



Cyber Security Unit – III

Dr. R. A. ROSELINE M.Sc., M.Phil., Ph.D.,
Associate Professor and Head,
Post Graduate Department Of Computer Applications,
Government Arts College, Coimbatore – 18.

Contents

Asset Classification

1. Introduction
2. Overview
3. Why Classify Information?
4. What is Information Classification?
5. Where to Begin?
6. Information Classification Category Examples
7. Resist the Urge to Add Categories
8. Constitution of Confidential Information
9. Employee Responsibilities
10. Classification Examples
11. Declassification of Information
12. Records Management Policy
13. Information Handling Standards Matrix
14. Information Classification Methodology
15. Authorization for Access.



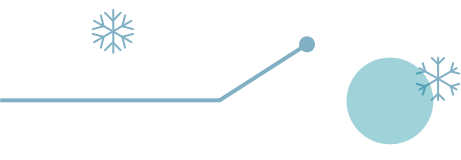
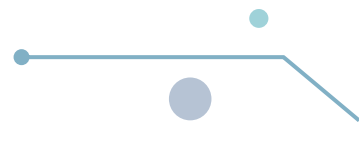
Asset Classification

1. Any security standard or best practice should be founded on a solid foundation of an asset classification.
2. To ensure proper protection of our information resources, it is necessary to define what an owner is and how that entity has ultimate responsibility for the information assets within its business unit, and this includes classification and assigning retention requirements.



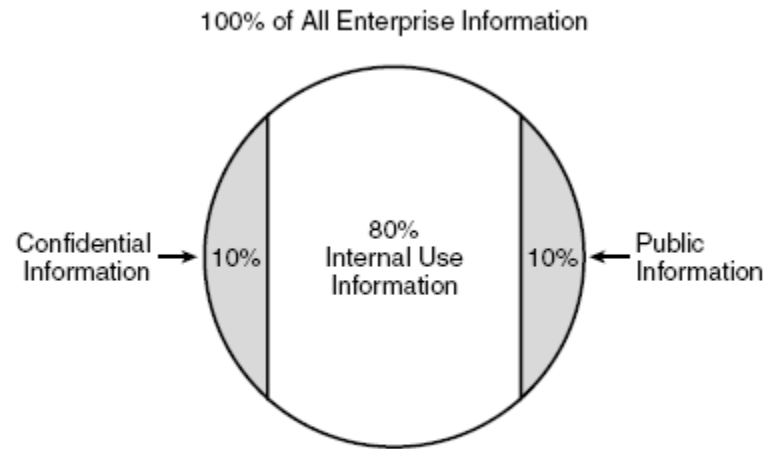


Overview

1. information classification is only one of the elements in an effective information management program.
 2. Knowing what we have and how important it is to the organization is key to the success for the information security program.
 3. The implementation of this program requires that representatives of the organization be charged with exercising the organization's proprietary rights.
- 
- 

Why Classify Information?

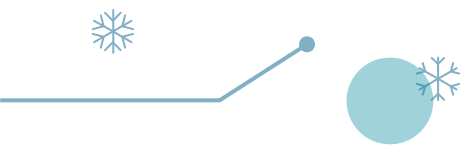
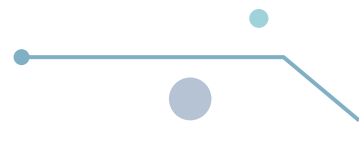
1. Organizations classify information to establish the appropriate levels of protection for these resources.
2. Because resources are limited, it is necessary to prioritize and identify what really needs protection.



| Information Classification Breakdown

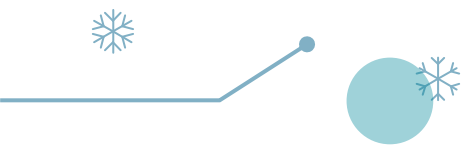
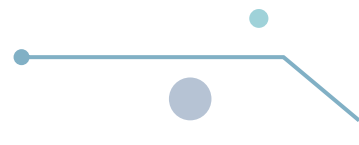


What Is Information Classification?

1. An information or asset classification process is a business decision process.
 2. Information is an asset of the organization, and managers have been charged with protecting and accounting for proper use of all assets. An information classification process will allow managers to meet this fiduciary responsibility.
 3. The role of the information security professional — or even information systems personnel — is one of advice and consulting. The final decision is made by the business unit managers or, as we will define soon, the asset owner.
- 
- 



Where to Begin?

1. By being a member of the Computer Security Institute (CSI), the Information System Security Association (ISSA), and the Information Systems Audit and Control Association (ISACA), I have ready access to people in my area that are usually willing to share examples of their work.
 2. The Internet can generate some examples of classification policies, but many of them are university or government agency related.
- 
- 



Information Classification Category Examples

Example 1: The manager can determine the level of criticality of an information asset

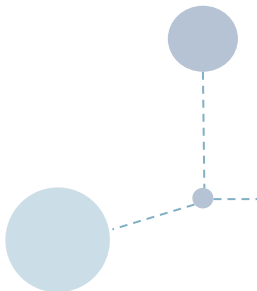
TABLE 5.1 Information Classification Category: Example 1

Mega Oil Corporation

- **HIGHLY CONFIDENTIAL** — Information whose unauthorized disclosure will cause the corporation severe financial, legal, or reputation damage. Examples: acquisitions data, bid details, contract negotiation strategies.
- **CONFIDENTIAL** — Information whose unauthorized disclosure may cause the corporation financial, legal, or reputation damage. Examples: employee personnel and payroll files, competitive advantage information.
- **GENERAL** — Information that, because of its personal, technical, or business sensitivity, is restricted for use within the company. Unless otherwise classified, all information within Amoco is in this category.

At this point in the classification scheme, this company has included a mechanism to establish the criticality of the information. It has established its three information classification categories and now adds three impact categories. Using these sets of definitions, the manager of information resources will be able to determine how critical the asset is to the company.

- **MAXIMUM** — Information whose unauthorized modification and destruction will cause the company severe financial, legal, or reputation damage.
- **MEDIUM** — Information whose unauthorized modification and destruction may cause the company financial, legal, or reputation damage. Examples: electronic funds transfer, payroll, and commercial checks.
- **MINIMUM** — Although an error in this data would be of minimal consequence, this is still important company information and therefore will require some minimal controls to ensure a minimal level of assurance that the integrity of the data is maintained. This applies to all data that is not placed in one of the above classifications. Examples: lease production data, expense data, financial data, and exploration data.
- **CRITICAL** — It is important to assess the availability requirements of data, applications, and systems. A business decision will be required to determine the length of unavailability that can be tolerated prior to expending additional resources to ensure the information availability that is required. Information should be labeled "CRITICAL" if it is determined that special procedures should be used to ensure its availability.





Example 2

This service provider has established five categories for use by managers in classifying information assets

TABLE 5.2 Criticality Matrix

<i>Business Impact</i>	<i>Classification Level</i>		
Maximum	1	2	3
Medium	2	2	3
Minimum	2	3	4

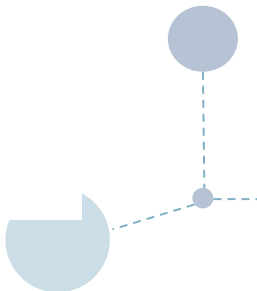
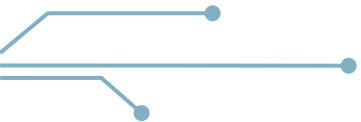
- 1: Availability safeguards must be implemented.
- 2: Availability safeguards should be implemented.
- 3: Continue to monitor availability requirements.
- 4: No additional action required at this time.

TABLE 5.3 Information Classification Category: Example 2

International Service Provider

- **Top Secret** — Information that, if disclosed, could cause severe impact to the company's competitive advantage or business strategies.
- **Confidential** — Information that, if disclosed, could violate the privacy of individuals, reduce competitive advantage, or damage the company.
- **Restricted** — Information that is available to a specific subset of the employee population when conducting company business.
- **Internal Use**— Information that is intended for use by all employees when conducting company business.
- **Public** — Information that has been made available to the public through authorized company channels.

- Make no copies
- Third-party confidential
- Attorney–client privileged document
- Distribution limited to ____
- Covered by a nonanalysis agreement



Example 3

1. The company that created it to find out how they use the Information Security Handbook included in this book also classification.

TABLE 5.4 Information Classification Category: Example 3

Global Manufacturer

- *Company Confidential Red* — Provides a significant competitive advantage. Disclosure would cause severe damage to operations. Relates to or describes a long-term strategy or critical business plans. Disclosure would cause regulatory or contractual liability. Disclosure would cause severe damage to our reputation or the public image. Disclosure would cause a severe loss of market share or the ability to be first to market. Disclosure would cause a loss of an important customer, shareholder, or business partner. Disclosure would cause a long-term or severe drop in stock value. Strong likelihood somebody is seeking to acquire this information.
- *Company Confidential Yellow* — Provides a competitive advantage. Disclosure could cause moderate damage to the company or an individual. Relates to or describes an important part of the operational direction of the company over time. Provides important technical or financial aspects of a product line or a business unit. Disclosure could cause a loss of customer or shareholder confidence. Disclosure could cause a temporary drop in stock value. Very likely that some third party would seek to acquire this information.
- *Company Confidential Green* — Might provide a business advantage over those who do not have access to the same information. Might be useful to a competitor. Not easily identifiable by inspection of a product. Not generally known outside the company or available from public sources. Generally available internally. Little competitive interest.
- *Company Public* — Would not provide a business or competitive advantage. Routinely made available to interested members of the general public. Little or no competitive interest.

Example 4

1. The company also requires that specific levels of information contain appropriate markings to identify it as classified information.

TABLE 5.5 Information Classification Category: Example 4

- *Company CONFIDENTIAL* — A subset of Company Internal information, the unauthorized disclosure or compromise of which would likely have an adverse impact on the company's competitive position, tarnish its reputation, or embarrass an individual. Examples: customer, financial, pricing, or personnel data; merger/acquisition, product, or marketing plans; new product designs, proprietary processes and systems.
- *Company INTERNAL* — All forms of proprietary information originated or owned by the Company, or entrusted to it by others. Examples: organization charts, policies, procedures, phone directories, some types of training materials.
- *Company PUBLIC* — Information officially released by the Company for widespread public disclosure. Example: press releases, public marketing materials, employment advertising, annual reports, product brochures, the public Web site, etc.



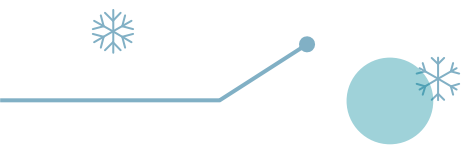
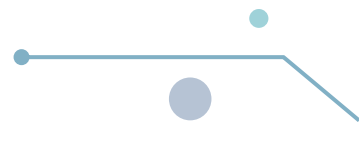
Resist the Urge to Add Categories

1. Keep the number of information classification categories to as few as possible. If two possible categories do not require substantially different treatment, then combine them.
2. The more categories available, the greater the chance for confusion among managers and employees. Normally, three or four categories should be sufficient to meet your organization's needs.





What Constitutes Confidential Information

1. There are a number of ways to look at information that can be classified as confidential.
 2. Information that is disclosed could violate the privacy of individuals, reduce the company's competitive advantage, or could cause damage to the organization.
 3. The Economic Espionage Act of 1996 (EEA) defines "trade secret" information to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," regardless of "how it is stored, compiled, or memorialized."
- 
- 



The EEA criminalizes the actions of anyone who:

1. Steals, or without authorization, appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret
2. Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade Secret
3. Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization
4. Conspires with one or more other persons to commit any offense described in the EEA under the heading “conspiracy”






Copyright

1. At regular intervals, employees will be creating new work in the form of application programs, transactions, systems, Web sites, etc.
 2. The types of work that qualify for copyright protection include:
 1. All types of written works
 2. Computer databases and software programs (including source code, object code, and micro code)
 3. Output (including customized screens and printouts)
 4. Photographs, charts, blueprints, technical drawings, and flowcharts
 5. Sound recordings
- 
- 



A copyright does not protect:

1. Ideas, inventions, processes, and three-dimensional designs (these are covered by patent law)
 2. Brands, products, or slogans (covered by trademark law)
- 



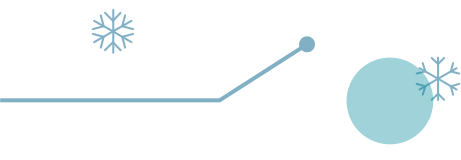
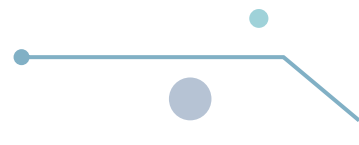
Employee Responsibilities

1. The “Information Owner” means the party who confides the referenced Confidential Information to the other party, the Confidant. Despite the name, the Information Owner benefits from a Confidentiality Engagement with respect to Confidential Information that it owns or possesses.
2. Three areas of employee responsibility: owner, user, and custodian.






1.Owner

1. The information owner is the entity within the organization that has been assigned the responsibility to exercise the organization's proprietary rights and grant access privileges to those with a true business need.
 2. This role is normally assigned to the senior level manager within the business unit where the information asset was created or is the primary user of that asset.
 3. The managers will have the ultimate responsibility for compliance but will probably delegate the day-to-day activities to some individual who reports to them.
- 
- 



Owners have the responsibility to:

1. Identify the classification level of all corporate information within their organizational unit
 2. Define and implement appropriate safeguards to ensure the confidentiality, integrity, and availability of the information resource
 3. Monitor safeguards to ensure their compliance and report situations of noncompliance
 4. Authorize access to those who have a business need for the information
 5. Remove access from those who no longer have a business need for the information
- 



Information Owner

1. The person who creates, or initiates the creation or storage, of the information is the initial owner. In an organization, possibly with divisions, departments, and sections, the owner becomes the unit itself, with the person responsible designated the “head” of the unit.





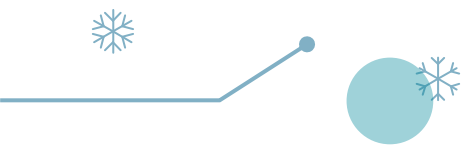
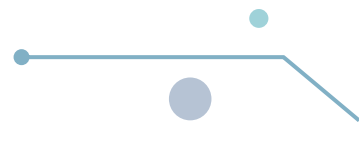
The information owner is responsible for ensuring that:

1. There exists an agreed-upon classification hierarchy, and this hierarchy is appropriate for the types of information processed for that business unit.
2. Classify all information stored into the agreed types and create an inventory (listing) of each type.
3. For each document or file within each classification category, append its agreed (confidentiality) classification. Its availability should be determined by the respective classification.
4. Ensure that, for each classification type, the appropriate level of information security safeguards is available (e.g., the log-on controls and access permissions applied by the Information Custodian provide the required levels of confidentiality).
5. Periodically check to ensure that information continues to be classified appropriately and that the safeguards remain valid and operative.



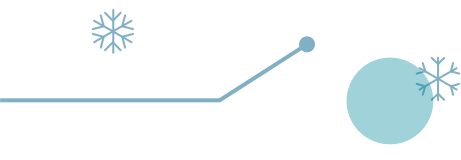
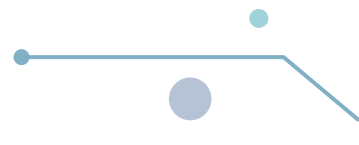


2.Custodian

1. An Information Custodian is the person responsible for overseeing and implementing the necessary safeguards to protect assets, at the level classified by the information owner.
 2. Custodians are authorized system support persons or organizations (employees, contractors, consultants, vendors, etc.) responsible for maintaining the safeguards established by owners. The owner designates the custodian.
 3. The custodian is the “steward of the data” for the owner; that is, the Data Center may be the custodian for business application “owned” by a business unit.
- 
- 

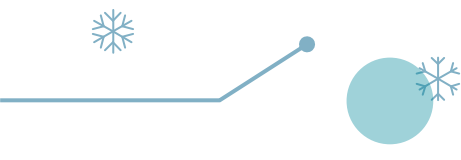
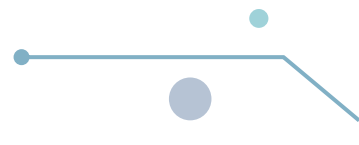


3. User

1. An information user is the person responsible for viewing, amending, or updating the content of the information assets. This can be any user of the information in the inventory created by the information owner.
 2. Users are authorized system users (employees, contractors, consultants, vendors, etc.) responsible for using and safeguarding information under their control according to the directions of the owner. Users are authorized access to information by the owner.
- 
- 

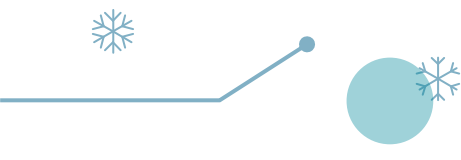
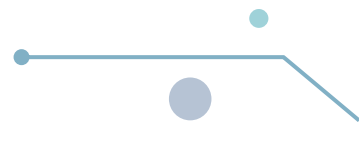


Classification Examples

1. This section examines attributes and examples of different classification categories, and presents examples of organization information classification policies.
 2. Classification: Example 1
 3. This is an actual classification policy (very high level) for the executive branch of a national government. There is little here to help the average user. This is an example of a program or general policy statement; however, a topic-specific policy statement may have been more beneficial.
- 
- 



Classification: Example 3

1. The policy seems to stress competitive advantage information in its opening paragraphs. It does not appear to address personal information about employees or customers.
 2. Classification: Example 3
 3. Example 3 does address the role of the owner but fails to define what an owner is. It does not address the issue of noncompliance, and the scope of the policy is vague.
- 
- 



Classification: Example 4

1. The intent of the policy states that “Information is a corporate asset and is the property of Corporation.” The scope of the policy states that “Corporate information includes electronically generated, printed, filmed, typed, or stored.” The responsibilities are well-established. The issue of compliance is the only policy element that appears lacking.





Declassification or Reclassification of Information

1. Information assets must be protected, stored, and then destroyed, based on a policy and a set of standards.
2. The Records Management Policy requires the owner to provide a brief description of the information record and the record retention requirements. These requirements will be a set of standards that support the Records Management Policy.





Records Management Policy

1. An organization's records are one of its most important and valuable assets. Almost every employee is responsible for creating or maintaining organization records of some kind, whether in the form of paper, computer data, optical disk, electronic mail, or voice-mail. Letters, memoranda, and contracts are obviously information records, as are things such as a desk calendar, an appointment book, or an expense record.





Information Handling Standards Matrix:

1. Printed Material
2. Electronically Stored Information
3. Electronically Transmitted Information
4. Record Management Retention Schedule





Information Classification Methodology

1. The final element in an effective information classification process is to provide management and employees with a method to evaluate information and provide them with an indication of where the information should be classified . To accomplish this, it may be necessary to create information classification worksheets. These worksheets can be used by the business units to determine what classifications of information they have within their organization.



TABLE 5.15 Information Classification Worksheet

Information Classification Review Worksheet

Organization: _____ Group: _____

Review Performed by/Phone: _____ Date: _____

		<i>Classifications (Select One)</i>			
		<i>CONFIDENTIAL</i>	<i>RESTRICTED</i>	<i>INTERNAL USE</i>	<i>PUBLIC</i>
<i>Information Name/Description</i>	<i>Storage Medium</i>	<i>If disclosed, could violate the privacy of individuals, reduce the company's competitive advantage, or cause damage to the company.</i>	<i>Intended for use by a subset of employees when conducting company business (usually regulatory requirement)</i>	<i>Intended for use by all employees when conducting company business.</i>	<i>Made available for public distribution through authorized company channels.</i>

Employee Records

- 1
- 2
- 3
- 4
- 5
- 6

Group Administrative Records

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Business Process Records

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10





Authorization for Access

1. there are typically three categories of employee responsibilities.
2. Depending on the specific information being accessed, an individual may fall into more than one category.
3. For example, an employee with a desktop workstation becomes the owner, custodian, and user.



