NIST Internal Report
NIST IR 8477

Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines

Developing Cybersecurity and Privacy Concept Mappings

Karen Scarfone
Murugiah Souppaya
Michael Fagan

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8477

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8477

Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines

Developing Cybersecurity and Privacy Concept Mappings

Karen Scarfone
Scarfone Cybersecurity

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

Michael Fagan
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8477

February 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies

NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-02-23

How to Cite this NIST Technical Series Publication
Scarfone KA, Souppaya MP, Fagan MJ (2024) Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines: Developing Cybersecurity and Privacy Concept Mappings. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8477. https://doi.org/10.6028/NIST.IR.8477

Author ORCID iDs
Karen Scarfone: 0000-0001-6334-9486
Murugiah Souppaya: 0000-0002-8055-8527
Michael Fagan: 0000-0002-1861-2609

Contact Information
mapping@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8477/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document describes the National Institute of Standards and Technology's (NIST's) approach to mapping the elements of documentary standards, regulations, frameworks, and guidelines to a particular NIST publication, such as Cybersecurity Framework (CSF) Subcategories or SP 800-53r5 controls. This approach is to be used to map relationships involving NIST cybersecurity and privacy publications that will be submitted via the NIST National Online Informative References (OLIR) process and hosted on NIST's online Cybersecurity and Privacy Reference Tool (CPRT). The approach provides flexibility to capture relationships for various levels of concepts and in different degrees of detail in human-consumable, machine-readable formats. The approach has been informed by concept system and terminology standards, as well as experience with what information the security and privacy community would find most valuable.

Keywords

concept mapping; crosswalk; cybersecurity; mapping; privacy; relationship; terminology science.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Audience

The primary audience is subject-matter experts (SMEs) for a documentary standard, regulation, framework, guideline, or other content who want to map between concepts in their content and concepts in NIST publications. SMEs may own the content being mapped to NIST publications. This document may also be of interest to SMEs who choose to follow this same approach for interoperability and compatibility reasons when mapping between two non-NIST publications. A secondary audience for this document includes the users who will leverage the mappings to support various use cases.

Acknowledgments

The authors thank everyone who contributed to this publication by applying the approach to their mapping scenarios and providing feedback on the approach.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

Following the ITL call for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, notice of one or more such claims has been received.

By publication, no position is taken by ITL with respect to the validity or scope of any patent claim or of any rights in connection therewith. The known patent holder(s) has (have), however, provided to NIST a letter of assurance stating either (1) a general disclaimer to the effect that it does (they do) not hold and does (do) not currently intend holding any essential patent claim(s), or (2) that it (they) will negotiate royalty-free or royalty-bearing licenses with other parties on a demonstrably nondiscriminatory basis with reasonable terms and conditions.

Details may be obtained from mapping@nist.gov.

No representation is made or implied that this is the only license that may be required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Executive Summary

Understanding how the elements of diverse cybersecurity and privacy standards, regulations, frameworks, guidelines, and other content are related to each other is an ongoing challenge for people in nearly every organization. It can be time-consuming and difficult to answer questions like:

- How does conforming to one standard help the organization conform to another standard? What parts of the second standard does the first standard fail to address?
- Where can we find more information on how to satisfy a particular requirement in a guideline? What types of technologies can we use, and what types of skills do the implementers need to have?
- If we want to conform to a particular standard, what types of cybersecurity capabilities do our technology product and service providers need to support?
- If we perform a particular security assessment methodology, what requirements will be sufficiently validated across our compliance portfolio?
- What recommendations substantially changed from a guideline's previous version to its current version?
- What security and privacy controls must be in place before we adopt a new technology?

This document explains NIST's approach for identifying and documenting the relationships between concepts in cybersecurity and privacy, such as how the concepts of a NIST or third-party standard or guideline relate to the concepts of a foundational NIST publication like the Cybersecurity Framework (CSF) or NIST Special Publication (SP) 800-53. There are many possible *concept types*, including controls, requirements, recommendations, outcomes, technologies, functions, processes, techniques, roles, and skills. NIST's approach is to be used by both NIST and third parties for mapping all relationships involving NIST cybersecurity and privacy publications that will be submitted to NIST's National Online Informative References (OLIR) Program and hosted in NIST's online Cybersecurity and Privacy Reference Tool (CPRT).

By following this approach, NIST and others in the cybersecurity and privacy standards community can jointly establish a single *concept system* over time that links cybersecurity and privacy concepts from many sources into a cohesive, consistent set of relationship mappings. The mappings can then be used by different audiences to better describe the interrelated aspects of the global cybersecurity and privacy corpus.

1. Introduction

A *concept* is a "unit of knowledge created by a unique combination of characteristics" [ISO1087]. In cybersecurity and privacy, there are many *concept types*, including controls, requirements, recommendations, outcomes, technologies, functions, processes, techniques, roles, and skills. The term *mapping* indicates that one concept is related to another concept.

Many existing mappings do not characterize their relationships. In other words, they do not indicate how the two concepts are related. For example, a mapping can say that a cybersecurity standard's Identity Governance control is related to NIST SP 800-53's control AC-2, Account Management. However, this mapping does not indicate whether the two controls are equivalent, whether one helps achieve the other, whether one is a prerequisite for or a component of the other, or whether they overlap.

Mapping is often conducted as an abstract exercise (e.g., "map A to B") without explicitly determining, documenting, or communicating the mapping's purpose, use cases, scope, audience, or other assumptions. As a result, people who use the mapping must guess at its meaning and context. These kinds of mappings save people a little time by pointing them to potentially relevant information. Users of these mappings still need to read and comprehend the concepts in both documents within the documents' respective contexts to understand the nature of the relationship.

This highlights another issue: the lack of consistency and transparency in the assumptions and mapping approaches followed by the subject-matter experts (SMEs) who create the mappings. Mappings are less valuable and harder to use and maintain without clearly indicating why two concepts were mapped and what that mapping signifies. There is also the chance SMEs will utilize their own perspectives and concepts while mapping without documenting them, and the perspectives and understanding of the concepts may be significantly different for future users of the mapping. This is especially true in emerging disciplines like cybersecurity and privacy, where concepts and concept types are abundant, change over time, and are not always well-documented. Additionally, terms like "mapping" and "crosswalk" are widely used but not consistently defined. Without consistent terminology and definitions, information sharing is difficult and can be prone to miscommunications and loss of nuance.

1.1. Purpose and Scope

This document explains the basics of cybersecurity and privacy concept mapping, including defining foundational terminology. It also presents the technical elements of NIST's approach for creating human-consumable mappings that involve NIST cybersecurity and privacy publications. NIST's approach is to be used by both NIST and third parties for mapping all relationships involving NIST cybersecurity and privacy publications that will be submitted to NIST's National Online Informative References (OLIR) Program and hosted in NIST's online Cybersecurity and Privacy Reference Tool (CPRT). The elements of NIST's approach are meant to supplement — not replace — organizations' existing mapping methodologies.

Examples throughout this document come from other NIST publications. This is not intended to imply that only NIST publications can be sources of concepts for mappings. The mapping approach should work for any type of information, particularly cybersecurity or privacy content, regardless of source.

Mapping for prose concepts (i.e., ideas in the form of ordinary written language), such as requirements in documentary standards, is fundamentally different than mapping for specific technology elements, such as individual software configuration settings that can be unambiguously documented and implemented by machines. Mapping prose concepts necessitates human interpretation and understanding of the concepts and their sources, as does using the resulting mappings. The scope of this document is the creation of human-consumable mappings for prose concepts. Lower-level concepts that can be expressed without prose are out of scope.

Details about how to organize, format, and submit mapping data for potential inclusion in NIST repositories and NIST's processes for reviewing and posting submitted mappings are out of scope for this document. See Section 1.2 for more information.

1.2. Related Work

The CPRT offers a consistent data format for browsing and downloading digitized reference data for various NIST cybersecurity and privacy standards, guidelines, and frameworks. These datasets make it easier for users to identify, locate, and customize content in and across NIST resources without needing to review hundreds of pages of narrative within the publications. The reference data are exportable in different data formats, including Excel and JavaScript Object Notation (JSON) (machine-readable). As the tool evolves, users will be able to draw upon multiple NIST resources to answer specific cybersecurity and privacy questions and build their own guidance.

NIST encourages SMEs for third-party standards, guidance, and other cybersecurity and privacy content to submit mappings to NIST publications to the National OLIR Program [IR8278A]. Such mappings must comply with requirements available through the OLIR Program website. NIST will make mappings available through the CPRT interface in human-consumable, machine-readable formats. Future OLIR and CPRT updates will enable convenient, rapid updates to mappings by their creators.

1.3. Publication Structure

The rest of this publication contains the following sections and appendices:

- Section 2 provides an overview of the approach for concept mapping.
- Section 3 discusses the need to identify and document use cases for each mapping.
- Section 4 describes several concept relationship styles for mapping and suggests suitable situations for each style.
- Section 5 offers tips for evaluating concept pairs and documenting relationships.
- The References section lists the references cited throughout this publication.

- Appendix A provides a glossary of selected terms used in this publication.

2. Concept Mapping Approach Overview

The approach to cybersecurity and privacy concept mapping draws from the field of terminology science. As described in International Organization for Standardization (ISO) 1087:2019, *Terminology work and terminology science – Vocabulary*, terminology science is "concerned with the systematic collection, description, processing and presentation of concepts and their designations" [ISO1087]. Terminology science is typically used to identify concepts within a particular domain, such as cybersecurity or privacy, and to define those concepts and their relationships to each other within a single, cohesive concept system. ISO 1087 defines a *concept system* as a "set of concepts structured in one or more related domains according to the concept relations among its concepts" [ISO1087]. As ISO 704:2022, *Terminology work – Principles and methods* states, "Concepts do not exist as isolated units of knowledge but always in relation to each other" [ISO704].

In the case of cybersecurity and privacy mapping, the concepts are already defined in *concept sources*, including documentary standards, regulations, frameworks, and guidelines. In some cases, concepts may be directly known (i.e., terminology), but they are more often reflected in the requirements, recommendations, outcomes, controls, technologies, and architectures in standards, guidance, and other sources. These concept definitions are analogous to the definitions in the ISO 1087 and ISO 704 standards. The task in mapping is to define the relationships between existing concepts that are defined in different sources with the goal of illuminating the concept systems in them and the relationships that exist between them. Using a consistent approach and terminology for creating mappings could establish a single concept system for cybersecurity and privacy concepts from many sources.

This approach has adapted numerous concept relationship types from ISO 704 and reiterates that standard's assertion that concept definitions should be supplemented by gathering context, examples, and other related information. This effort will improve understanding of each concept and involve the *concept source owners* in developing, reviewing, maintaining, and supporting respective mappings when feasible. In concept systems, the definition of a concept is not all-encompassing. It provides enough information to distinguish the concept from others but does not include every detail regarding the concept [ISO704].

NIST proposes that SMEs add these steps to their existing processes for creating mappings that involve NIST content:

- Identify and document use cases for the mapping (Section 3).
- Choose a concept relationship style (Section 4).
- Evaluate concept pairs and document their relationships (Section 5).

Each of these will be discussed in more detail. Note that these steps do not encompass a complete mapping development life cycle, as described in NIST IR 8278Ar1 [IR8278A]. The steps enhance rather than replace what SMEs have already been doing.

3. Identify and Document Use Cases for the Mapping

Most mappings involve two sources, such as a NIST publication and a third-party publication. In the NIST OLIR and CPRT contexts, the NIST publication is called the *focal document*, and the second publication is called the *reference document*. Some mappings involve only one version of one source; in other words, they map concepts within the source to other concepts within the same source (i.e., the focal document and the reference document are the same). NIST anticipates creating and publishing these *one-source mappings* for appropriate publications.

After choosing the sources you want to map, document your assumptions in one or more use cases *before* mapping. Each use case provides context for the mapping and improves its usability and transparency. Five assumptions that are typically important to document are:

1. **The intended users of the mapping.** Include the skills and knowledge that the mapping users are expected to have. A mapping can be consumed by tools and technologies as well.
2. **Why someone would want to use this mapping.** This gets to the core of why you want to create the mapping. For example, you may want to help people understand how complying with standard A can help them to comply with standard B or point people from the skills defined in standard A to the corresponding items in standard B for which those skills are necessary.
3. **The types of concepts to be mapped.** As mentioned in Section 1, there are many types of cybersecurity and privacy concepts. Each source often has multiple types of concepts (e.g., outcomes, implementations, requirements/recommendations, principles, technologies, techniques/methodologies, roles). There are some factors to consider and document when selecting concept types:
    - **Relevance:** Generally, you want to select the concept type from each source that is most relevant to the use case. Combining multiple concept types from each source into a single mapping may be more confusing than defining multiple use cases and having a separate mapping for each one.
    - **Level of granularity:** Many sources have concepts defined at multiple levels of granularity. For example, NIST SP 800-53r5 (Revision 5) [SP800-53] defines 20 control families. Each of those families contains multiple controls, and some controls also contain control enhancements. Mapping a technology’s cybersecurity functions to the 20 control families would be faster and easier than mapping them to the individual controls or control enhancements but generally would not be as valuable to mapping users. However, mapping at the lowest level is not always practical. For example, if a document defines 10 high-level concepts, 100 mid-level concepts, and 1000 low-level concepts, mapping for all 1000 low-level concepts may take far more time than is practical. It may also provide a level of detail that your intended mapping users neither need nor want. Just because you can map at the lowest level does not mean you should.

  - **Conceptual relationship between sources:** Sources and the concept types they contain may have different target audiences or speak to different conceptual layers within the concept system. For example, workforce skills from the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NICE Framework) or device capabilities from the NIST Internet of Things (IoT) Device Cybersecurity Baselines may be related to organizational activities documented in other sources, such as industry guidance that recommends cybersecurity controls for systems. In this case, the cybersecurity controls are a concept type that would be defined for one conceptual layer (e.g., information technology [IT]/system cybersecurity), while the workforce skills or device capabilities would be concept types from related but distinct conceptual layers (i.e., cybersecurity education and workforce development and system component cybersecurity development, respectively). Therefore, it is important to establish and document assumptions about how the two sources are conceptually related overall before attempting to define more specific relationships.

4. **The direction of the mapping.** A mapping could indicate how a concept in source A maps to a concept in source B, vice versa, or both. As Section 4 discusses, many mappings either have an obvious direction or are inherently directionless, so explicitly indicating the direction of mapping is often not necessary.
5. **How exhaustive the mapping will be.** An exhaustive mapping will not be necessary in most cases, such as mapping between concept systems in different domains (e.g., NICE Framework roles to Secure Software Development Framework [SSDF] categories) or at different levels of abstraction (e.g., CSF to SP 800-53 controls). Mapping indirect or tenuous relationships would create so many mappings that they would lose their value. Instead, we recommend capturing the strongest direct relationships between concepts. This helps keep the mapping clear and in line with the stated use case, targets the needs of the audience, and helps them prioritize their work.

You could document a use case by writing a brief sentence that combines these assumptions. For example:

- Chief Information Security Officers (CISOs), risk officers, and assessors need to determine how meeting the requirements of standard A will help satisfy the recommendations of standard B.
- Technology project managers need to know which types of technologies and human knowledge, skills, or abilities defined in guidance A are most helpful for performing tasks in document B.
- Cloud administrators need additional information on how to implement the processes in guidance A within cloud environment B.
- The organization’s cybersecurity professionals who evaluate the capabilities of technology products and services need to know which device capabilities defined in

guidance A support the organization's implementation of cybersecurity capabilities specified in guidance B.

- Users of standard A need to know which of its clauses have substantially changed from one version to a subsequent version.

You could also document your assumptions for each use case as four columns in a spreadsheet or table or through a markup language (e.g., JSON, Extensible Markup Language [XML]). **Table 1** illustrates an example of this.

Table 1. Notional documentation of assumptions

Target Audience	Source A Concepts	Source B Concepts	Reason and Exhaustiveness
CISOs	Requirements of standard A	Recommendations of standard B	Which source A concepts are most helpful for satisfying source B concepts

4. Choose a Concept Relationship Style

Once the use case is documented, choose a *relationship style*, which is an explicitly defined convention for characterizing relationships for a use case. Think about which concept relationship style is appropriate for your mapping, and consider your documented assumptions. A predefined style increases interoperability among mappings and allows a broader group of users to efficiently and effectively use them to meet a more expansive set of needs. If predefined styles do not adequately describe the relationships you intend to capture in your mapping, create a style that better characterizes the relationships between the two sets of concepts.

This section describes NIST's definitions for relationship styles and offers suggestions for which style is typically best for various situations. The styles described in this section are listed in **Table 2** along with a notional example of each style. The styles are generally listed in order from the most subjective to the most objective. As of this writing, NIST accepts OLIR submissions and provides OLIR templates for three styles: concept crosswalk, supportive relationship mapping, and set theory relationship mapping.

Table 2. Concept relationship styles

Concept Relationship Style	Typical Situations	Notional Example
Concept crosswalk (Section 4.1)	• Pointing to additional information on a topic • Documenting diverse concept types at a consistent level • Having few resources available to do the mapping	CSF 2.0 subcategory ID.RA-01 SP 800-53r5 control CA-2
Supportive relationship mapping (Section 4.2)	• Characterizing relationships between similar concept types • Characterizing relationships between different but strongly related concept types	Zero trust architecture (ZTA) project capability Certificate Authority ***Relationship type: Supports*** ***Relationship property: Example of*** CSF 2.0 subcategory PR.AA-01
Set theory relationship mapping (Section 4.3)	• Indicating commonality between two similar sets of concepts, like two versions of the same standard	CSF 2.0 subcategory PR.IR-03 ***Rationale: Semantic*** ***Relationship type: Equal*** Privacy Framework 1.0 subcategory PR.PT-P4
Structural relationship mapping (Section 4.4)	• Indicating the inherent hierarchical structure of concepts within a single source or duplicated in two sources	CSF 2.0 category DE.AE ***Relationship type: Parent-child*** CSF 2.0 subcategory DE.AE-07

Section 4.5 discusses when a custom style might be appropriate as an alternative to one of these predefined styles. Section 4.6 discusses the use of mappings with different relationship styles.

Multiple concept relationship styles can be used to document relationships between two concept sources or even when documenting relationships within one source. For example, consider the NIST CSF. NIST could use parent-child (i.e., structural) relationships to define the structure of the CSF and use supportive relationships to indicate when achieving one CSF Subcategory helps support achieving other Subcategories. You could then create concept crosswalks between the CSF's Subcategories and other sources, effectively pointing people to additional sources of information on each Subcategory. These three types of mappings can all be combined into one concept system, which provides a richer and more useful explanation of how the concepts are related than any of the mappings could provide on its own.

4.1. Concept Crosswalk

Definition: A *concept crosswalk* indicates that a relationship exists between two concepts without any additional characterization of that relationship. In other words, a relationship statement in a concept crosswalk only indicates that concept A and concept B are related and captures no additional information about the relationship between the two concepts. Therefore, it's particularly important to document the use case for a concept crosswalk because the use case is the only source of contextual information about the intention and meaning of each relationship.

Primary Uses: Crosswalks are generally well-suited to the following situations:

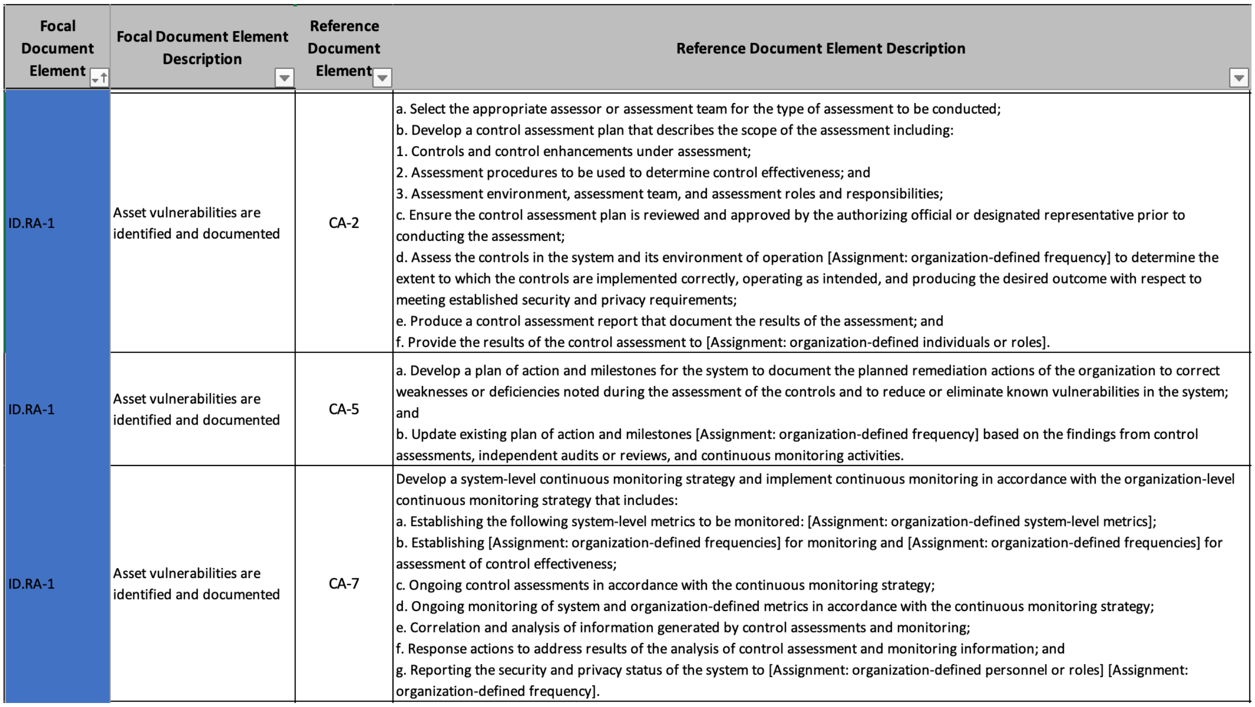
- Pointing to additional information on a topic (e.g., for more information on how to implement concept A, see clause 10 in source B), which has historically been called an *informative reference*
- Documenting a set of mappings at a consistent level even though several types of concepts are being mapped and the relative strength of their relationships varies significantly
- Mapping two sources with different and weakly related concept types

Mappers may also choose to create a crosswalk for exploratory or preparatory purposes as the initial draft of a mapping that will eventually follow a more detailed relationship style. This may be helpful, for example, if a working group wants to first reach consensus on which relationships to characterize before making that characterization.

Examples:

- SP 800-53r5 cross-references [SP800-53]
- Cybersecurity Framework (CSF) 1.1 [CSF11] and 2.0 [CSF20] informative references
- SSDF informative references [SP800-218]
- Various crosswalks in the repository for the NIST OLIR Program

Figure 1 shows a screenshot from an SP 800-53r5 to CSF crosswalk with the CSF as the focal document and SP 800-53r5 as the reference document.



Focal Document Element	Focal Document Element Description	Reference Document Element	Reference Document Element Description
ID.RA-1	Asset vulnerabilities are identified and documented	CA-2	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
ID.RA-1	Asset vulnerabilities are identified and documented	CA-5	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
ID.RA-1	Asset vulnerabilities are identified and documented	CA-7	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Fig. 1. Concept crosswalk example between SP 800-53r5 and the NIST CSF

4.2. Supportive Relationship Mapping

Definition: *Supportive relationship mapping* indicates how a *supporting concept* can or does help achieve a *supported concept*. The supportive relationship mapping style supports the use of the following *relationship types*:

- *Supports*: Concept A supports concept B when A can be applied alone or in combination with one or more other concepts to achieve B in whole or in part.
- *Is supported by*: Concept A is supported by concept B when B can be applied alone or in combination with one or more other concepts to achieve A in whole or in part.
- *Identical:* Concept A and concept B are identical. They use exactly the same wording.
- *Equivalent:* Concept A and concept B are equivalent. They have the same meaning but different wording.
- *Contrary:* Concept A and concept B each have one or more elements that contradict one or more elements of the other concept. The contradictions may be opposites but do not have to be. This is based on the contrary concept type in Section 6.5.4 of [ISO704].
- *No relationship:* Concept A and concept B are not related or are not sufficiently related to merit another supportive relationship type.

The *supports* and *is supported by* relationships are more than simply cause and effect. They can also indicate whether or not the supporting concept is necessary for achieving the supported concept. One of the following *relationship properties* can optionally be assigned to each *supports* and *is supported by* relationship:

- *Example of:* The supporting concept C is one way (an example) of achieving the supported concept D in whole or in part. However, the supported concept D could also be achieved without applying the supporting concept C. In other words, one can accomplish D without C. This is based on the generic relationship type in Section 5.5.4.2 of [ISO704].
- *Integral to:* The supporting concept C is integral to and a component of the supported concept. The supporting concept must be applied as part of achieving the supported concept. In other words, one cannot accomplish D without C. This is based on the partitive relationship type in Section 5.5.4.3 of [ISO704].
- *Precedes:* The supporting concept C precedes the supported concept D when concept C must be achieved before applying the supported concept D. In other words, concept C is a prerequisite for concept D. The supporting concept itself is not part of the supported concept. This is based on the sequential relation type in Section 5.5.5 of [ISO704].

There are no supportive relationship properties for *identical*, *equivalent*, and *contrary* relationships.

The supportive relationship types and properties indicate the relative relationships between pairs of concepts within the context of a specified use case. The relationship types and properties are unlikely to have exactly the same meaning in different mappings because each use case will be different and the resulting mapping will be unique, taking into account mappers' assumptions and viewpoints. While relationship types and properties have the same basic meaning across mappings, be careful not to assume that the way concept A supports concept B is the same as the way concept B supports concept C. Always refer to the use case documentation described in Section 3 to understand the context and assumptions for each mapping.

Primary Uses: The supportive relationship mapping style is generally well-suited to the following situations:

- The sources have similar concept types. Examples include the following:
  - A controls community mapping security controls in their control catalog to controls in the SP 800-53r5 catalog
  - NIST authors mapping a set of procedures for assessing of security and privacy controls employed within systems and organizations to an assessment methodology performed within an effective risk management framework, with both the procedures and methodology defined in SP 800-53A

- The sources have different but strongly related concept types. Examples include the following:
    - A standards developer mapping cybersecurity requirements in one of their standards to NIST CSF subcategories (outcomes)
    - An industry working group mapping implementation recommendations in their DevSecOps guidelines to implementation examples from the NIST SSDF
    - A community mapping the capabilities of security principles and architectures, like zero trust, to the technology functional components provided by a NIST National Cybersecurity Center of Excellence (NCCoE) project build
    - A software vendor mapping recommended configuration settings for their software to technology function components in an NCCoE project build
    - A guidance developer mapping elements from their guidance to the NICE Framework Competency Areas that support them
    - A cryptographic module software developer mapping evidence from test results for their module to corresponding requirements in Federal Information Processing Standard (FIPS) 140-3

Examples:

- NIST SP 1800-36 Volume E, Section 4.1, Table 4-1 contains a mapping between functions from the NIST NCCoE's Trusted IoT Device Onboarding project reference design and NIST CSF 1.1 subcategories to show how the reference design's functions help support the CSF subcategories and vice versa. **Table 3** shows an excerpt from that mapping.

Table 3. Supportive relationship mapping examples from SP 1800-36 Vol. E

Logical Component	Component's Function	Function's Relationships to CSF 1.1 Subcategories (and Relationship Properties)	Relationship Explanation
Certificate Authority (CA)	Issues and signs certificates as needed.	Supports (example of) PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	The fact that a credential is signed by a trusted CA provides a mechanism that may be used for enabling the credential to be verified and revoked.
		Supports (integral to) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	If the device credential is an X.509 certificate (e.g., an IDevID) that is signed by a CA, this certificate binds the device's credential to the device's identity.
Application-Layer Onboarding Service	After the device connects to the network, this component interacts with the device using…	Is Supported by (precedes) ID.AM-2: Software platforms and applications within the organization are inventoried	In some application-layer onboarding mechanisms, the IoT device must be prepared for application-layer onboarding during the factory provisioning process. In these cases, the…

- NIST SP 1800-35 Volume E, Section 4.2.1, Table 4-9 contains a mapping between zero trust architecture functions from the NIST NCCoE's ZTA project reference design and SP 800-53 controls. Because hundreds of NIST SP 800-53 controls can help support ZTA functions, mapping was only performed on existing SP 800-53 controls. **Table 4** shows an excerpt from that table.

Table 4. Supportive relationship mapping examples from SP 1800-35 Vol. E

ZTA Project Component	ZTA Project Function	Function's Relationships to SP 800-53 Controls (and Relationship Properties)	Relationship Explanation
ICAM - Identity Governance	Provides policy-based, centralized, automated processes to manage user identity and access control functions (e.g., ensuring segregation of duties, role management, logging, auditing, access reviews, analytics, and reporting) to ensure compliance with requirements and regulations.	Supports (integral to) AC-2: Account Management	The Identity Governance function includes account management such as authorized users of the system, access authorizations (i.e., privileges), and assignment of organization-defined attributes.
		Supports (integral to) AC-3: Access Enforcement	The Identity Governance function enforces approved authorizations for logical access to information and system resources by identified users in accordance with applicable access control policies.
		Supports (precedes) AC-4: Information Flow Enforcement	The Identity Governance function is a necessary component of the identity component of access authorizations on which information flow enforcement depends.
		Supports (integral to) AC-5: Separation of Duties	The Identity Governance component can manage access permissions and authorizations in a way that incorporates the separation of duties principle.

4.3. Set Theory Relationship Mapping

Definition: *Set theory relationship mapping* is a relationship style derived from the branch of mathematics known as set theory. Each mapping done with this style includes both a rationale for the mapping and a relationship type.

Set theory relationship mapping supports three 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 **results** of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

The set theory relationship mapping style supports five *relationship types* for documenting the logical similarity of two concepts:

1. *Subset of:* Concept A is a subset of concept B. In other words, concept B contains everything that concept A does and more.
2. *Intersects with:* Concept A and concept B have some overlap, but each includes content that the other does not.
3. *Equal:* Concept A and concept B are the same, although not necessarily identical.
4. *Superset of:* Concept A is a superset of concept B. In other words, concept A contains everything that concept B does and more.
5. *No relationship:* Concept A and concept B are unrelated; their content does not overlap.

The relationship type and the rationale must be used together. For example, consider CSF 1.1's PR.AC-1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes" [CSF11] and the Privacy Framework's PR.AC-P1, "Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices." These two concepts have identical wording except for "users" versus "individuals" and the order of the last few words. With a rationale of *syntactic*, the relationship type would be *intersects with* because the two overlap, but each includes content that the other does not. However, with a rationale of *semantic*, the relationship type would be *equal* if "users" and "individuals" have the same meaning in their respective sources, *subset* if "users" was a subset of "individuals," and so on.

More than one rationale may apply to a pair of concepts. The SME who performs the mapping also chooses the rationale that they deem most useful. The expert can also do multiple mappings for the concept pair, each using a different rationale.

The set theory relationship mapping style has been supported by NIST OLIR since its launch, and it is also leveraged by the NIST Open Security Controls Assessment Language (OSCAL) to support automated cybersecurity control assessment.

Primary Uses: The set theory relationship mapping style is generally well-suited to the following situations:

- Indicating how much commonality two similar sets of concepts have, such as how requirements in a new version of a standard compare to their counterparts in a previous version or how requirements in one standard compare to a second standard based on the first one
- Mapping two sets of concepts when the pairs of concepts are mostly the same as each other or supersets or subsets of each other (when there are relatively few relationships of type *intersects with*)

Examples: Examples of set theory relationship mapping are available from the OLIR repository.

- NIST has mapped the Functions, Categories, and Subcategories of the NIST Cybersecurity Framework version 1.1 (focal document) to the Functions, Categories, and Subcategories of its Privacy Framework version 1.0 (reference document). The Privacy Framework is based on the Cybersecurity Framework, so the set theory relationship mapping indicates where the two frameworks have identical concepts, as well as how their corresponding concepts differ at a high level. **Table 5** shows an example from the full mapping.

Table 5. Set theory relationship mapping example from OLIR repository

CSF 1.1 Element	CSF 1.1 Element Description	Rationale	Relationship	Privacy Framework Element	Privacy Framework Element Description
PR	Develop and implement appropriate safeguards to ensure delivery of critical services.	Syntactic	Intersects with	PR-P	Develop and implement appropriate data processing safeguards.
PR.AC	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Functional	Intersects with	PR.AC-P	Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Semantic	Equal to	PR.AC-P1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.
PR.AC-2	Physical access to assets is managed and protected	Functional	Superset of	PR.AC-P2	Physical access to data and devices is managed.

4.4. Structural Relationship Mapping

Definition: The *structural relationship mapping* style captures an inherent hierarchical structure of concepts, usually defined within a single source. For example, the CSF defines several Functions. Each Function is composed of Categories, and each Category is composed of Subcategories. This structure is a hierarchy of a *parent-child* relationship and, thus, a form of mapping. Structural relationships are not as informative as the ones used in the supportive, extended, or set theory styles. A parent-child relationship implies that the child concept is part of the parent concept, but it does not specify whether the child concept is required or optional in order to achieve the parent concept.

Structural relationships are fully objective because they are only based on a source's intrinsic structure. Even though subjectivity was likely involved in the structure's creation, the scope of the mapping is the final structure, and that is objective. However, structural relationships provide no insights as to how concepts relate to each other independent of the structure. A second mapping using a different concept relationship style can supplement a structural relationship mapping.

Structural relationships may already be defined in data models and other forms.

Primary Uses: The structural relationship mapping style is generally well-suited to the following situations:

- Indicating the parent-child structure of the elements of a framework, standard, regulation, or other content defined in a formal hierarchy (within one or more sources)

Examples: The NIST CPRT makes the structure of CSF 1.1 and 2.0, SSDF 1.1, SP 800-53r5, and other NIST frameworks and baselines available in downloadable Excel and JSON formats. The parent-child relationships are implied but not explicitly stated as of this writing. **Table 6** contains a notional example from SSDF 1.1 of how a set of parent-child relationships can capture the structure of a standard, framework, or other hierarchical content. Each row in the table has the relationship *parent-child*.

Table 6. Notional example of parent-child relationships

Concept A (Parent)	Concept B (Child)
Prepare the Organization (**PO**): Organizations should ensure that their people, processes, and technology are prepared to perform…	Define Security Requirements for Software Development (**PO.1**): Ensure that security requirements for software development are known…
Define Security Requirements for Software Development (**PO.1**): Ensure that security requirements for software development are known…	**PO.1.1**: Identify and document all security requirements for the organization's software development infrastructures and processes…
Define Security Requirements for Software Development (**PO.1**): Ensure that security requirements for software development are known…	**PO.1.2**: Identify and document all security requirements for organization-developed software to meet…
Define Security Requirements for Software Development (**PO.1**): Ensure that security requirements for software development are known…	**PO.1.3**: Communicate requirements to all third parties who will provide commercial software components to the organization…
Prepare the Organization (**PO**): Organizations should ensure that their people, processes, and technology are prepared to perform…	Implement Roles and Responsibilities (**PO.2**): Ensure that everyone inside and outside of the organization involved in the SDLC is prepared…
Implement Roles and Responsibilities (**PO.2**): Ensure that everyone inside and outside of the organization involved in the SDLC is prepared…	**PO.2.1**: Create new roles and alter responsibilities for existing roles as needed to encompass all parts of the SDLC. Periodically review and maintain the defined roles and responsibilities, updating them as needed.

4.5. Custom

This approach does not attempt to capture every conceivable style or type of relationship. For example, the approach does not provide a way for someone studying the cybersecurity risks of a particular technology (e.g., mobile, semiconductors) to map the components of that technology to NIST-catalogued threats and countermeasures.

Using more relationship styles and types can make it difficult or impossible to link concepts together in a consistent way in a single concept system. Additional relationship types can also make it more challenging and time-consuming for SMEs because distinctions between relationship styles and types may be subtle, so selecting the appropriate one will require more thought and evaluation.

NIST welcomes suggestions for relationship types and properties to add to existing styles. NIST also recognizes that there may be cases in which none of the existing styles are suitable and a new custom style is needed. NIST encourages SMEs considering the development of a custom style to first contact NIST to discuss the situation, learn what other style changes or additions may be in progress, and determine a recommended course of action.

In the future, NIST will release details of how a SME would document a custom style so that mapping users will understand it and be able to convert it to other styles if appropriate.

4.6. Using Mappings with Different Relationship Styles

Different relationship styles are best suited for particular situations. Rather than trying to force the use of one relationship style for all mappings, this approach enables the use of multiple relationship styles while also ensuring a level of interoperability for all mappings that use any of those styles. This enables mapping users to choose to either have all mappings within a single concept system downgraded to the lowest common denominator in terms of relationship styles or have a concept system using multiple relationship styles.

Interoperability is also important because the SMEs who perform mappings may decide that they want to switch relationship styles because of time constraints involving the style they originally chose. For example, concept crosswalks are the most basic relationship style because they provide the least information. Mappings in all other relationship styles can be trivially downgraded to concept crosswalks by omitting all their relationship types and properties, leaving just concept pairs.

Most set theory relationships can be automatically converted to their supportive relationship counterparts, as depicted in **Table 7**. This might be of interest to SMEs who want to convert existing set theory relationship mappings to the new supportive relationship mappings. However, set theory *intersects with* relationships cannot be automatically converted because they only indicate overlap between the concepts, not the nature of that overlap. An *intersects with* relationship can either be automatically converted to a concept crosswalk or manually reevaluated by an SME in order to remap it as a supportive relationship.

Table 7. Converting set theory relationships to supportive relationships

Set Theory Relationship	Supportive Relationship
subset of	supports (integral to)
equal	equivalent
superset of	is supported by (integral to)

Set Theory Relationship	Supportive Relationship
intersects with	N/A

When converting mappings in a way that attempts to preserve relationship meaning (e.g., using the conversions stated in Table 7), it is important to consider the assumptions and other context captured related to the mapping being converted. The context in which a mapping was performed may impact exactly how relationships should be interpreted, which can in turn impact how one relationship should be converted to another.

5. Evaluate Concept Pairs and Document Their Relationships

After documenting the use cases for the mapping and choosing the relationship style, the identification of relationships that constitute the mapping can commence. It is recommended that a SME start a new mapping by documenting a representative sample of the mapping in an ad hoc format of their choice, like a spreadsheet or document. There are two major objectives for this sample: 1) identify issues with the use cases or relationship style choice that may necessitate changes, and 2) have other SMEs review the sample and the use case documentation, and provide feedback on them to help improve the quality of the mapping. Having a sample reviewed is a recommended practice because it helps reduce the impact of individual bias and the likelihood of inconsistent mapping.

When mapping, the SME should document the rationale for each relationship. This provides valuable context and justification that other SMEs can use to evaluate the mappings and that mapping users can utilize to better understand each mapping.

Here are a few mapping tips for SMEs based on feedback from users of the NIST approach:

- If you are planning to map in only one direction (from A to B), it may still be valuable to examine the concept pairs in the opposite direction. Sometimes that will identify previously unknown relationships.
- A mapping between two sources is likely to use a subset of the relationship types for a style. If you narrowly define your use case, such as only indicating absolute requirements, you might only use one relationship type.
- You may want to take a phased approach to mapping. For example, you may initially want to map only one or two particular relationship types within a style. In the future, you can always revisit your mapping and add more relationship types to it.
- Filling in the blanks in the relationship statements may make the mapping process less abstract. For example, instead of saying “X is one way of doing or achieving Y,” you might say, “Project function X is one way (an example) of doing or achieving SP 800-53 control Y.”
- If you want to distinguish the strongest (primary) relationships from other relationships, consider creating one mapping for the primary relationships and a separate mapping for the secondary relationships.
- Mapping can highlight ambiguities with wording, differences in granularity, duplication of concepts, and other issues within either of the sources being mapped. Be sure to capture and share these observations because they can significantly improve the next version of the affected sources.

References

[CSF11] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[CSF20] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[IR8278r1] Keller N, Quinn SD, Scarfone KA, Smith MC, Johnson V (2024) National Online Informative References (OLIR) Program: Overview, Benefits, and Use. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8278r1. https://doi.org/10.6028/NIST.IR.8278r1

[IR8278Ar1] Barrett MP, Keller N, Quinn SD, Smith MC, Scarfone KA, Johnson V (2024) National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8278Ar1. https://doi.org/10.6028/NIST.IR.8278Ar1

[ISO704] International Organization for Standardization (2022) *ISO 704:2022 – Terminology work – Principles and Methods* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/79077.html

[ISO1087] International Organization for Standardization (2019) *ISO 1087:2019 – Terminology work and terminology science – Vocabulary* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/62330.html

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-218] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

Appendix A. Glossary

concept
A “unit of knowledge created by a unique combination of characteristics.” [ISO1087]

concept crosswalk
A concept relationship style that identifies that a relationship exists between two concepts without any additional characterization of that relationship.

concept mapping
An indication that one concept is related to another concept.

concept relationship style
An explicitly defined convention for characterizing relationships for a use case.

concept source
A document or other resource that contains definitions of concepts.

concept system
A “set of concepts structured in one or more related domains according to the concept relations among its concepts.” [ISO1087]

concept type
A category of concepts found within a particular domain.

> *Note:* In the domain of cybersecurity and privacy, concept types include controls, requirements, recommendations, outcomes, technologies, functions, processes, techniques, roles, and skills.

mapping
See *concept mapping*.

one-source mapping
A mapping between concepts within a single concept source.

relationship style
See *concept relationship style*.

set theory relationship mapping
A concept relationship style derived from the branch of mathematics known as set theory.

> *Note:* Set theory relationship types include subset of, intersects with, equivalent, and superset of.

structural relationship mapping
A concept relationship style that captures an inherent hierarchical structure of concepts, usually defined within a single concept source.

> *Note:* Structural relationship types are parent-child.

supportive relationship mapping
A concept relationship style that identifies how one concept can or does help achieve another concept.

> *Note:* Supportive relationship types include supports, is supported by, identical, equivalent, and contrary.