Control Mapping: Additional Equivalencies (#1332)

Control Mapping Model currently in the development snapshot for review.

Relationships:

- **equivalent-to**:
- **equal-to**
- **subset-of**
- **superset-of**
- **intersects-with**

Req 1: Based on discussion, when an equivalent-to relationship between two controls is described, there will be **situations where the relationship needs context to specifically describe how the equivalence is achieved**.

Req 2: Additionally, there may be situations where this equivalency can be assured only in **one direction**, unless the how is precisely defined in a way that automation can interpret the intention of the author.

Req 3: Term **exceeds** - The source control, statement and/or requirement is more constrained than the target requirement. The requirement in the target will be met, but the comparison is not completely (or mathematically) equivalent. Term **precludes** - The source control, statement and/or requirement **prevents equivalency in the target**, or is deficient in some manner. The requirement in the target may not be met without constraints in the source. Some combinations may never be allowed.

Req 4 (1333): Not mapped.

Comparison

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

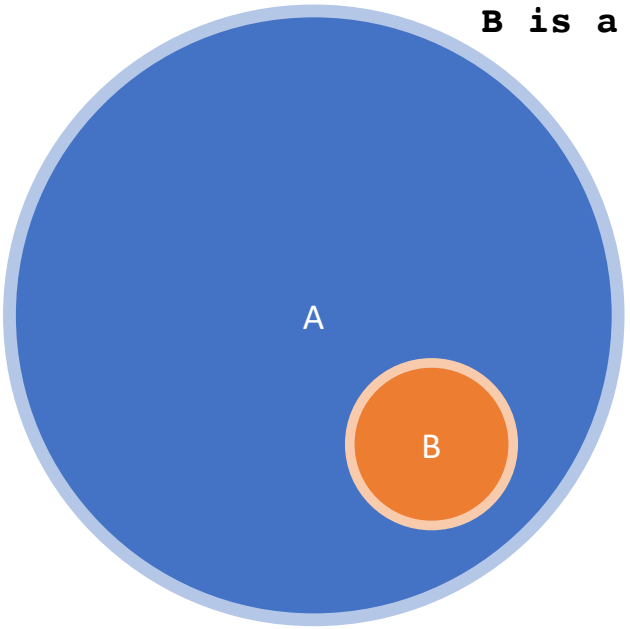
How are we comparing?

⊃

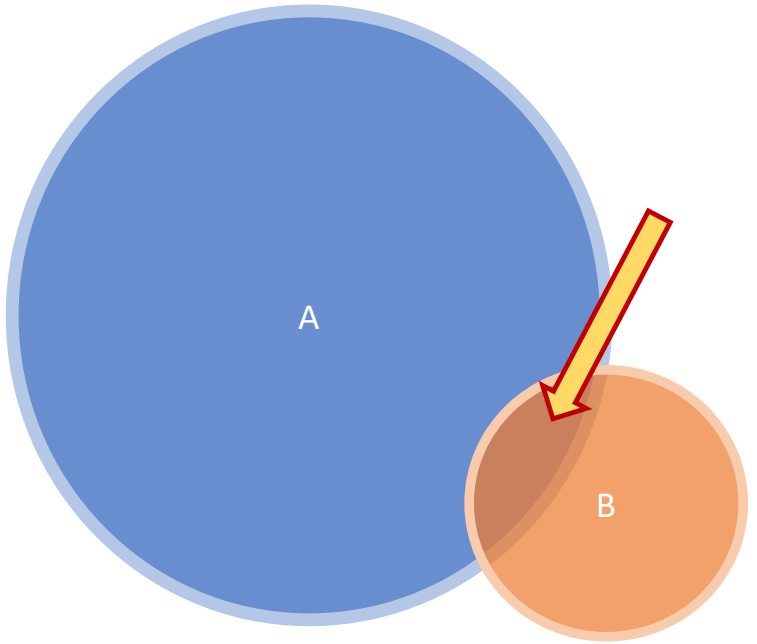
A is a SUPERSET of B

B is a SUBSET of A

⊂



A INTERSECTS B



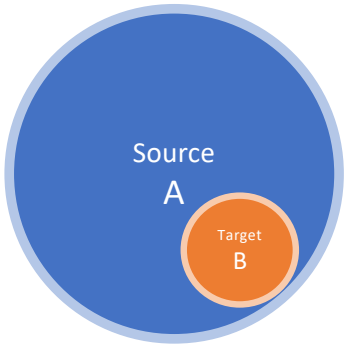
How is it described?

Fig 1

subset-of (Fig 1):

The effective requirements of the **source (A)** is a semantic **subset** of the effective requirements of the **target (B)**. This relationship may be reversed as a `superset-of`, since `A subset-of B` also means that `B superset-of A`.

Fig 2



superset-of (Fig 2):

The effective requirements of the **source (A)** is a semantic **superset** of the effective requirements of the **target (B)**. This relationship may be reversed as a `subset-of`, since `A superset-of B` also means that `B subset-of A`.

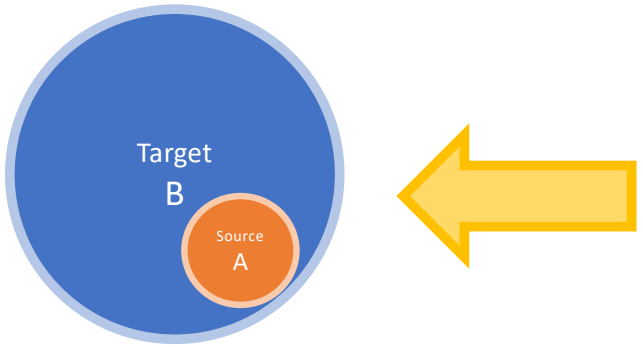
intersects-with (Not Shown):

The effective requirements of the source and target have **some semantic equivalence, but not all effective requirements from each are contained within the other**. This relationship may be reversed, since `A intersects-with B` also means that `B intersects-with A`. A lower granularity mapping, such as a statement level mapping using 'equivalent-to', 'subset-of', and/or 'superset-of', may provide a more functional mapping that allows for more inference than using this relationship type.

https://pages.nist.gov/OSCAL/reference/develop/mapping/json-definitions/#/assembly/oscal-mapping-common/map/relationship

What are we comparing?

Fig 1



subset-of (Fig 1):

The effective requirements of the **source (A)** is a semantic **subset** of the effective requirements of the **target (B)**. This relationship may be reversed as a `superset-of`, since `A subset-of B` also means that `B superset-of A`.

Terms:

- "Effective Requirements"
- "Semantic"

Guidance (OSCAL Documentation):

- "When establishing relationships, mapping SHOULD be done at the control statement level where possible."

All requirements of **A** are covered by **B**.

ALSO

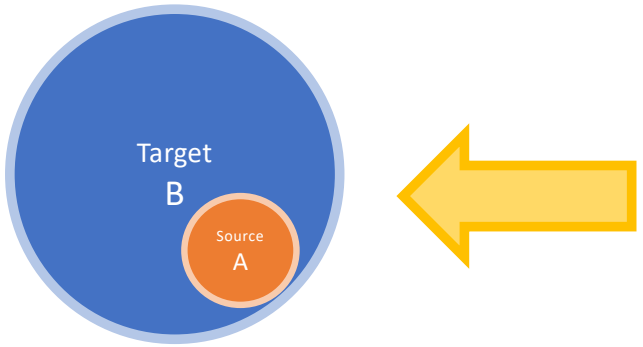
Superset B subsumes **Subset A**.

ALSO

B is more **COMPREHENSIVE** than A.

A Basic Subset

Fig 1



subset-of (Fig 1):

The effective requirements of the **source (A)** is a semantic **subset** of the effective requirements of the **target (B)**. This relationship may be reversed as a `superset-of`, since `A subset-of B` also means that `B superset-of A`.

Source (Control A): **Encrypts data in transit.**

Target (Control B): **Encrypts data in transit.**
Encrypts data at rest.

All requirements of **A** are covered by **B**.

ALSO

Superset B subsumes **Subset A**.

ALSO

B is more **COMPREHENSIVE** than A.

Scenario 1

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

Scenario 1

NIST 800-53 Rev 5, CM-8 CONFIGURATION MANAGEMENT

- **CM-8** SYSTEM COMPONENT INVENTORY
- **CM-8.1** UPDATES DURING INSTALLATION AND REMOVAL

~~NIST CSF | Asset Management (ID.AM)~~

~~HIPAA / Code Federal of Regulations (CFR)~~

- ~~§ 164.310 Physical safeguards.~~

CIS Controls v8, Establish and Maintain Detailed Enterprise Asset Inventory

- **1.1 Establish and Maintain Detailed Enterprise Asset Inventory**
- ~~2.1 Establish and Maintain a Software Inventory~~

~~FedRAMP~~

NIST 800-53 Rev 5 - CM-8

System Component Inventory

a. Develop and document an inventory of system components that:

1. Accurately reflects the system;
2. Includes all components within the system;
3. Does not include duplicate accounting of components or components assigned to any other system;
4. Is at the level of granularity deemed necessary for tracking and reporting; and
5. Includes the following information to achieve system component accountability:
   [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and

b. Review and update the system component inventory ***[Assignment: organization-defined frequency].***

NIST 800-53 Rev 5 - CM-8.1 **(must include CM-8)**

Update the inventory of system components as part of component installations, removals, and system updates.

https://raw.githubusercontent.com/usnistgov/oscal-content/main/nist.gov/SP800-53/rev5/xml/NIST_SP-800-53_rev5_catalog.xml

CIS v8 – Control 1.1 (One Statement)

Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include:

- end-user devices (including portable and mobile),
- network devices,
- non-computing/IoT devices, and
- servers.

Ensure the inventory records the:

- network address (if static),
- hardware address,
- machine name,
- data asset owner,
- department for each asset,
- and whether the asset has been approved to connect to the network.

For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise.

Review and update the inventory of all enterprise assets bi-annually, or more frequently.

https://github.com/CISecurity/CISControls_OSCAL/blob/main/src/catalogs/xml/cis-controls-v8_OSCAL-1.0.xml#L64

Keep this question in mind!

Is **CISC 1.1** more ***strict*** than **CM-8 + CM-8.1**?

Are all these saying the same thing? (Req 3)

- **CISC 1.1** SUPERSET of **CM-8+**?
- **CISC 1.1** more comprehensive than **CM-8+**?
- **CISC 1.1** subsumes **CM-8+**?
- All requirements of **CM-8+** are covered by **CISC 1.1**?

The Snapshot Example

```
<mapping uuid="9eb2019c-f3be-4f96-947e-58876a46b2a9">
    <source-resource type="catalog" href="#NOTAUUID-CISC-0000-..."></source-resource>
    <target-resource type="catalog" href="#NOTAUUID-NIST-0000-..."></target-resource>
    <map uuid="NOTAUUID-0000-...">
        <relationship> subset-of </relationship>

        <source type="control" id-ref="#cis-1.1"/>
        <target type="control" id-ref="#cm-8">
        + <using-param id="cm-08_odp.02">at least bi-annually</using-param>
          <!— Meets Req 1: And does that mean this relationship is now equivalent? -->
        </target>
        <target type="control" id-ref="#cm-8.1"/>

        <remarks>
            <p>The combination of SP 800-53 CM-8 and CM-8(1)
                describe similar implementation requirements to CIS 1.1.</p>
        </remarks>
    </map>
</mapping>
```

subset-of:

The effective requirements of the **source (A)** is a semantic **subset** of the effective requirements of the **target (B)**. This relationship may be reversed as a `superset-of`, since `A subset-of B` also means that `B superset-of A`.

https://raw.githubusercontent.com/usnistgov/OSCAL/develop/src/metaschema/examples/cis-sp-800-53-mapping.xml