Capability 4.1

Body

Edit

A. CDMC Description

COMPONENT 4.0: PROTECTION & PRIVACY	
CAPABILITY 4.1 DATA IS SECURED AND CONTROLS ARE EVIDENCED	
Control 9: Security Controls	
Control Description	1. Appropriate **Security Controls** must be enabled for sensitive data. 2. Security control evidence must be recorded in the data catalog for all sensitive data.
Risks Addressed	Data is not contained within the parameters determined by the legislative, regulatory or policy framework in which the enterprise operates. Data loss or breaches of privacy requirements resulting in reputational damage, regulatory fines and legal action.
Drivers / Requirements	The level of sensitivity of the data dictates what level of encryption, obfuscation and data loss prevention should be enforced. The requirements for **Security Controls** and Data Loss Prevention become increasingly more stringent as the sensitivity level of the data increases.
Legacy / On-Premises Challenges	It is difficult to ensure that encryption is always on for sensitive data.
Automation Opportunities	• Provide **security controls** capabilities including encryption, masking, obfuscation and tokenization that are turned on automatically based on the sensitivity of a data set. • Automate recording of the application of security controls.
Benefits	Evidence that the appropriate level of encryption is on and has been consistently applied is easy to produce. During a security audit, a data owner has a list of what their data is and how much of it is sensitive. For every piece of sensitive data, they can provide evidence that the data is encrypted and there is a data loss prevention regime in place for all the compute environments it resides in. Having security control evidence to deliver through the catalog rather than performing a forensic cyber review is a cost savings opportunity, since this work is typically handled by a full-time team of employees.
Summary	An automation that enforces and records the appropriate encryption level based on a data asset's sensitivity level ensures security compliance and reduces manual effort to provide evidence of the controls.

B. Commentary

- We believe 'always on' encryption is a minimum requirement for any cloud data storage platform. That means it should be intrinsic and automatically applied. There should be no effort required to turn it and no risk associated

Properties

TEMPLATE
CDMC Controls Example Guide

LAST UPDATED
Sep 17 2021 at 2:46 pm

CREATED
Aug 3 2021 at 4:49 pm

Edited By

Jonathan Sander
John Wills

Domains

No Domains

Glossaries

Tags

No tags