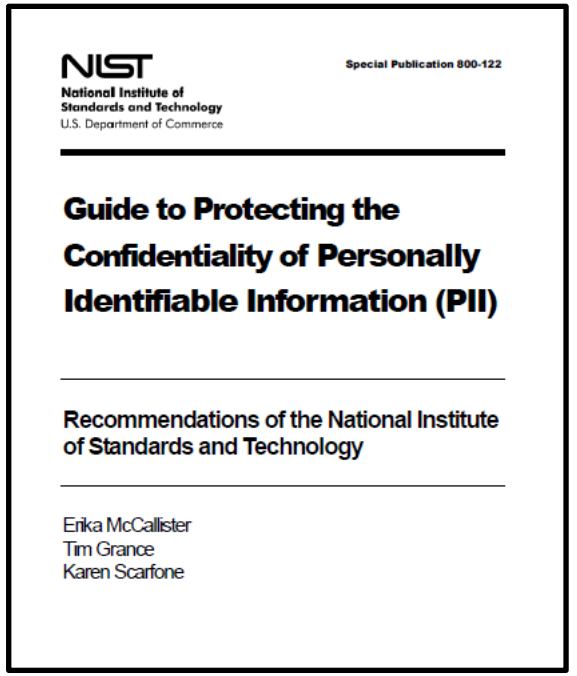
5.1.2 Sensitive Information: Information shall be designated as "Sensitive" if the unauthorized disclosure, alteration or destruction of such information could be expected to have a **serious** adverse effect on the City's operations, organizational assets, or individuals or if such information is only intended for internal use.

5.1.3 Non-Restricted Information: Information shall be designated as "Non-Restricted" if the unauthorized disclosure, alteration or destruction of such information could be expected to have a **limited** adverse effect on the City's operations, organizational assets, or individuals, or if the public disclosure of such information is not likely to have an adverse effect on the ability of the City to deliver services efficiently and effectively.

5.1.4 Identifying Information: "Identifying Information" as defined in the New York City Administrative Code section 23-1201 and "Personal Identifying Information" as defined in the New York City Administrative Code section 10-501 must be classified as either "Sensitive" or "Restricted" Information, except where the Agency's privacy officer or the City's Chief Privacy Officer determines such classification is not required.

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

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

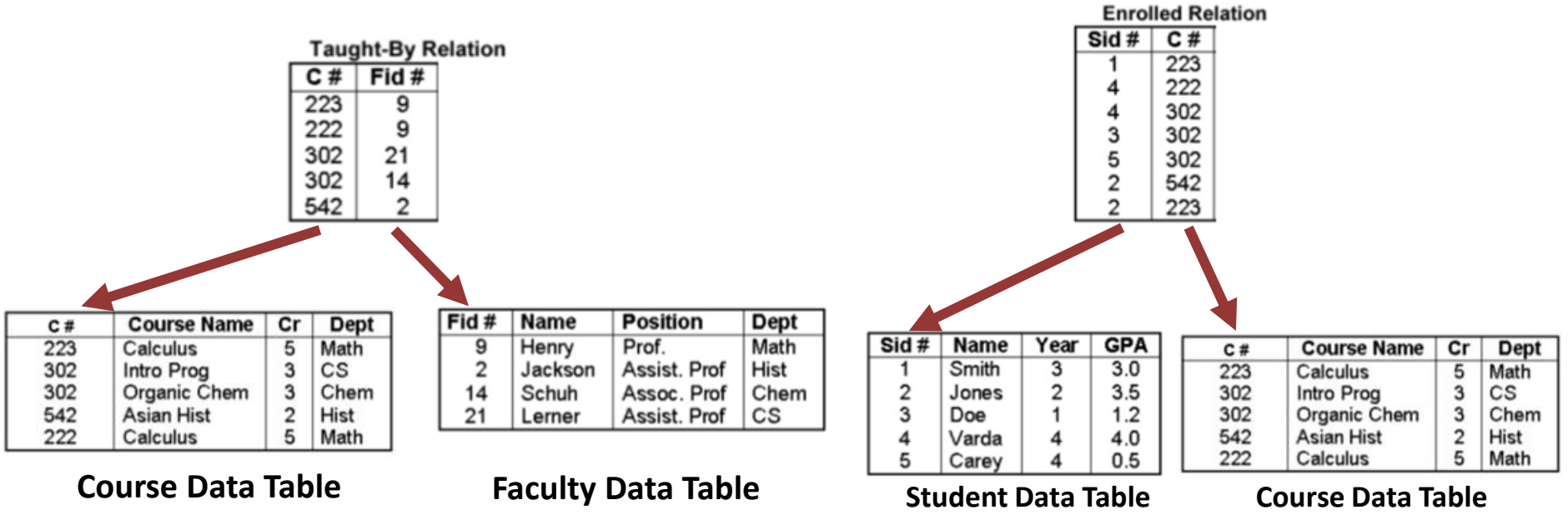


Personally Identifiable Information (PII)

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

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

Linked information in relational database



Taught-By Relation

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

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

Course Data Table

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

Faculty Data Table

Enrolled Relation

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

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

Student Data Table

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

Course Data Table

Linkable information

Property ("Parcel") Data Table

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

PIN is a common identifying number that can serve as a "foreign key" to link the data tables together

Owner Tax Data Table

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

Personally Identifiable Information (PII)

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

1. Any information that can be used to distinguish (i.e. identify) or trace an individual's identity, such as:
   - *Name*
   - *Identifying number*
   - *Address*
   - *Asset identifier*
   - *Telephone number*
   - *Personal characteristics*
   - *Personally owned property identifiers*

2. Any other information that is linked or linkable to the identifiers listed in #1:
   - Date of birth
   - Place of birth
   - Race
   - Religion
   - Weight
   - Geographic indicators
   - Medical information
   - Educational information
   - Financial information
   - Employment information
   - …

Is this PII ?

Property ("Parcel") Data Table

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

Owner Tax Data Table

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

Agenda

- ✓Vocabulary: Taxonomies of Information Security Controls
- ✓Data Classification Process and Models
- ✓Vocabulary: Policy, Standard, Guideline, Procedure
- Test taking tip
- Quiz

Test Taking Tip

- Read the answers first -

This contradicts many people's test taking recommendations…

…but, it works. Here's why:

- Quickly alerts you to the type of question to expect
- Focuses your attention in reading the question for meaningful information
- Gives you advanced warning that there may be more than one significant concepts (option to answer in the form "Both A & B")
- Gives you an opportunity to get a sense of the sort of answer the test maker is looking for
- There may be more than one valid answer, but the test maker may be looking for "best mitigation for the situation" or "least risk in the situation"

Test Taking Tip

Example:

A. Sensitivity
B. Source
C. Likelihood of theft
D. Likelihood of data loss

Test Taking Tip

Example:

Tony is developing a data classification system for his organization. What factor should he use as the primary driver when determining the classification level of each type of information?

A. Sensitivity
B. Source
C. Likelihood of theft
D. Likelihood of data loss

Test Taking Tip

Example:

Tony is developing a data classification system for his organization. What factor should he use as the primary driver when determining the classification level of each type of information?

A. Sensitivity
B. Source
C. Likelihood of theft
D. Likelihood of data loss

Answer: A

Quiz

1. Which of the choices below is the most often used criteria to determine the classification of a business object?

   a. Value
   b. Useful life
   c. Age
   d. Personal association

Quiz – Unit #2

1. Which of the choices below is the most often used criteria to determine the classification of a business object?

   a. Value
   b. Useful life
   c. Age
   d. Personal association

Quiz

2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

Quiz

2. Which of the below definitions is the best description of a vulnerability?

a. A weakness in a system that could be exploited
b. A company resource that is lost due to an incident
c. The minimum loss associated with an incident
d. A potential incident that could cause harm

Quiz

3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ratio for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats

Quiz

3. Which statement below best describes the purpose of risk analysis?

a. To develop a clear cost-to-value ration for implementing security controls
b. To influence the system design process
c. To influence site selection decisions
d. To quantify the impact of potential threats

Quiz

4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat
c. A number that represents the estimated frequency of an expected event
d. The percentage of loss that would be realized for a specific asset if a threat occurred

Quiz

4. What is an ARO?

a. A dollar figure assigned to a single event
b. The annual expected financial loss to an organization from a threat
c. A number that represents the estimated frequency of an expected event
d. The percentage of loss that would be realized for a specific asset if a threat occurred

Quiz

5. Which group represents the most likely source of an asset loss through in appropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs

Quiz

5. Which group represents the most likely source of an asset loss through in appropriate computer use?

a. Crackers
b. Hackers
c. Employees
d. Saboteurs

Agenda

- ✓Vocabulary: Taxonomies of Information Security Controls
- ✓Data Classification Process and Models
- ✓Vocabulary: Policy, Standard, Guideline, Procedure
- ✓Test taking tip
- ✓Quiz