Infopercept

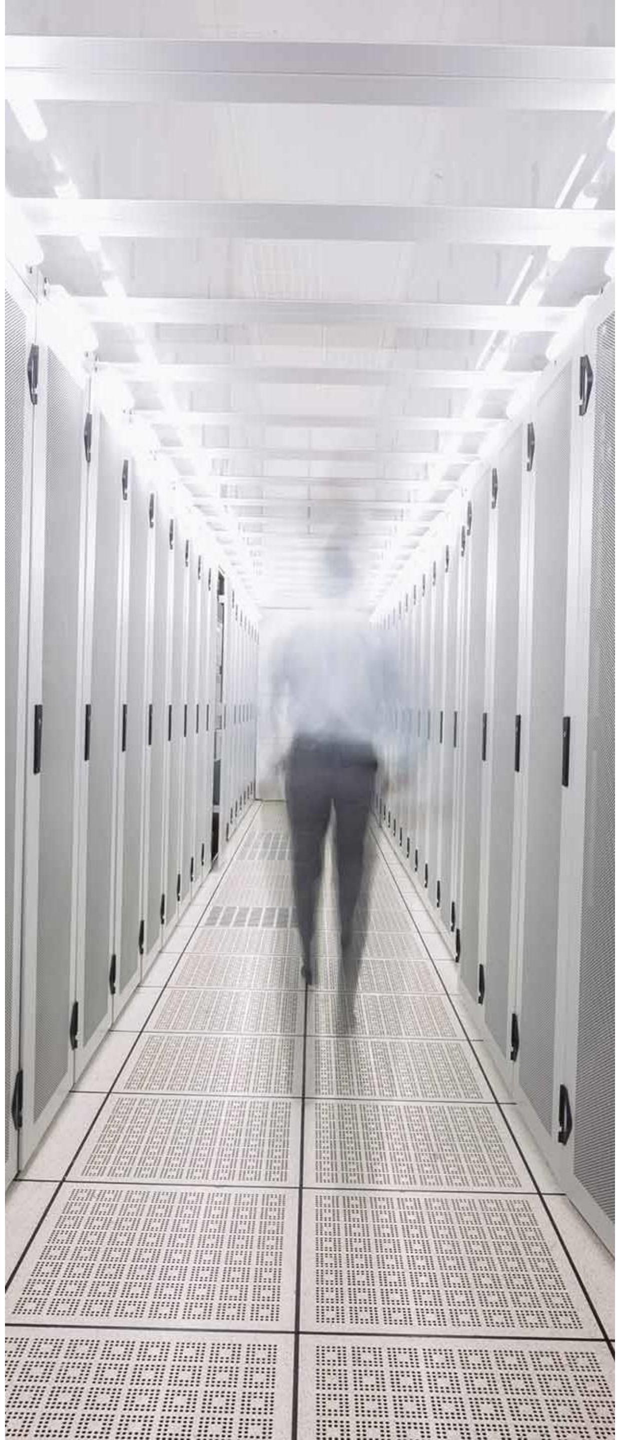
DATA CLASSIFICATION

Infopercept

Overview

What is Data Classification?

Data classification is broadly defined as the process of organizing data by relevant categories so that it may be used and protected more efficiently.



Benefits of Data Classification

- On a basic level, the classification process makes data easier to locate and retrieve.
- Data classification is of particular importance when it comes to risk management, compliance, and data security.
- Data classification involves tagging data to make it easily searchable and trackable.
- It also eliminates multiple duplications of data, which can reduce storage and backup costs while speeding up the search process.

REASON FOR DATA CLASSIFICATION

- Data may be classified for a number of reasons, including ease of access, maintaining regulatory compliance, and to meet various other business or personal objectives.

Literature Review

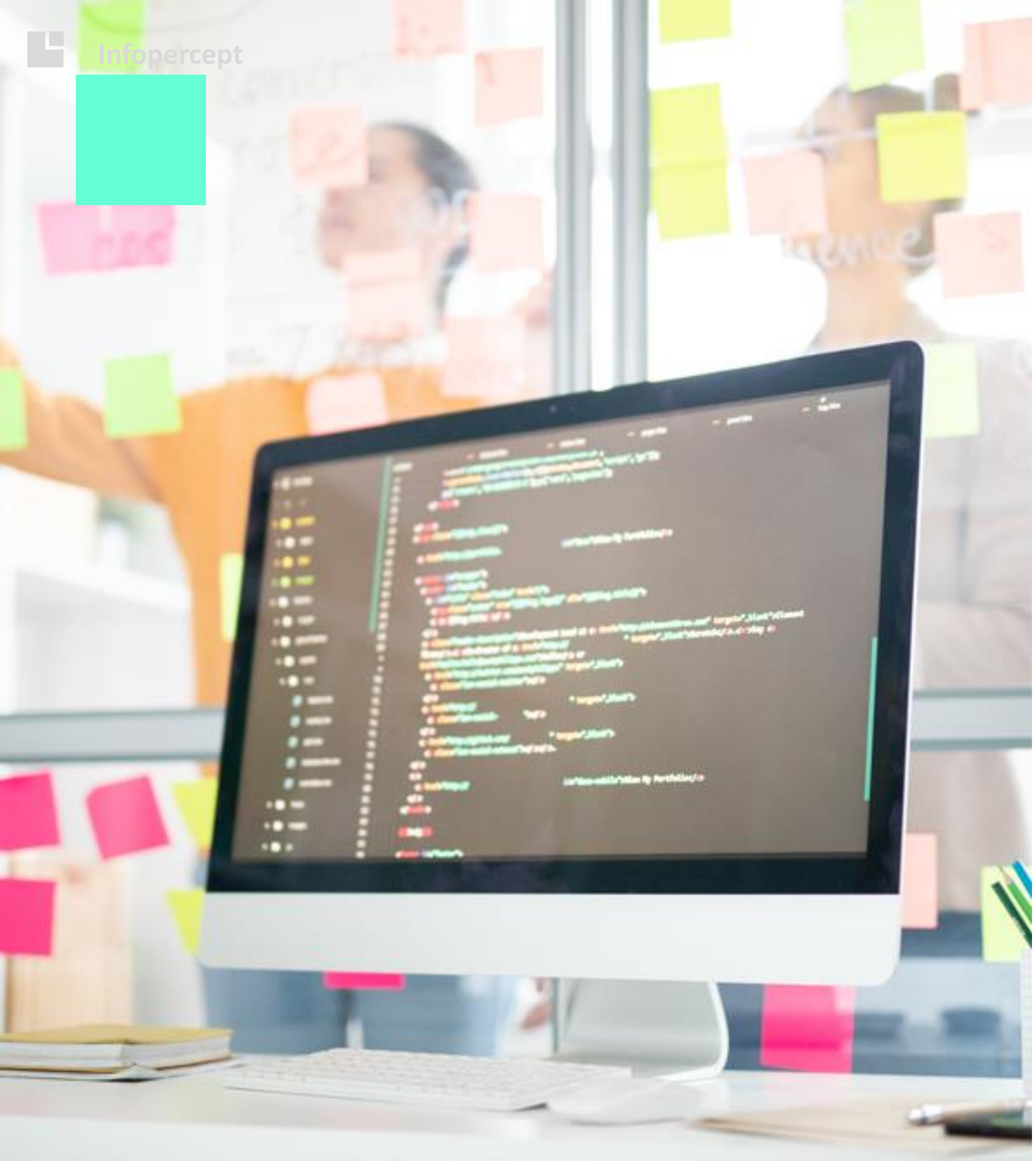
There are three main types of data classification that are considered industry standards:

Benefits of Data Classification

- **Content**-based classification inspects and interprets files looking for sensitive information.
- **Context**-based classification looks at application, location, or creator among other variables as indirect indicators of sensitive information.
- **User**-based classification depends on a manual, end-user selection of each document. User-based classification relies on user knowledge and discretion at creation, edit, review, or dissemination to flag sensitive documents.

Purpose of the Study

The purpose of the study is to know about data classification & the use and importance of classifying data while dealing with large chunks of data.



Findings

THE DATA CLASSIFICATION PROCESS

Automated systems can help streamline the process, but an enterprise must determine the categories and criteria that will be used to classify data, understand and define its objectives, outline the roles and responsibilities of employees in maintaining proper data classification protocols, and implement security standards that correspond with data categories and tags.

When done correctly, this process will provide employees and third parties involved in the storage, transmission, or retrieval of data with an operational framework.

Infopercept

Findings

STEPS FOR EFFECTIVE DATA CLASSIFICATION

- Understand the Current Setup: You must know what data you have before you can classify it.
- Creating a Data Classification Policy: Creating a policy should be your top priority.
- Prioritize and Organize Data: Decide on the best way to tag your data based on its sensitivity and privacy.
- Data sorting based on content/file type, size and time of data.
- Sorting for security reasons by classifying data into restricted, public or private data types.
- Some examples and applications of data classification include: Separating customer data based on gender.
- Identifying and keeping frequently used data in disk/memory cache.

GDPR DATA CLASSIFICATION

With the General Data Protection Regulation (GDPR) in effect, data classification is more imperative than ever for companies that store, transfer, or process data pertaining to EU citizens. It is crucial for these companies to classify data so that anything covered by the GDPR is easily identifiable and the appropriate security precautions can be taken.

Classification of data should be performed by an appropriate Data Steward. A data steward is a role within an organization responsible for utilizing an organization's data governance processes to ensure fitness of data elements - both the content and metadata.

On a periodic basis, it is important to reevaluate the classification of Institutional Data. If any change is found in classification of certain data set then an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing controls, they should be corrected in a timely manner.

Being able to accurately identify, manage, and secure data is imperative in an era where every sector, higher education included, is data-driven.

The goal of data classification policy is to allow users to understand, better manage, and employ an appropriate level of security for the data.

Most organization data classification policies assign data into three categories:

Public

data that typically is publicly accessible, requires minimal security controls, and poses little or no risk to the organization's reputation, resources, services, or individuals.

Confidential

data whose unauthorized disclosure may have moderate adverse effects on a organization's reputation, resources, services, or individuals. This is typically the default classification for most organizations and requires a moderate level of security.

Sensitive(or Restricted)

data whose unauthorized disclosure may have serious adverse effects on a organization's reputation, resources, services, or individuals. Typically, this includes data protected under federal or state regulations, or data that carries with it proprietary, ethical, or privacy considerations. Sensitive data requires the highest level of security.

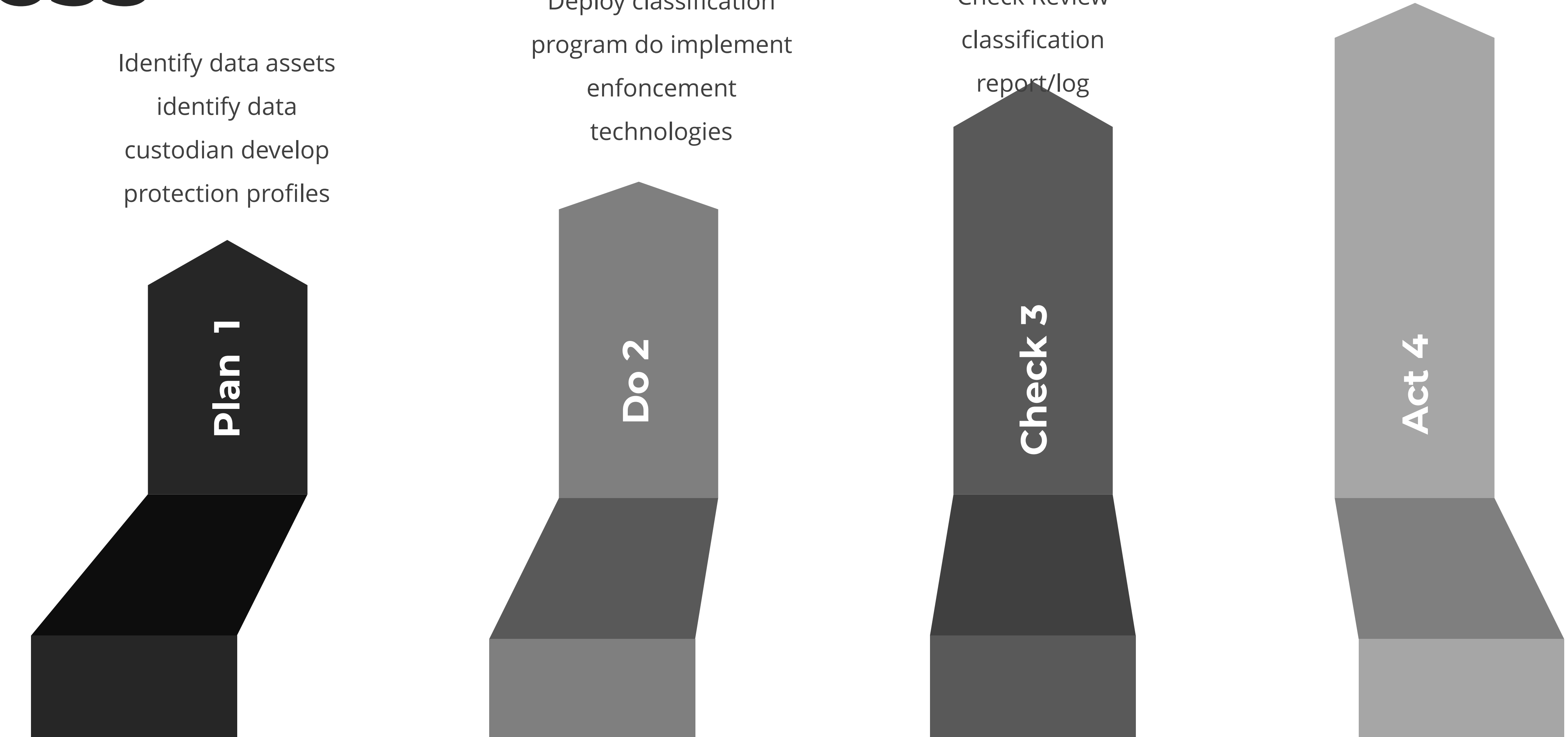
Categories of Data Classification

Public

Sensitive

Confindential

The Process



Plan 1

Identify data assets identify data custodian develop protection profiles

Do 2

Deploy classification program do implement enfoncement technologies

Check 3

Check Review classification report/log

Act 4

Reclassify data act

Thanks!

For More Information Please Visit our Website

www.infopercept.com