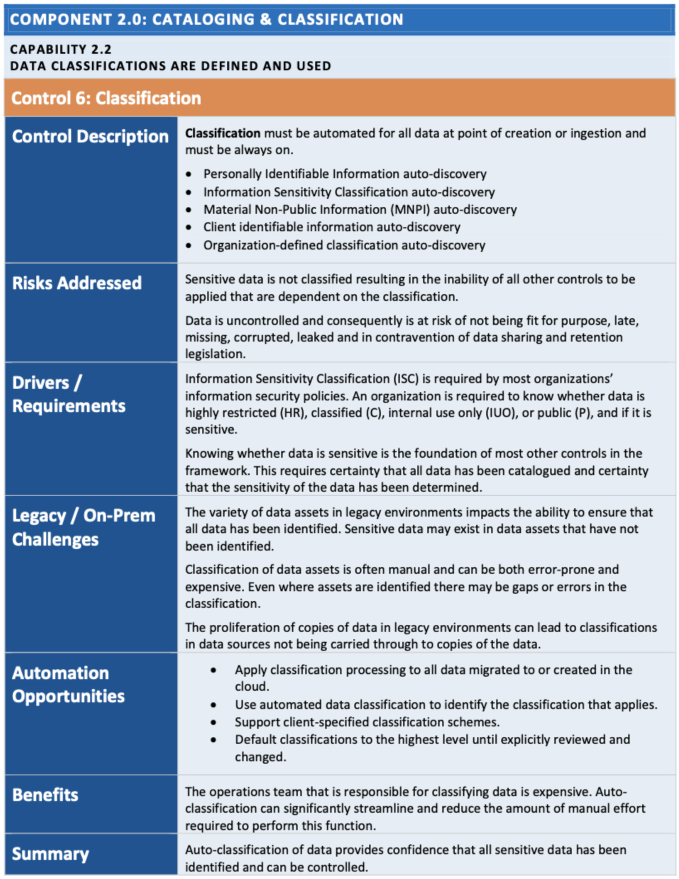
Capability 2.2

Body

Edit

A. CDMC Description



COMPONENT 2.0: CATALOGING & CLASSIFICATION	
CAPABILITY 2.2 DATA CLASSIFICATIONS ARE DEFINED AND USED	
Control 6: Classification	
Control Description	**Classification** must be automated for all data at point of creation or ingestion and must be always on. • Personally Identifiable Information auto-discovery • Information Sensitivity Classification auto-discovery • Material Non-Public Information (MNPI) auto-discovery • Client identifiable information auto-discovery • Organization-defined classification auto-discovery
Risks Addressed	Sensitive data is not classified resulting in the inability of all other controls to be applied that are dependent on the classification. Data is uncontrolled and consequently is at risk of not being fit for purpose, late, missing, corrupted, leaked and in contravention of data sharing and retention legislation.
Drivers / Requirements	Information Sensitivity Classification (ISC) is required by most organizations' information security policies. An organization is required to know whether data is highly restricted (HR), classified (C), internal use only (IUO), or public (P), and if it is sensitive. Knowing whether data is sensitive is the foundation of most other controls in the framework. This requires certainty that all data has been catalogued and certainty that the sensitivity of the data has been determined.
Legacy / On-Prem Challenges	The variety of data assets in legacy environments impacts the ability to ensure that all data has been identified. Sensitive data may exist in data assets that have not been identified. Classification of data assets is often manual and can be both error-prone and expensive. Even where assets are identified there may be gaps or errors in the classification. The proliferation of copies of data in legacy environments can lead to classifications in data sources not being carried through to copies of the data.
Automation Opportunities	• Apply classification processing to all data migrated to or created in the cloud. • Use automated data classification to identify the classification that applies. • Support client-specified classification schemes. • Default classifications to the highest level until explicitly reviewed and changed.
Benefits	The operations team that is responsible for classifying data is expensive. Auto-classification can significantly streamline and reduce the amount of manual effort required to perform this function.
Summary	Auto-classification of data provides confidence that all sensitive data has been identified and can be controlled.

B. Commentary

- Automated classification and discovery provides great lift and scalability for stewards who find it difficult to keep up with the pace of data source creation and change. It is, however

Properties

TEMPLATE

CDMC Controls Example Guide

LAST UPDATED

Sep 17 2021 at 12:06 pm

CREATED

Aug 3 2021 at 4:48 pm

Edited By

Jonathan Sander

John Wills

Domains

+

No Domains

Glossaries

+

Tags

+

No tags