Security Control Traceability Matrix (SCTM)

Go up to Terms and Definitions

Discussion

A Security Control Traceability Matrix (SCTM) records traceable relationships between identified security controls and the system information used to demonstrate how those controls are selected, implemented, assessed, and supported by evidence.

An SCTM provides a structured view of security-control implementation and assessment information.

An SCTM can associate a security control with:

- A control identifier
- A control source or framework
- A control implementation description
- An implementing system element
- A responsible organization or role
- An assessment objective
- An assessment procedure
- An assessment result
- A compliance finding
- An identified risk
- A remediation activity
- An Evidence reference
- An Evidence Artifact
- A configuration or deployment record
- Provenance
- Traceability

The SCTM supports review of whether each identified security control has corresponding implementation and assessment information.

Within Crucible documentation, an SCTM can reference evidence generated by Crucible without requiring Crucible to own, approve, or authorize the security-control implementation.

Definition

matrix that records traceable relationships between security controls and the implementation, assessment, finding, remediation, and evidence information associated with those controls

Source

DIDO-controlled term adapted from:

- National Institute of Standards and Technology definition of Traceability Matrix
- Committee on National Security Systems Instruction 4009 definition of Security Requirements Traceability Matrix
- National Institute of Standards and Technology Special Publication 800-37 Revision 2

Note

The acronym **SCTM** means **Security Control Traceability Matrix**.

SCTM is a DIDO-controlled term. NIST and CNSSI sources commonly use the related term **Security Requirements Traceability Matrix (SRTM)**.

An SCTM focuses on security controls and their associated implementation, assessment, and evidence relationships. An SRTM can have a broader focus on security requirements derived from multiple sources.

An SCTM does not by itself establish that a control is implemented effectively. The matrix records traceable information that reviewers and assessors use when reaching that determination.

An SCTM can support Risk Management Framework (RMF) activities and an Authorization to Operate (ATO) decision.

Example

An SCTM associates a security control identifier with its implementation description, the deployed system elements that implement the control, the compliance findings produced during assessment, and references to Crucible-generated Evidence Artifacts.
