## **Set Theory Relationship Mapping (STRM)**



Reference Document: Secure Controls Framework (SCF) version 2024.4

Focal Document: Department of Homeland Security (DHS) Zero Trust Capability Framework (ZTCF)

Focal Document URL: TBD - No yet published

STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-4-dhs-ztcf.pdf

Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

- 1. Syntactic: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
- 2. Semantic: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
- 3. Functional: How similar are the <u>results</u> of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

- 1. Subset Of
- 2. Intersects With
- 3. Equal
- 4. Superset Of
- 5. No Relationship



## Relationship Type #1: Relationship Type #2: Relationship Type #3: Relationship Type #4: Relationship Type #5: SUBSET OF INTERSECTS WITH NO RELATIONSHIP **EQUAL** SUPERSET OF SCF control and Focal Focal Document Element is SCF control has some SCF control and Focal Focal Document Element is a a subset of SCF control. In other words, SCF control overlap with Focal Document Element are Document Element are the superset of SCF control. In unrelated; their content does Document Element, but same, although not other words. Focal Document contains everything that not overlap. each includes content that necessarily identical Focal Document Element the other does not. that SCF control does and does and more. INTERSECTS WITH SUBSET OF **EOUAL** SUPERSET OF NO RELATIONSHIP Relative Relationship Relative Relationship Relative Relationship Strength Relative Relationship Strength Relative Relationship Strength Strength (control versus Strength (control versus (control versus control) (control versus control) (control versus control) STRONG STRONG (10)(10)(10)NONE EQUAL MODERATE MODERATE MODERATE COVERAGE (NOT APPLICABLE) (10)

NOMINAL



NOMINAL

NOMINAL

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
DEV-03	DevSecOps	The ability of an organization to integrate security into emerging agile IT and DevOps development as seamlessly as possible.		Intersects With	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to:  (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar	8	
DEV-04	Software Supply Chain Protection	The ability of an organization to protect software in the CI/CD context ensuring that the software is not compromised through the various stages of build, test, package and deploy.		Intersects With	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to:  (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar	8	
			Functional	Intersects With	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	



Secure Controls Framework (SCF) 2 of 2