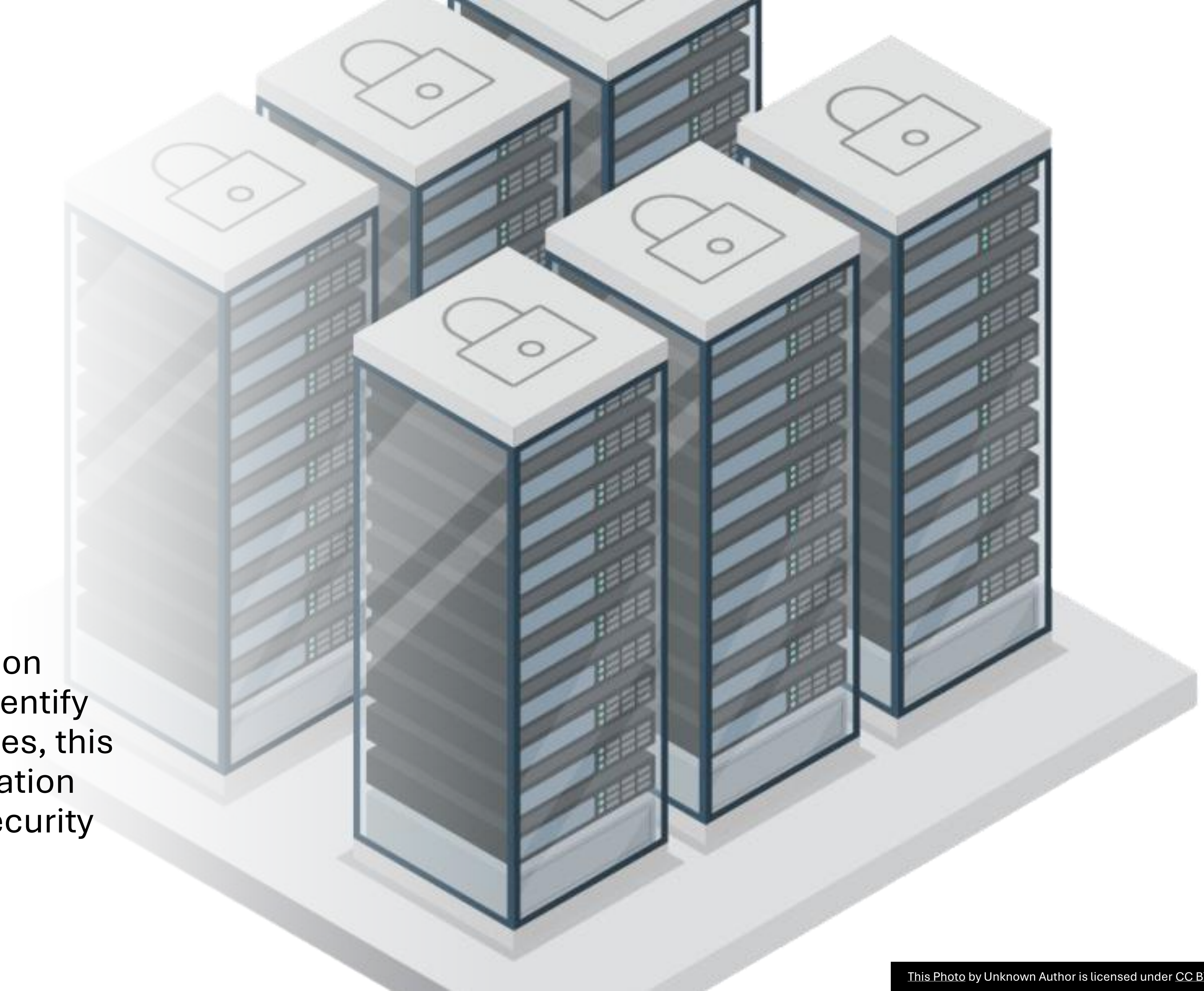
Project 1

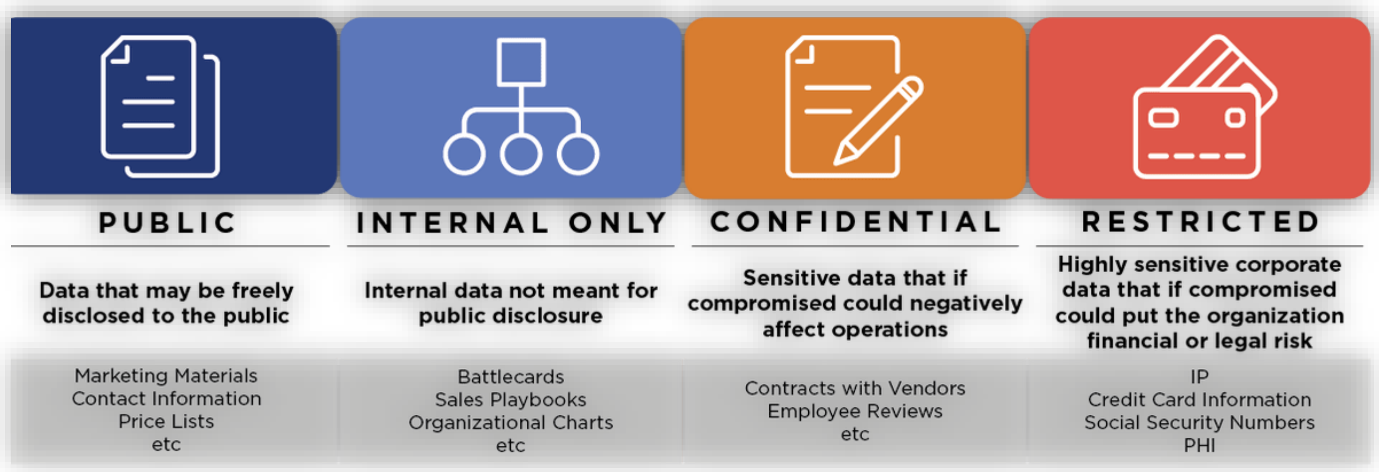
Fernando Parra

CSS 2754-001 – Host Security



To perform data classification standards, it is critical to identify the data that Fullsoft handles, this will set criteria for classification levels and define certain security controls that ensure their safeguard.

- Classification schemes typically categorize information into high, medium, and low sensitivity levels and differentiate between public and private information.
- In this manner, public, internal, sensitive, and highly sensitive data offers availability only to those authorized while strengthening Fullsoft’s security posture based on the sensitivity and criticality of the data that is being handled.

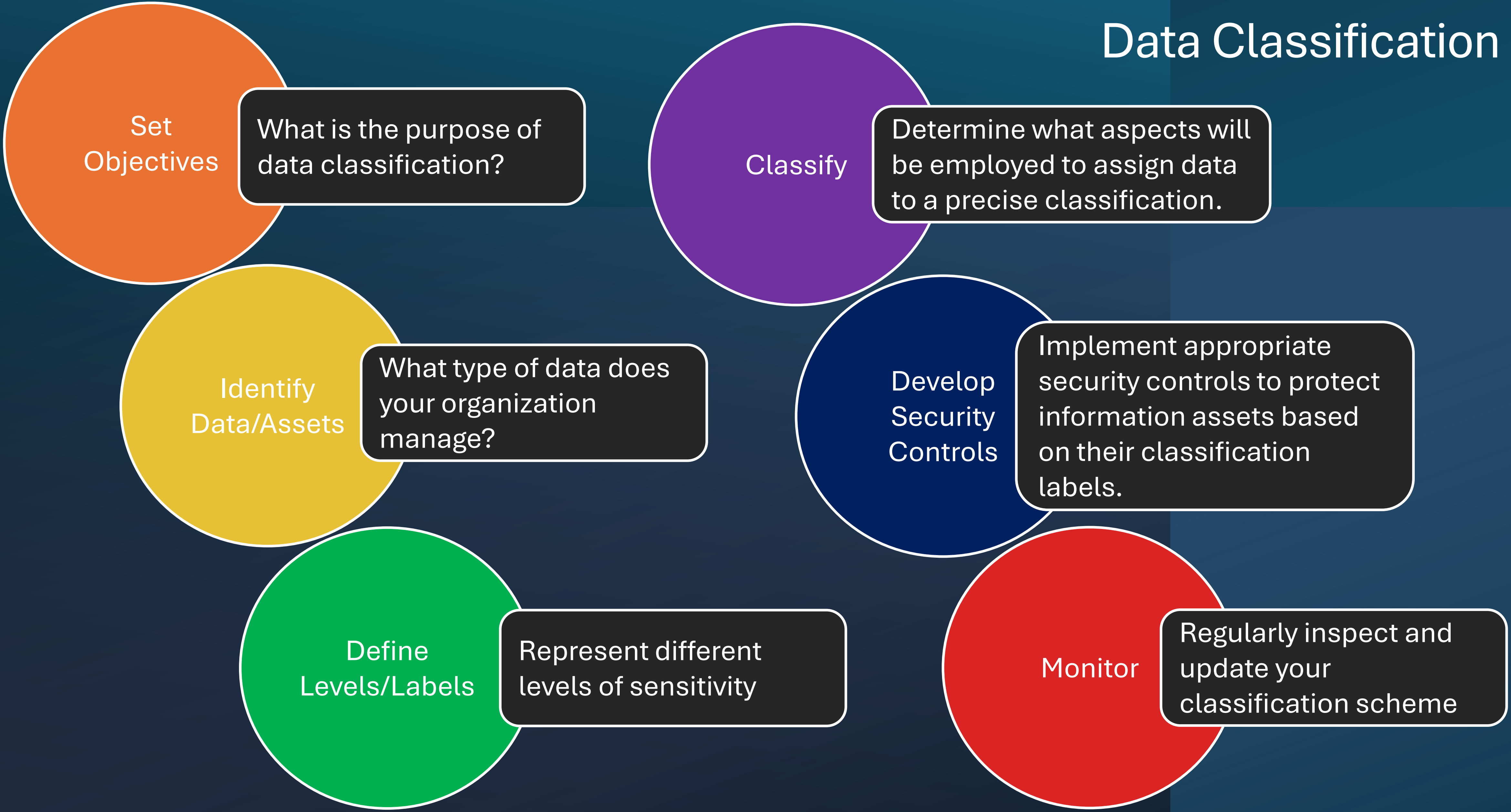


PUBLIC	INTERNAL ONLY	CONFIDENTIAL	RESTRICTED
Data that may be freely disclosed to the public	**Internal data not meant for public disclosure**	**Sensitive data that if compromised could negatively affect operations**	**Highly sensitive corporate data that if compromised could put the organization financial or legal risk**
Marketing Materials Contact Information Price Lists etc	Battlecards Sales Playbooks Organizational Charts etc	Contracts with Vendors Employee Reviews etc	IP Credit Card Information Social Security Numbers PHI

Source: https://www.linkedin.com/pulse/data-classification-compliance-looking-nuances-aaron-wagner/

Fullsoft’s specific concerns rely on their proprietary development code; the appropriate level for this type of data is confidential; it is not of internal/public use until it becomes a complete product, and it is considered intellectual property while in development.

Data Classification



Set Objectives

What is the purpose of data classification?

Identify Data/Assets

What type of data does your organization manage?

Define Levels/Labels

Represent different levels of sensitivity

Classify

Determine what aspects will be employed to assign data to a precise classification.

Develop Security Controls

Implement appropriate security controls to protect information assets based on their classification labels.

Monitor

Regularly inspect and update your classification scheme

Objective

Fullsoft aims to improve its security and compliance posture by identifying objectives to enhance data security.

Identify

The company will catalog its diverse data types, including customer information, software product development codes, financial records, and internal documents.

Labels and Levels

Fullsoft will establish classification levels such as public, internal, confidential, and private, tailoring security and access controls to each.

Classify

It will define classification criteria based on data type, legal requirements, business value, and the possible impact of threats.

Secure

Fullsoft will outline how confidential data is to be managed, securing it with controls, like encryption, back-ups, MFA, and specific data retention policies.

A company like Fullsoft requires strong encryption to protect sensitive information.

Monitor

To ensure long-term effectiveness, Fullsoft will continuously monitor and revise its classification scheme, ensuring alignment with business development and regulatory changes, while also encouraging constant compliance within the organization.

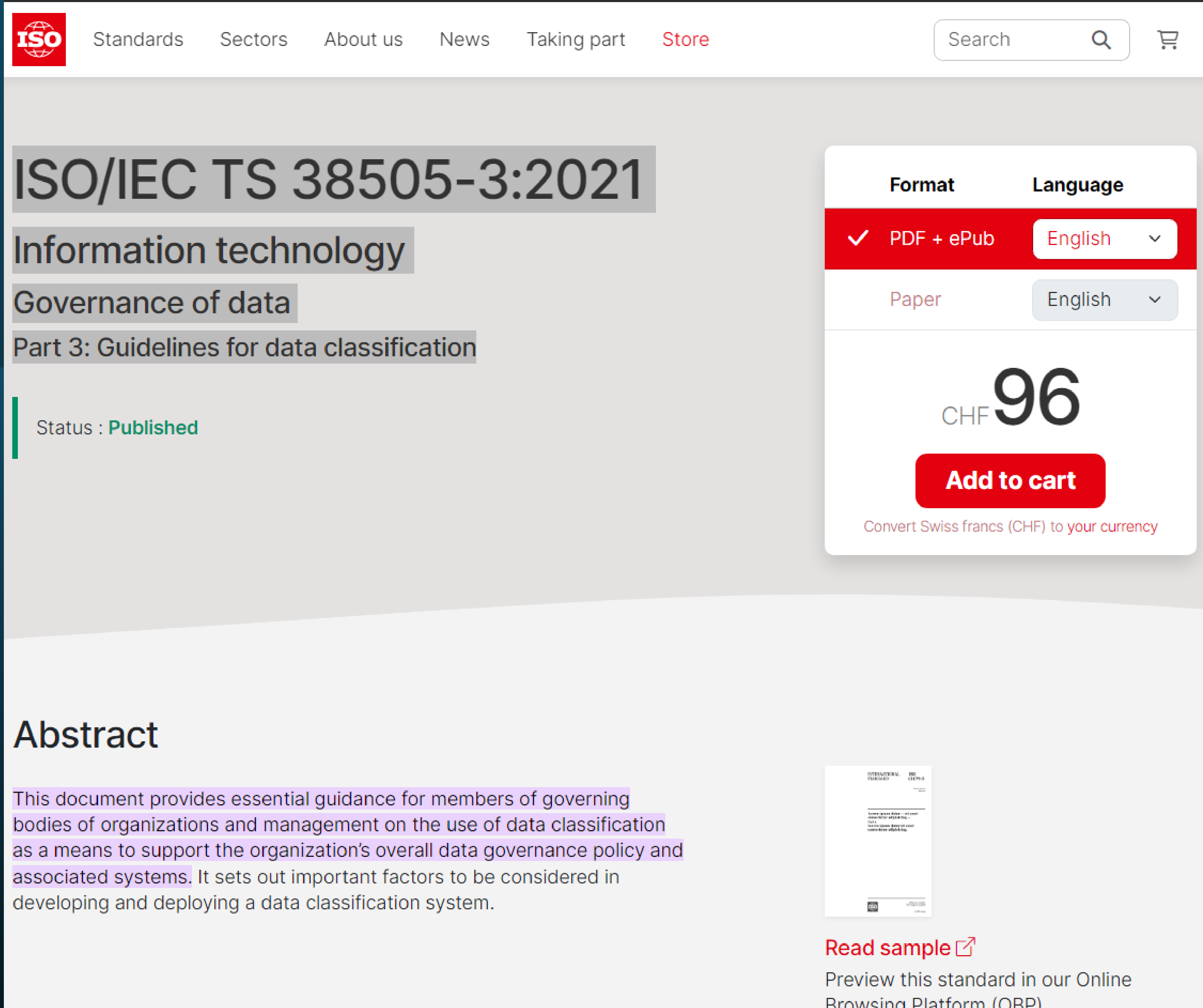
The processes, procedures, and controls that ensure the protection of confidential data also allow Fullsoft to adhere to regulations along the lines of GDPR, HIPPA, PCI, etc.

- The proper storage, handling, and access conditions for classified data are determined by an organization's security categories or classifications.
- This practice is highly encouraged
- Deleting files or formatting a hard disk is not enough to erase all data from a device once certain data is no longer in use. To prevent the recovery of data that has been deleted, security professionals should employ specialized tools to securely wipe storage devices

Professional Standards

- Standards such as ISO 27001 can support Fullsoft enforcing a robust and standardized data classification system.

Another standard from ISO with design especially for data classification can be found on the website.



ISO/IEC TS 38505-3:2021

Information technology

Governance of data

Part 3: Guidelines for data classification

Status : Published

Format	Language
✓ PDF + ePub	English
Paper	English

CHF 96

Convert Swiss francs (CHF) to your currency

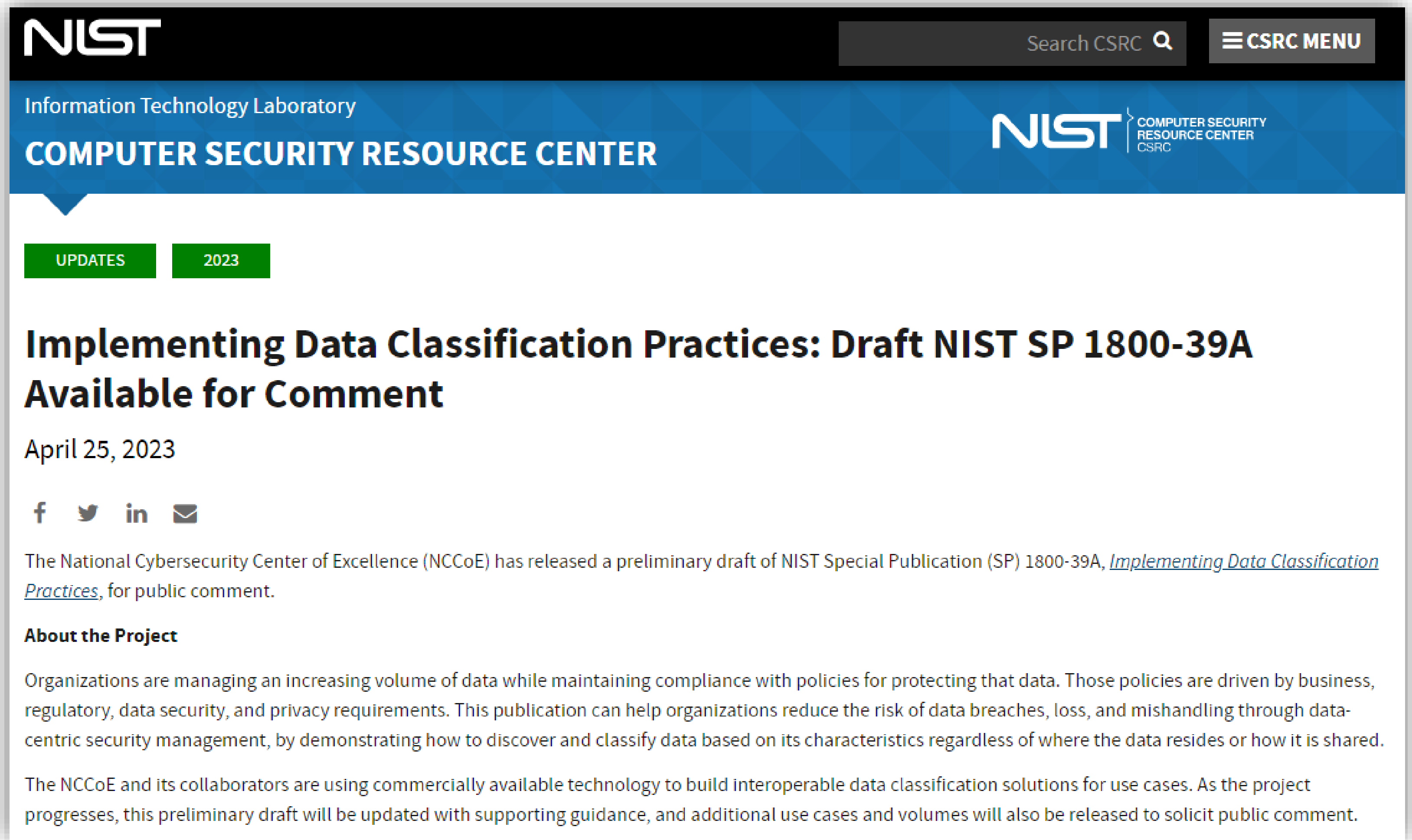
Abstract

This document provides essential guidance for members of governing bodies of organizations and management on the use of data classification as a means to support the organization's overall data governance policy and associated systems. It sets out important factors to be considered in developing and deploying a data classification system.

Read sample

Preview this standard in our Online Browsing Platform (OBP)

Coming Soon! Implementing Data Classification Practices (NIST SP 1800-39A). A project by NIST currently in process but a possible standard to be commonly use for data classification in the future.


NIST
Search CSRC
☰ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
UPDATES
2023

Implementing Data Classification Practices: Draft NIST SP 1800-39A Available for Comment

April 25, 2023

The National Cybersecurity Center of Excellence (NCCoE) has released a preliminary draft of NIST Special Publication (SP) 1800-39A, *Implementing Data Classification Practices*, for public comment.

About the Project

Organizations are managing an increasing volume of data while maintaining compliance with policies for protecting that data. Those policies are driven by business, regulatory, data security, and privacy requirements. This publication can help organizations reduce the risk of data breaches, loss, and mishandling through data-centric security management, by demonstrating how to discover and classify data based on its characteristics regardless of where the data resides or how it is shared.

The NCCoE and its collaborators are using commercially available technology to build interoperable data classification solutions for use cases. As the project progresses, this preliminary draft will be updated with supporting guidance, and additional use cases and volumes will also be released to solicit public comment.