

CAPORDINO: A Data Converter to OSCAL Catalogs

NIST

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

Selena Xiao, Computer Scientist, NIST

Disclaimer

Certain commercial OSCAL solutions (or companies) will be identified, discussed or demonstrated.

Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the solutions identified are necessarily the best available for the purpose.



Agenda



1. Background
2. CPRT
3. CAPORDINO high level
4. CAPORDINO technical details
5. Future work

Background



Executive Order 14144 - Strengthening and Promoting Innovation in the Nation's Cybersecurity

"... establish a pilot program of a rules-as-code approach for machine-readable versions of policy and guidance that OMB, NIST, and CISA publish and manage regarding cybersecurity."

OSCAL (Open Security Controls Assessment Language), a standardized machine-readable language to document security controls, supports this mission of security assessment automation.

Background



GOAL

security assessment
automation



REFERENCE DATA

standardized, machine-readable
format (OSCAL)



DATA CONVERSION

manual, time-intensive,
labor-intensive

CPRT

Cybersecurity and Privacy Reference Tool (CPRT) - <https://csrc.nist.gov/projects/cprt>

Cybersecurity and Privacy Reference Tool CPRT



CPRT Catalog

The Cybersecurity and Privacy Reference Tool (CPRT) highlights the reference data from NIST publications without the constraints of PDF files. This enables stakeholders to interactively browse, search, and export the data in a structured format that is human- and machine-consumable. For example, you can use the search tool to locate reference data in each publication and then download the reference data for each publication in MS Excel or JSON.

We will be adding more NIST datasets to this catalog. See the [CPRT Roadmap](#) for future planned functionalities.

Reference Dataset	Publication Title	Status	Released
SP 800-171A Rev 3	Assessing Security Requirements for Controlled Unclassified Information, 3.0.0	Final	05/14/2024
SP 800-171 Rev 3	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 3.0.0	Final	05/14/2024
NICE Components v1.0.0	Workforce Framework for Cybersecurity (NICE Framework) (NIST SP 800-181 Rev 1), 1.0.0	Final	03/05/2024
Cybersecurity Framework v2.0	NIST Cybersecurity Framework, Version 2.0	Final	02/26/2024
SP 800-66 Rev 2	Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide, 2.0.0	Final	02/14/2024

CPRT JSON

```
"documents": [
  {
    "doc_identifier": "CSF_2_0_0",
    "name": "The NIST Cybersecurity Framework 2.0 Draft",
    "version": "Version 2.0",
    "website": "https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd"
  }
],
"relationship_types": [
  {
    "relationship_identifier": "projection",
    "description": "Represents a relationship between two elements."
  }
],
"elements": [
  {
    "element_type": "function",
    "element_identifier": "GV",
    "title": "GOVERN",
    "text": "Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy",
    "doc_identifier": "CSF_2_0_0"
  },
  {
    "element_type": "category",
    "element_identifier": "GV.OC",
    "title": "Organizational Context",
    "text": "The circumstances - mission, stakeholder expectations, and legal, regulatory, and contractual requirements - surrounding the"
  }
],
"relationships": [
  {
    "source_element_identifier": "GV",
    "source_doc_identifier": "CSF_2_0_0",
    "dest_element_identifier": "GV.OC",
    "dest_doc_identifier": "CSF_2_0_0",
    "relationship_identifier": "projection",
    "provenance_doc_identifier": "CSF_2_0_0"
  }
],
```

Security
reference data
in a structured
format

Data is split into elements and relationships

CPRT and OSCAL

```
"elements": [  
  {  
    "element_type": "function",  
    "element_identifier": "GV",  
    "title": "GOVERN",  
    "text": "Establish and monitor the organization's  
    "doc_identifier": "CSF_2_0_0"  
  },  
  {  
    "element_type": "category",  
    "element_identifier": "GV.OC",  
    "title": "Organizational Context",  
    "text": "The circumstances – mission, stakeholder  
    "doc_identifier": "CSF_2_0_0"  
  },  
]
```

```
"relationships": [  
  {  
    "source_element_identifier": "GV",  
    "source_doc_identifier": "CSF_2_0_0",  
    "dest_element_identifier": "GV.OC",  
    "dest_doc_identifier": "CSF_2_0_0",  
    "relationship_identifier": "projection",  
    "provenance_doc_identifier": "CSF_2_0_0"  
  },  
]
```

```
<catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0" uuid="720a010b-253c-4a94-bb65-cb58400966f5">  
  <metadata>  
    </responsible-party>  
  </metadata>  
  <group id="GV" class="function">  
    <title>GOVERN</title>  
    <prop name="sort-id" value="00001" />  
    <prop name="label" value="GOVERN (GV)" />  
    <part id="GV_overview" name="overview">  
      <p>The organization's cybersecurity risk management strategy, expectations, and policy  
      are established, communicated, and monitored</p>  
    </part>  
    <control id="GV.OC" class="category">  
      <title>Organizational Context</title>  
      <prop name="sort-id" value="00001.00001" />  
      <prop name="label" value="Organizational Context (GV.OC)" />  
      <part id="GV.OC_statement" name="statement">  
        <p>The circumstances – mission, stakeholder expectations, dependencies, and legal,  
        regulatory, and contractual requirements – surrounding the organization's  
        cybersecurity risk management decisions are understood</p>  
      </part>  
      <control id="GV.OC-01" class="subcategory">  
        <title>GV.OC-01</title>  
        <prop name="risk-party" ns="https://csrc.nist.gov/ns/csrf" value="1st">  
          <remarks>  
            <p>1st Party Risk</p>  
          </remarks>  
        </prop>  
      </control>  
    </control>  
  </group>  
</catalog>
```

Without CAPORDINO



With CAPORDINO



<https://github.com/usnistgov/capordino>

Cybersecurity And Privacy Open Reference Datasets IN Oscal (CAPORDINO)

Development of tooling to allow conversion of datasets managed by the [Cybersecurity and Privacy Reference Tool \(CPRT\)](#) into [OSCAL](#) formats.

Currently, the command line tool supports generating CSF 2.0 catalog.

Building

Clone the git repository

```
git clone https://github.com/usnistgov/capordino.git  
cd capordino/
```



Installing Capordino

1. Use Maven to install dependencies and build

```
mvn install
```



CAPORDINO and OSCAL Projects

Modeling framework

Metaschema

Java library for Metaschema

metaschema-
java

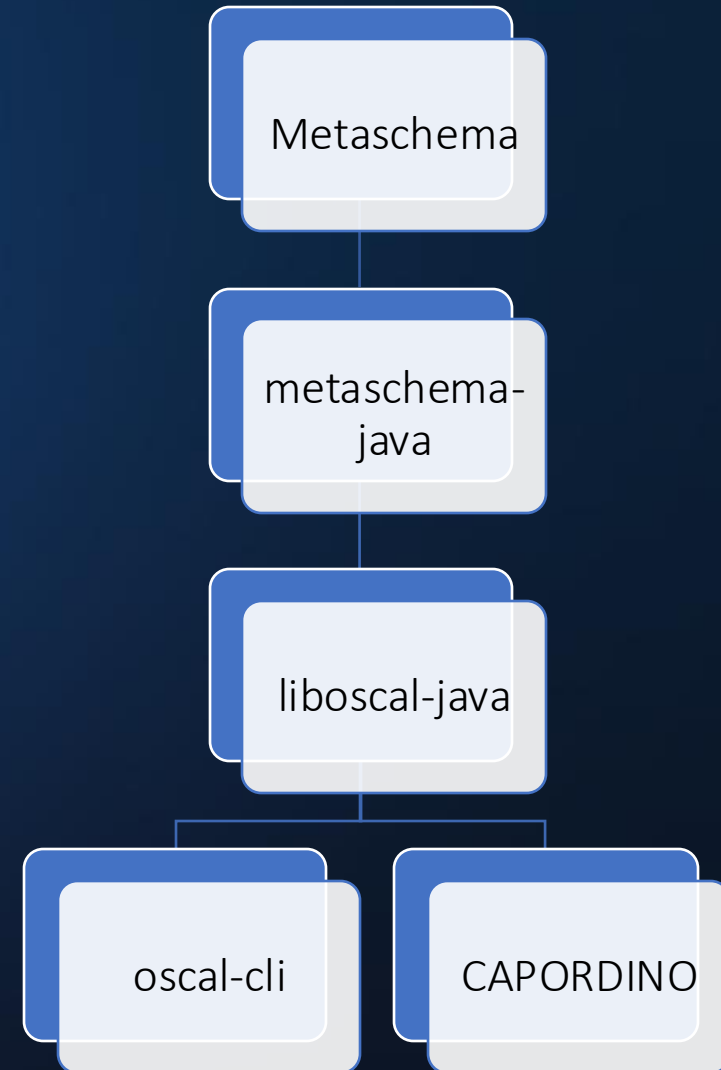
Java library for OSCAL

liboscal-java

Command line tools

oscal-cli

CAPORDINO



CAPORDINO

Running Capordino CLI

Basic template to run capordino.sh

Use --help to see the available options. `./capordino.sh --help`

```
Usage: capordino [-hV] [-o=<output_directory>] <framework version identifier>
       <framework version identifier>
       REQUIRED: framework version identifier to build catalog for
       Implemented: CSF_2_0_0, SP_800_171_3_0_0
-h, --help      Show this help message and exit.
-o, --output-directory=<output_directory>
                Directory for capordino tool output (built catalog), default
                is "./catalogs/"
-V, --version   Print version information and exit.
```

```
./capordino.sh -o "catalogs/nist.gov/CSF/" "CSF_2_0_0"
```

```
<?xml version="1.0" encoding="UTF-8"?>
<catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0" uuid="720a010b-253c-4a94-bb65-cb58400966f5">
  <metadata>
    <title>NIST Cybersecurity Framework</title>
    <published>2024-02-25T19:00:00-05:00</published>
    <last-modified>2025-02-10T12:08:20.050176-05:00</last-modified>
    <version>Version 2.0</version>
    <oscal-version>v1.1.2</oscal-version>
    <prop name="framework-identifier" ns="https://csrc.nist.gov/ns/cprt" value="CSF" />
    <prop name="framework-version-identifier" ns="https://csrc.nist.gov/ns/cprt"
      value="CSF_2_0_0" />
    <prop name="generated-by" ns="https://csrc.nist.gov/ns/cprt"
      value="Cybersecurity And Privacy Open Reference Datasets In OSCAL (CAPORDINO)" />
    <prop name="publication-status" ns="https://csrc.nist.gov/ns/cprt" value="Final" />
    <link href="#a7f54afa-16cf-4200-a043-85aa554b93e4" rel="alternate" />
    <link href="#2b37a38e-9ea9-482b-a1b4-ada6cca7e0bd" rel="canonical" />
    <role id="publisher">
      <title>Publisher</title>
    </role>
    <role id="contact">
      <title>Contact</title>
    </role>
    <role id="author">
      <title>Author</title>
    </role>
    <party uuid="8238c306-4ee0-4321-a4fb-503adda3d8c1" type="organization">
      <name>National Institute of Standards and Technology</name>
      <short-name>NIST</short-name>
    </party>
  </metadata>
</catalog>
```

Part 1: Mapping

CPRT API



CPRT JSON file



POJO – Plain Old
Java Objects
(CpRtElement,
CpRtRelationship)



Conversion (next
slide)

```
"elements": [  
  {  
    "element_type": "function",  
    "element_identifier": "GV",  
    "title": "GOVERN",  
    "text": "Establish and monitor the organization's cybersecurity risk",  
    "doc_identifier": "CSF_2_0_0"  
  },  
]
```

```
package gov.nist.capordino.cprt.pojo;  
  
public class CpRtElement {  
    public String element_type;  
    public String element_identifier;  
    public String title;  
    public String text;  
    public String doc_identifier;  
  
    public String getGlobalIdentifier() {  
        return doc_identifier + ":" + element_identifier;  
    }  
}
```

```
"relationships": [  
  {  
    "source_element_identifier": "GV",  
    "source_doc_identifier": "CSF_2_0_0",  
    "dest_element_identifier": "GV.OC",  
    "dest_doc_identifier": "CSF_2_0_0",  
    "relationship_identifier": "projection",  
    "provenance_doc_identifier": "CSF_2_0_0"  
  },  
]
```

```
public class CpRtRelationship {  
    public String source_element_identifier;  
    public String source_doc_identifier;  
    public String dest_element_identifier;  
    public String dest_doc_identifier;  
    public String relationship_identifier;  
    public String provenance_doc_identifier;  
}
```

```

public abstract class AbstractOscalConverter {
    protected Stream<CprtElement> getRelatedElementsBySourceIdWithType(String sourceId, String elemType) {
        return cprtRoot.getRelationships().stream()
            .filter(rel -> rel.getSourceGlobalIdentifier().equals(sourceId))
            .map(rel -> {
                CprtElement element = cprtRoot.getElementById(rel.getDestGlobalIdentifier());
                if (element == null) {
                    throw new IllegalArgumentException("Error getting elements related to sourceId " + sourceId +
                }
                return element;
            })
            .filter(elem -> elem.element_type.equals(elemType));
    }
}

```

```

public class Csf20CprtOscalConverter extends AbstractOscalConverter {
    /**
     * Build the top level group of the catalog, represented in CPRT as functions.
     */
    private List<CatalogGroup> buildFunctionGroups(Catalog catalog) {
        return cprtRoot.getElements().stream()
            .filter(elem -> elem.element_type.equals(FUNCTION_ELEMENT_TYPE))
            .map(elem -> {
                // For each CSF 2.0 function, create an OSCAL group
                CatalogGroup group = new CatalogGroup();
                group.setId(elem.element_identifier);
                group.setClazz(elem.element_type);
                group.setTitle(MarkupLine.fromMarkdown(elem.title));
            });
    }
}

```

Part 2: Conversion

Part 2: Conversion



NIST Cybersecurity Framework, Version 2.0

Search: 🔍 ℹ️

CPRT / Version 2.0 / All

GOVERN (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

> [Show all GV References](#) ℹ️

Export ℹ️

- JSON
- MS Excel

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood > Show all GV.OC References ℹ️	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management > Show all GV.OC-01 References ℹ️	Ex1: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered > Show all GV.OC-02 References ℹ️	Ex1: Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) Ex2: Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 3.0.0

CPRT / SP 800-171 / 03.01 / 03.01.01

Access Control (03.01)

03.01.01: Account Management

> [Show all 03.01.01 References](#) ⓘ

Different frameworks, different elements

Export ▾

SP 800-171 Security Requirement

SP 800-171A Assessment Procedure

Both

- a. Define the types of system accounts allowed and prohibited.
- b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.
- c. Specify:
 01. Authorized users of the system,
 02. Group and role membership, and
 03. Access authorizations (i.e., privileges) for each account.
- d. Authorize access to the system based on:
 01. A valid access authorization and
 02. Intended system usage.
- e. Monitor the use of system accounts.
- f. Disable system accounts when:
 01. The accounts have expired,
 02. The accounts have been inactive for [Assignment: organization-defined time](#)

SP 800-171A Assessment Objectives

Determine If

A.03.01.01.ODP[01]	the time period for account inactivity before disabling is defined.
A.03.01.01.ODP[02]	the time period within which to notify account managers and designated personnel or roles when accounts are no longer required is defined.
A.03.01.01.ODP[03]	the time period within which to notify account managers and designated personnel or roles when users are terminated or transferred is defined.

Catalog

NIST Cybersecurity Framework, Version 2.0

CPRT / Version 2.0 / All

GOVERN (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

[Show all GV References](#) ⓘ

Category	Subcategory
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood Show all GV.OC References ⓘ	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management Show all GV.OC-01 References ⓘ
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered Show all GV.OC-02 References ⓘ

```
<catalog xmlns="http://csrc.nist.gov/ns/oscal/1.0" uuid="720a010b-253c-4a94-bb65-cb58400966f5">
  <metadata>
    </responsible-party>
  </metadata>
  <group id="GV" class="function">
    <title>GOVERN</title>
    <prop name="sort-id" value="00001" />
    <prop name="label" value="GOVERN (GV)" />
    <part id="GV_overview" name="overview">
      <p>The organization's cybersecurity risk management strategy, expectations, and policy
        are established, communicated, and monitored</p>
    </part>
    <control id="GV.OC" class="category">
      <title>Organizational Context</title>
      <prop name="sort-id" value="00001.00001" />
      <prop name="label" value="Organizational Context (GV.OC)" />
      <part id="GV.OC_statement" name="statement">
        <p>The circumstances - mission, stakeholder expectations, dependencies, and legal,
          regulatory, and contractual requirements - surrounding the organization's
          cybersecurity risk management decisions are understood</p>
      </part>
      <control id="GV.OC-01" class="subcategory">
        <title>GV.OC-01</title>
        <prop name="risk-party" ns="https://csrc.nist.gov/ns/csrf" value="1st">
          <remarks>
            <p>1st Party Risk</p>
          </remarks>
        </prop>
      </control>
    </control>
  </group>
</catalog>
```

Challenges

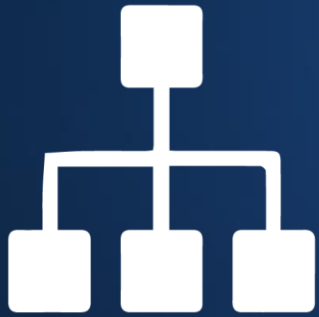
Some manual work is still required – identifying elements and relationships

Different security frameworks, different elements, different complexity in implementation

```
{
  "name": "Cybersecurity Framework",
  "elementTypes": ["category","function","implementation_example","party","sort","subcategory","withdraw_reason"]
}

{
  "name": "SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations",
  "elementTypes": ["determination","discussion","examine","family","interview","odp","odp_statement","odp_type",
    "reference","requirement","security_requirement","test","withdraw_reason"]
}
```

Future Work



Other frameworks
provided by CPRT



Collaborate with
OSCAL community



Extend to other
input sources



Thank you!