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

NIST Cybersecurity Framework 2.0:

Informative References Quick-Start Guide

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 1347 ipd
https://doi.org/10.6028/NIST.SP.1347.ipd
Please send comments to csf@nist.gov
March 2026

INTRODUCTION

What Are Informative References?

There are many national and international standards, guidelines, frameworks, and regulations for cybersecurity risk management. A common challenge for practitioners is identifying all the applicable requirements and recommendations across these documents and then making sense of them in aggregate. Here are two scenarios (from NIST IR 8278r1):

- Implementing a new security control X would help satisfy certain requirements and recommendations from other documents.
- The organization needs to comply with a new standard, so it is necessary to determine which of its requirements are already met, which are not currently met, and which potentially conflict with other requirements.

Informative References identify relationships between elements of different source documents and can be consumed in human- or machine-readable formats. For example, within the CSF 2.0, each informative reference indicates one or more parts of another document in which readers can find additional information on the topic (known as a *crosswalk*). This can be useful as organizations work toward achieving the outcomes of the CSF 2.0.

Purpose of this QSG:

- Feature multiple NIST tools for accessing, viewing, and using informative references
- Highlight how non-NIST entities can submit informative references
- Provide supporting materials and references for further exploration

NIST provides multiple ways to view and work with informative references. A few* tools that offer **different levels of detail and customization** are featured below. The following pages of this Quick-Start Guide (QSG) provide readers with an overview of how to find and use each of these tools.

1. Direct Download in Excel Format (Page 3)	This downloads **all CSF 2.0 informative references that have been published to date** into an Excel spreadsheet.
2. CSF 2.0 Reference Tool (Page 4)	This option allows users to filter **CSF 2.0 informative references to view**. Results can be exported into Excel or JSON.
3. Online Informative References Program (OLIR) (Page 5)	This tool offers the most customization and allows users to **expand beyond CSF 2.0** to view informative references for other NIST publications.

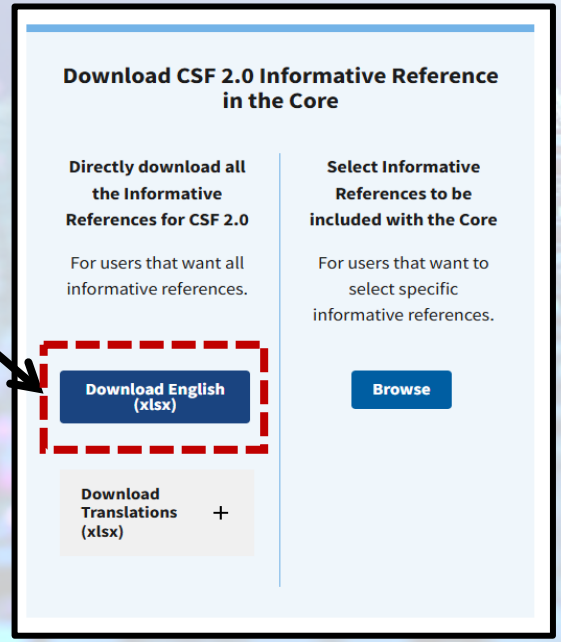
**The Cybersecurity and Privacy Reference Tool (CPRT) is another NIST tool that highlights the reference data from NIST publications. It provides a standard way to view NIST publications without the constraints of PDF and enables stakeholders to interactively browse, search, and export data in a structured format that is human- and machine-consumable.*

Option 1. Direct Download in Excel Format

*This option enables users to download **all CSF 2.0 informative references that have been published to date** into an Excel spreadsheet.*

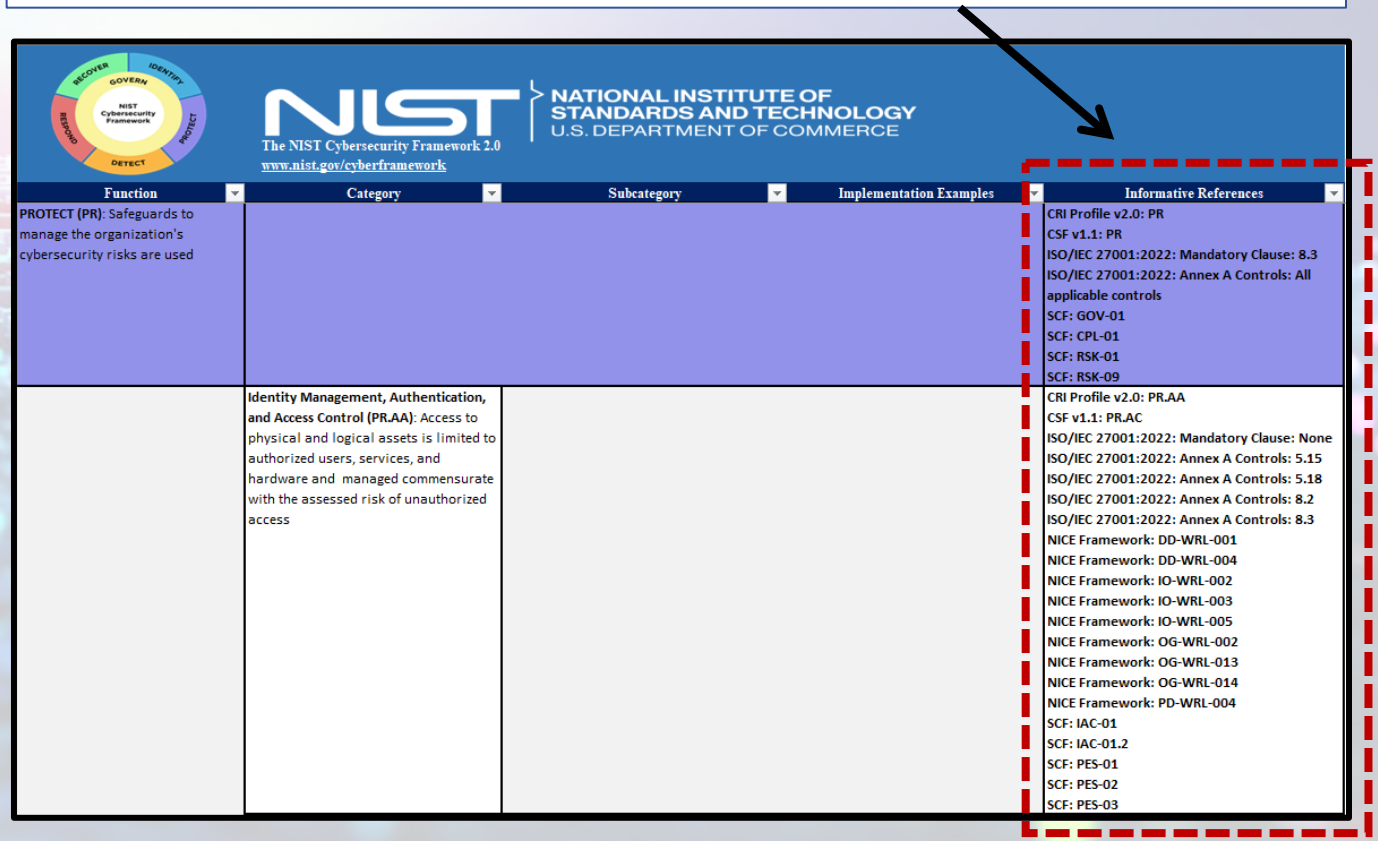
Get Started

1) Navigate to the CSF 2.0 Informative References page and select "Download CSF 2.0 Informative References in the Core."



View Results

2. Below is a snapshot of what the Excel file will look like with columns for CSF 2.0 Functions, Categories, Subcategories, implementation examples, and informative references.



The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework

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

Function	Category	Subcategory	Implementation Examples	Informative References
PROTECT (PR): Safeguards to manage the organization's cybersecurity risks are used				CRI Profile v2.0: PR CSF v1.1: PR ISO/IEC 27001:2022: Mandatory Clause: 8.3 ISO/IEC 27001:2022: Annex A Controls: All applicable controls SCF: GOV-01 SCF: CPL-01 SCF: RSK-01 SCF: RSK-09
	Identity Management, Authentication, and Access Control (PR.AA): Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access			CRI Profile v2.0: PR.AA CSF v1.1: PR.AC ISO/IEC 27001:2022: Mandatory Clause: None ISO/IEC 27001:2022: Annex A Controls: 5.15 ISO/IEC 27001:2022: Annex A Controls: 5.18 ISO/IEC 27001:2022: Annex A Controls: 8.2 ISO/IEC 27001:2022: Annex A Controls: 8.3 NICE Framework: DD-WRL-001 NICE Framework: DD-WRL-004 NICE Framework: IO-WRL-002 NICE Framework: IO-WRL-003 NICE Framework: IO-WRL-005 NICE Framework: OG-WRL-002 NICE Framework: OG-WRL-013 NICE Framework: OG-WRL-014 NICE Framework: PD-WRL-004 SCF: IAC-01 SCF: IAC-01.2 SCF: PES-01 SCF: PES-02 SCF: PES-03

Option 2. CSF 2.0 Reference Tool

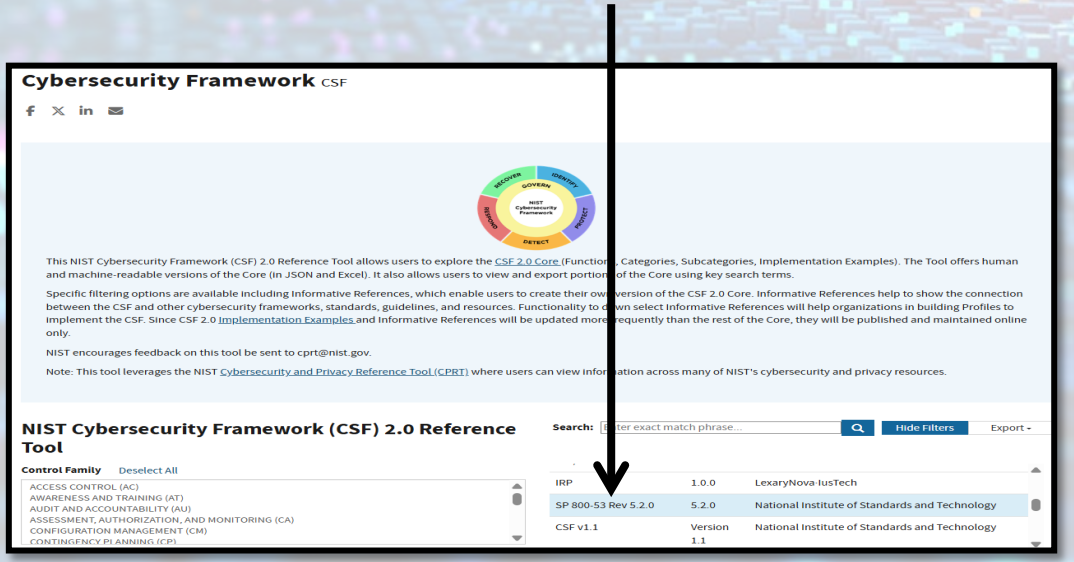
***This tool allows users to dynamically view, filter, and export** CSF 2.0 informative references right from a web browser.*

Get Started

1. Access the CSF 2.0 Reference Tool. The CSF 2.0 Core will automatically display on the page. From here, customize by filtering the informative references.

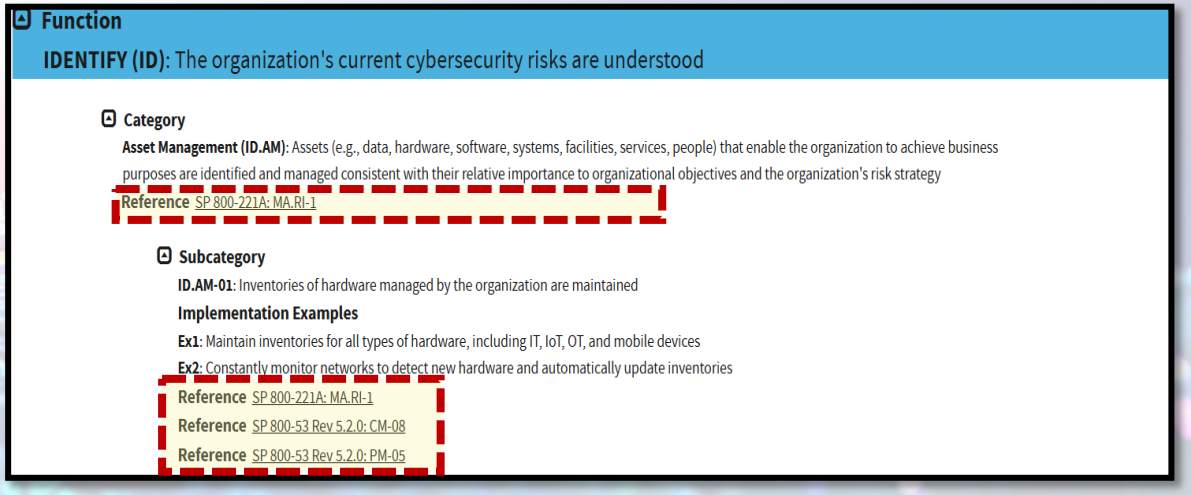
Filter by Informative References

2. Select the "**Filter**" button from the menu at the top of the page.
3. From the dropdown list, choose one or more of the available options. The row will highlight to indicate which informative reference is selected.



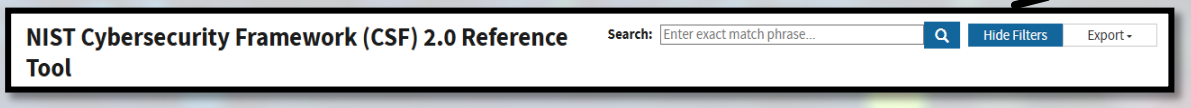
View Results

4. View the chosen informative references from the browser (highlighted below for emphasis).



Export Results

5. Export the results into Excel or JSON by selecting the "Export" button at the top of the page.



Option 3. Online Informative References Program (OLIR)

This tool offers the most customization for viewing informative references and ***allows users to expand beyond the CSF 2.0 to see informative references for other NIST publications****.*

How to Get Started

1. Access the Online Informative References Program (OLIR).

Filter by Informative References

2. Open the Informative Reference Catalog and select a focal document. A focal document is a NIST document (e.g., CSF 2.0, SP 800-53) whose elements are compared with those from another document.
3. Select an informative reference from the dropdown list.
4. Click the "**search**" button at the bottom of the page.
5. The results will appear at the bottom of the page.

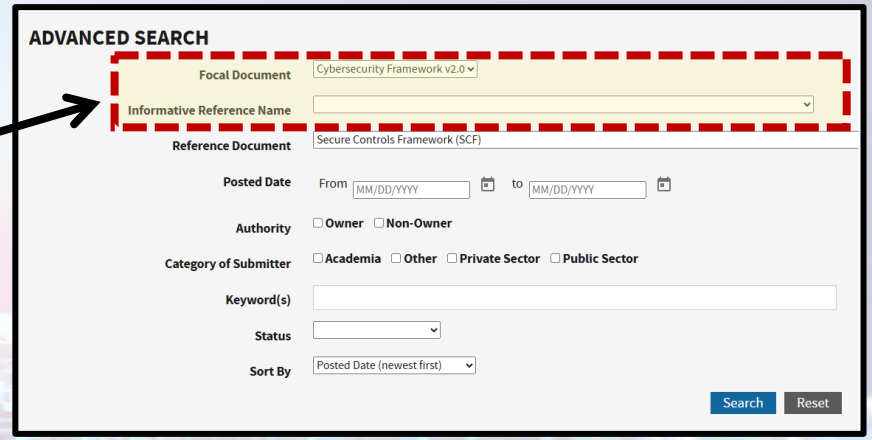
View Elements Across Multiple Informative References

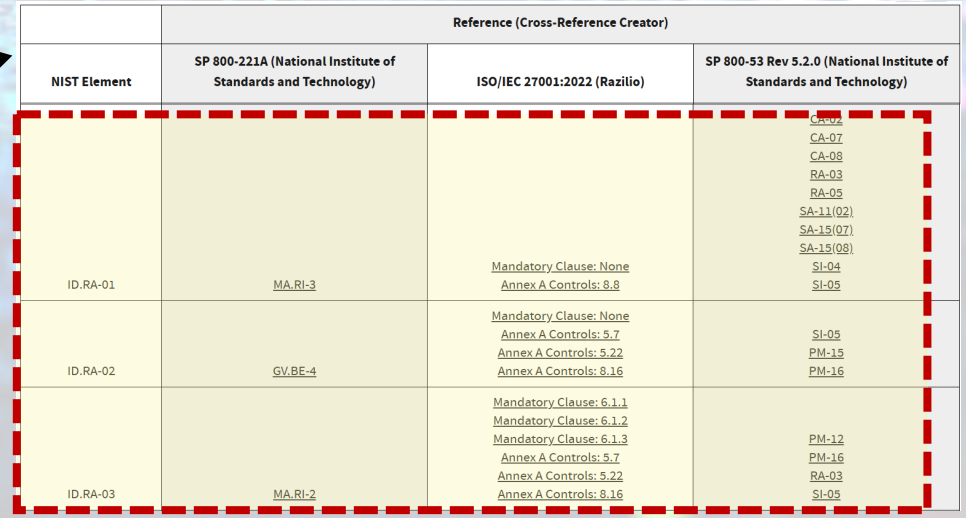
6. Open the cross-reference comparison report.
7. Select the NIST focal document and informative reference(s). You can display potential relationships for as many references that are available for a given focal document by selecting all available references from the menu.
8. Generate results to view in the browser or export into CSV or JSON.

Submit an Informative Reference to OLIR

Informative references are submitted by NIST and non-NIST entities.

Follow NIST IR 8278A Rev. 1 submission guidelines and complete the OLIR submission template. Email questions to olir@nist.gov.





	Reference (Cross-Reference Creator)		
NIST Element	SP 800-221A (National Institute of Standards and Technology)	ISO/IEC 27001:2022 (Razilio)	SP 800-53 Rev 5.2.0 (National Institute of Standards and Technology)
ID.RA-01	MA.RI-3	Mandatory Clause: None Annex A Controls: 8.8	CA-02 CA-07 CA-08 RA-03 RA-05 SA-11(02) SA-15(07) SA-15(08) SI-04 SI-05
ID.RA-02	GV.BE-4	Mandatory Clause: None Annex A Controls: 5.7 Annex A Controls: 5.22 Annex A Controls: 8.16	SI-05 PM-15 PM-16
ID.RA-03	MA.RI-2	Mandatory Clause: 6.1.1 Mandatory Clause: 6.1.2 Mandatory Clause: 6.1.3 Annex A Controls: 5.7 Annex A Controls: 5.22 Annex A Controls: 8.16	PM-12 PM-16 RA-03 SI-05

USE CASE 1: USING INFORMATIVE REFERENCES TO ACHIEVE CYBERSECURITY OUTCOMES

Below is a sample use case that highlights how informative references and the NIST tools featured in this QSG can be used to view a connected path from the high-level integration of information and communications technology (ICT) risk into enterprise risk management (ERM) programs all the way down to the controls that can be used to achieve desired outcomes.

Start by ensuring that ICT risks receive appropriate attention within ERM programs.

SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*, provides **a framework of outcomes that apply to all types of ICT risks**, including cybersecurity, privacy, supply chain, and artificial intelligence.

View a crosswalk of CSF 2.0 to SP 800-221A to understand how elements across the two documents relate to one another.

Begin managing cybersecurity-specific ICT risks through CSF 2.0 outcomes.

The CSF 2.0 provides high-level outcomes to **address cybersecurity ICT risks**.

View the CSF 2.0 outcomes in the CSF 2.0 Reference Tool. Filter it to look for SP 800-221A and SP 800-53 informative references.

Apply SP 800-53 controls to achieve CSF 2.0 outcomes.

SP 800-53 provides a catalog of security and privacy controls for information systems and organizations. This can be **used to achieve the outcomes from the CSF 2.0.**

Delve deeper into the SP 800-53 informative reference in the CPRT to review specific control assessment procedures, explanations, control enhancements, and more.

USE CASE 2: USING INFORMATIVE REFERENCES FOR COMPARATIVE ANALYSIS

Organizations often incorporate more than one standard, guideline, or framework into their cybersecurity risk management strategy. Below is a sample use case that highlights how informative references and the NIST tools featured in this QSG can be used to view alignment and differences across "peer" documents. The hypothetical use case below shows an organization that is currently implementing the CSF 2.0 and wishes to also adopt ISO/IEC 27001.

Begin with the Framework Currently in Use

Start with a framework that the organization has already implemented (i.e., CSF 2.0).

- View the CSF 2.0 outcomes in the CSF 2.0 Reference Tool and export to JSON or Excel to identify CSF 2.0 outcomes that the organization is currently achieving.
- The organization can also reference its most recently completed CSF 2.0 Organizational Profile.

View a Crosswalk

From the CSF 2.0 Reference Tool, filter to select an informative reference that the organization wants to view, such as ISO/IEC 27001:2022.

- Export the results to view how the elements of the ISO standard relate to the CSF 2.0 outcomes.
- Use the OLIR cross-reference comparison report to view elements of more than one informative reference.

Conduct Comparative Analysis

While viewing the output, ask:

- Which cybersecurity outcomes or requirements are already being met by the organization?
- Which cybersecurity outcomes or requirements are not currently being met by the organization?
- Which cybersecurity outcomes or requirements conflict with each other?
- What resources will be needed to address gaps?
- Use this information to develop a CSF 2.0 Target Profile.

Important Note: Informative references submitted to the NIST OLIR Catalog, which feed into the CSF 2.0 Reference Tool, are developed by NIST and non-NIST entities. NIST conducts limited conformance testing of OLIR submission to IR 8278A. NIST does not conduct correctness testing on non-NIST submitted mappings, and the listing for non-NIST mappings in the catalog does not imply NIST endorsement.

USING INFORMATIVE REFERENCES IN CSF PROFILE DEVELOPMENT

What is an Organizational Profile?

- An Organizational Profile describes an organization's current or target cybersecurity posture in terms of the cybersecurity outcomes in the CSF Core.
- It is an exercise that helps leaders understand, tailor, assess, and prioritize CSF 2.0 outcomes based on the organization's mission objectives, stakeholder expectations, threat landscape, and requirements.

Using Informative References in CSF 2.0 Profile Development

- Informative references show examples of how other standards or guidelines address each CSF outcome.
- They help show what "good" for the organization can look like.
- The **gap** between today and the future helps the organization plan improvements by creating action plans.
- A recommended approach for developing action plans is to use the NIST CSF 2.0 Reference Tool to follow the references from the pertinent subcategories in the organization's Target Profile to the associated SP 800-53 security and privacy controls.

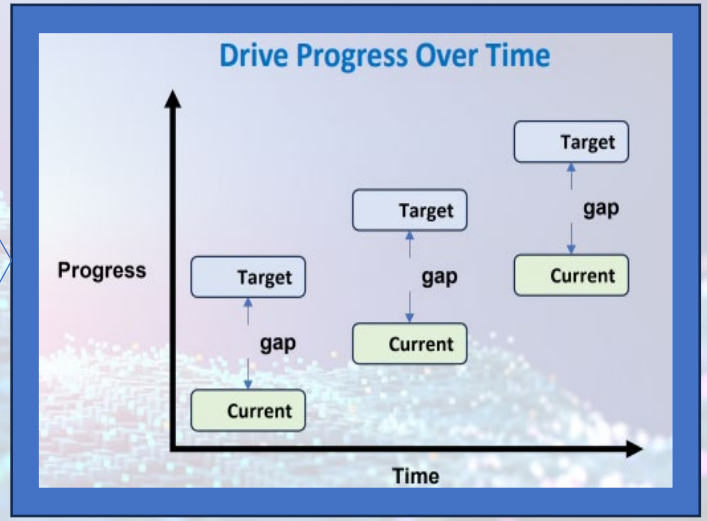
Applying Informative References to a Target Profile

- Look at the references that the organization plans to use.
- Pick the practices that represent where the organization wants to be in the future.

gap

Applying Informative References to a Current Profile

- Look at the references and check what is being achieved today.
- Decide whether the outcome is fully, partially, or not implemented today.



REFERENCE DATA AND ARTIFICIAL INTELLIGENCE (AI)

Reference Data and AI

- CPRT, the CSF 2.0 Reference Tool, and OLIR enable organizations to understand relationships among reference data within frameworks and guidelines, including NIST's AI-related work products (e.g., Cyber AI Profile, AI Risk Management Framework (AI RMF), SP 800-53 Control Overlays for Securing AI Systems), to show how they complement and relate to each other in support of effective implementation.
- As previously illustrated, data can be exported from these tools into a structured format. Practitioners can then leverage AI tools to analyze, compare, or crosswalk frameworks.
- The table below shows examples of how artificial intelligence (AI) tools can support reference data use.

Why It's Useful	What AI Can Do
NIST reference data includes authoritative identifiers (e.g., CCEs, CVEs, control IDs, document element IDs).	Anchor reasoning to real, globally unique elements and avoid hallucinated mappings.
Informative References define explicit human-curated relationships between frameworks.	Perform accurate crosswalks based on validated NIST relationships.
DRMs connect transitive logic relationships across documents.	Surface deeper alignment patterns and identify overlaps/gaps that are not explicitly mapped.
CPRT and CSF 2.0 Reference Tool exports include structured formats (e.g., JSON, Excel, XML, XLSX).	Directly ingest structured data and perform automated comparison, alignment, and aggregation.
OCIL/OSCAL artifacts convert human responses into machine-readable data.	Merge policy texts, assessments, and scan results to generate SSPs, SARs, RARs, and other outputs.

Glossary of Acronyms

- **CCE:** Common Configuration Enumeration
- **CVE:** Common Vulnerabilities and Exposures
- **DRM:** Derived Relationship Mapping
- **JSON:** JavaScript Object Notation
- **OCIL:** Open Checklist Interactive Language
- **OSCAL:** Open Security Controls Assessment Language
- **RAR:** Risk Assessment Report
- **SAR:** Security Assessment Report
- **SSP:** System Security Plan
- **XLSX:** Microsoft Excel Spreadsheet Format
- **XML:** eXtensible Markup Language

ADDITIONAL RESOURCES

Additional Resources

CSF 2.0 References

- CSF 2.0 Resource Library
- CSF 2.0 Informative References page

OLIR References

- OLIR Program (CSRC)
- OLIR Submissions
- NIST IR 8278 Rev. 1 (Overview, Benefits, Use)
- NIST IR 8278A Rev. 1 (Submission Guidance)

Email submissions

- NIST CSF feedback: csf@nist.gov
- OLIR email submission: olir@nist.gov

Glossary of Acronyms

- **CSF:** Cybersecurity Framework
- **CSRC:** Computer Security Resource Center
- **OLIR:** Online Informative References
- **QSG:** Quick-Start Guide