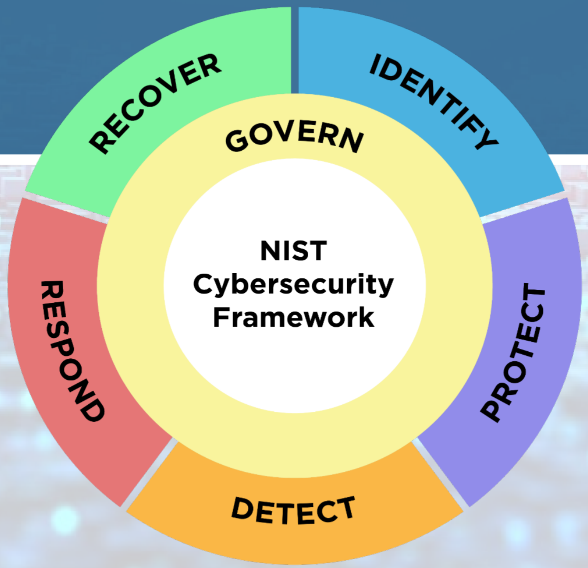
NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# NIST Cybersecurity Framework 2.0:

## Quick-Start Guide for Creating and Using Organizational Profiles



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*

**NIST Special Publication**
**NIST SP 1301**
https://doi.org/10.6028/NIST.SP.1301
February 2024

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## INTRODUCTION

### Drive Progress Over Time with Organizational Profiles

An ***Organizational Profile*** describes an organization's current and/or target cybersecurity posture in terms of cybersecurity outcomes from the Cybersecurity Framework (CSF) Core. Organizational Profiles are used to understand, tailor, assess, and prioritize cybersecurity outcomes based on an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. The organization can then act strategically to achieve those outcomes. These Profiles can also be used to assess progress toward targeted outcomes and to communicate pertinent information to stakeholders.

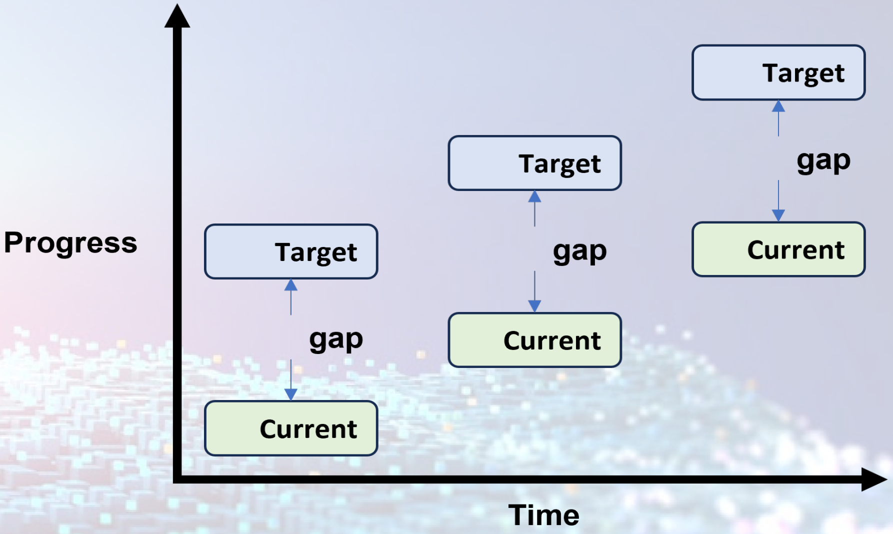
Organizational Profiles can be categorized as:

- A ***Current Profile*** that specifies the CSF outcomes an organization is currently achieving and characterizes how or to what extent each outcome is being achieved.
- A ***Target Profile*** that specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and trends in threat intelligence.

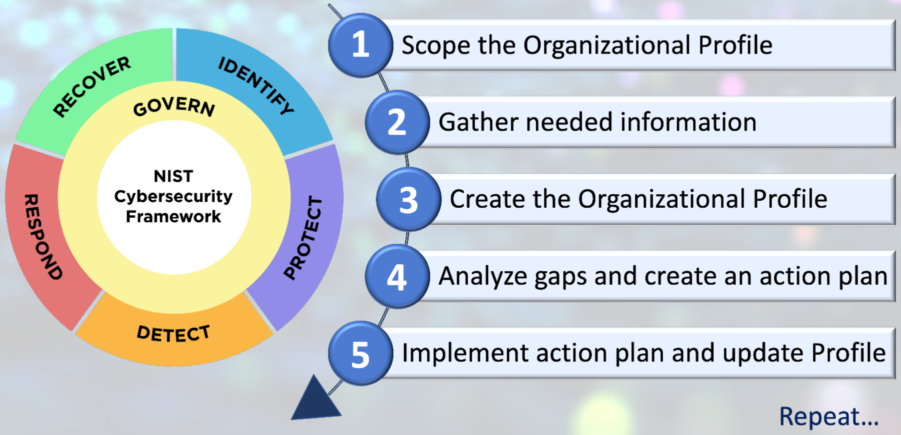
### Create and Use Organizational Profiles with the CSF Five-Step Process

CSF 2.0 describes a five-step process for creating and using Organizational Profiles. More specifically, the process compares an aspirational Target Profile to an assessed Current Profile. Then, a gap analysis is performed, and an action plan is developed and implemented. This process naturally leads to refinements in the Target Profile to be used during the next assessment.

### Drive Progress Over Time



### Create and Use Organizational Profiles



1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. Analyze gaps and create an action plan
5. Implement action plan and update Profile

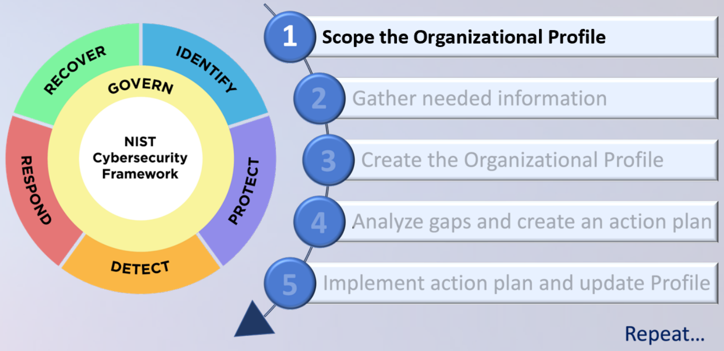
# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## SCOPE THE ORGANIZATIONAL PROFILE

***The scope defines the high-level facts and assumptions on which the Profiles will be based.*** You can have as many Organizational Profiles as desired, each with a different scope. Questions to answer as you scope your Profile include:

- What's the reason for creating the Organizational Profile?
- Will the Profile cover the entire organization? If not, which of the organization's divisions, data assets, technology assets, products and services, and/or partners and suppliers will be included?
- Will the Profile address all types of cybersecurity threats, vulnerabilities, attacks, and defenses? If not, which types will be included?
- Which individuals or teams will be responsible for developing, reviewing, and operationalizing the Profile?
- Who will be responsible for setting expectations for actions to achieve the target outcomes?



1 Scope the Organizational Profile

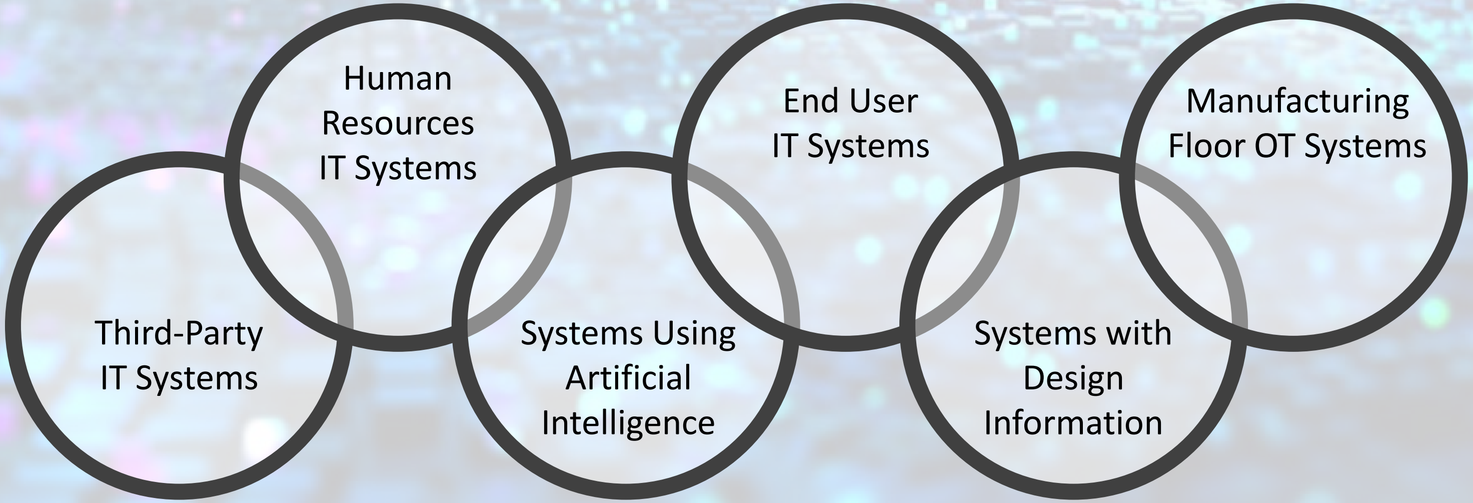
2 Gather needed information

3 Create the Organizational Profile

4 Analyze gaps and create an action plan

5 Implement action plan and update Profile

Repeat…



Human Resources IT Systems

End User IT Systems

Manufacturing Floor OT Systems

Third-Party IT Systems

Systems Using Artificial Intelligence

Systems with Design Information

## Organizational Profile Facts

***Ways to Think about Profiles***

A given organization may wish to use several Profiles.

Each Profile can have a distinct scope based on factors like:

- technology category (IT, OT)
- data types (PII, PHI, PCI)
- users (employees, third-parties)

The scope of a Profile determines the *applicability* of a given CSF outcome.

It may be helpful to combine two or more Profiles when scopes overlap.

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## GATHER NEEDED INFORMATION

***Examples of information may include organizational policies, risk management priorities and resources, cybersecurity requirements and standards...*** The sources of information needed will depend on the use case, the elements that the Profiles will capture, and the level of detail desired. Common sources of information include:

### 1. Community Profiles

A ***Community Profile*** is a baseline of CSF outcomes created and published to address *shared interests and goals among a number of organizations*. A Community Profile is typically intended for a particular sector or subsector, technology, threat type, or other use case.

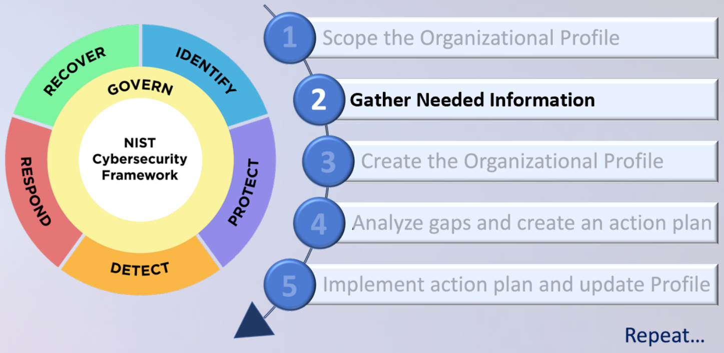
An organization can use a Community Profile as the basis for its own Target Profile by copying the Community Profile into an Organizational Profile. A Community Profile can be adapted by:

- Adjusting the priorities of particular CSF outcomes
- Adding organization-specific Subcategories, Informative References, or implementation guidance

See *A Guide to Creating CSF 2.0 Community Profiles* for more information on creating and using Community Profiles.

### 2. NIST Organizational Profile Template

NIST provides a **CSF Organizational Profile template** as a Microsoft Excel spreadsheet. You can download it and fill it in to create Current and Target Profiles for your organization. The template facilitates side-by-side comparison of Current and Target Profiles to identify and analyze gaps. You can find the template on the CSF 2.0 website.



1 Scope the Organizational Profile
2 **Gather Needed Information**
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement action plan and update Profile

Repeat...

## Prioritization

***The Defining Feature of a Profile***

The central notion of a Target Profile is to determine differing priorities for applicable CSF outcomes. Priorities help you determine parts of your cybersecurity program that should be resourced more, or less. Cybersecurity priorities are driven by strategic objectives, laws, regulations, and risk responses. To learn more, see **SP 800-37** about organization-wide risk management tasks in the *Prepare Step*. **IR 8286B** offers information about how the CSF Core supports risk response decisions.

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## CREATE THE ORGANIZATIONAL PROFILE – PART 1

***Determine what types of supporting information each Profile should include for the selected CSF outcomes...*** Steps for creating an Organizational Profile are:

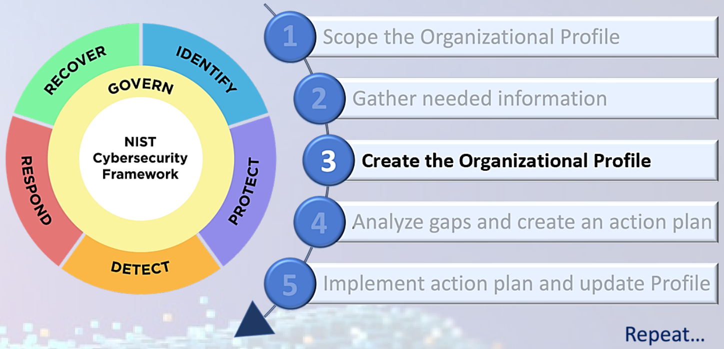
**3a**: Download the latest CSF Organizational Profile template spreadsheet and customize as desired.

**3b**: Include cybersecurity outcomes that apply to your use case, and document rationales as needed.

**3c**: Document current cybersecurity **Practices** in the Current Profile columns. More detailed entries may provide better insights for later steps.

**3d**: Document cybersecurity **Goals** and the plans for achieving them in the Target Profile columns. Entries may be based on CSF Informative References, new cybersecurity requirements, new technologies, and trends in cyber threat intelligence.

**3e**: Note the importance of each Goal using the **Priority** field.



1 Scope the Organizational Profile

2 Gather needed information

**3 Create the Organizational Profile**

4 Analyze gaps and create an action plan

5 Implement action plan and update Profile

Repeat...

| CSF Outcomes | | Current Profile | | | Target Profile | |
|---|---|---|---|---|---|---|
| **Identifier** | **Description** | **Practices** | **Status** | **Rating** | **Priority** | **Goals** |
| The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization's unique risks and requirements. | | Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome. | The current state or condition of an outcome, such as whether it is being achieved and to what degree. | An assessment or evaluation of current practices using scales such as:<br>• high/medium/low<br>• 1-5<br>• 0-100%,<br>• red/yellow/green | The relative importance of an outcome using scales such as:<br>• Low/Medium/High<br>• 1/2/3/4/5<br>• rankings (1, 2, 3…) | Such as:<br>• Policies, Processes, and Procedures<br>• Roles and Responsibilities<br>Selected from:<br>• Informative References - standards, guidance, and best practices |

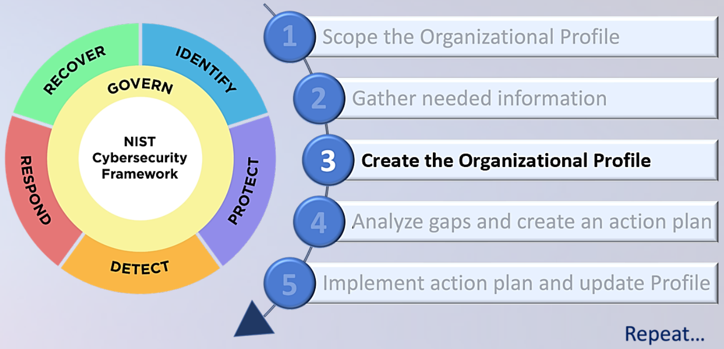
# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## CREATE THE ORGANIZATIONAL PROFILE – PART 2

**The table below shows a notional example of a single row from an Organizational Profile.** This is meant for illustrative purposes only. Here are some tips drawn from the example:

- Add and remove columns from the Organizational Profile template to suite your needs. The CSF encourages users to record whatever information is significant and to use whatever format they prefer.
- The columns do not have to be the same for the Current Profile and the Target Profile.
- Include Informative References to understand differences between Practices and Goals. This example shows SP 800-53 controls in the square brackets.



1 Scope the Organizational Profile

2 Gather needed information

3 **Create the Organizational Profile**

4 Analyze gaps and create an action plan

5 Implement action plan and update Profile

Repeat...

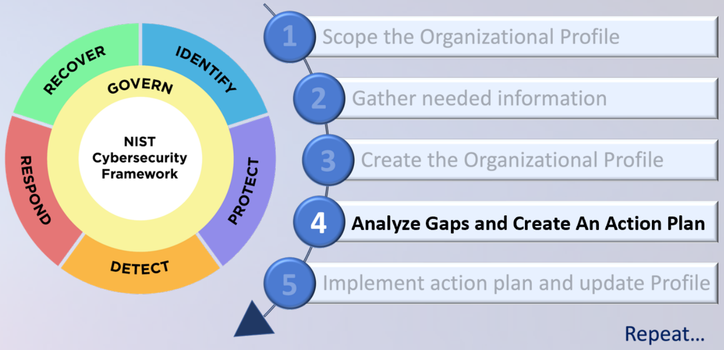
| CSF Outcomes | | Current Profile | | | Target Profile | |
|---|---|---|---|---|---|---|
| **Identifier** | **Description** | **Practices** | **Status** | **Rating** | **Priority** | **Goals** |
| PR.PS-01 | Configuration management practices are established and applied | Policy: Configuration Management policy version 1.4, last updated 10/14/22. Defines the configuration change control policy [**CM-1**].<br>Procedures: System owners and technology managers informally implement configuration management practices. Change control processes are not consistently followed. The CIO specifies configuration baselines [**CM-2**] for the IT platforms and applications most widely used within the organization, but baseline use is not monitored or enforced consistently across the organization. | Configuration management is partially implemented within the organization. Some systems do not follow available baselines and other systems do not have baselines, so they may have weak configurations that make them more susceptible to misuse and compromise. Unauthorized changes may go undetected. Some changes are not tested or tracked. | 3<br>*out of 5* | High | Policy: The Configuration Management policy requires configuration baselines to be specified, used, enforced, and maintained for all commodity technologies used by the organization. The policy requires change control processes to be followed for all technologies within the organization [**CM-1**].<br>Procedures: Each division of the organization has a configuration management plan [**CM-9**], as well as maintains, implements, and enforces configuration baselines [**CM-2**] and settings [**CM-6**] for their systems. Baselines are applied to all systems before production release. All systems are continuously monitored for unexpected configuration changes, and tickets are automatically generated when deviations from baselines occur. Designated parties review change requests and corresponding impact analyses [**CM-4**] and approve or deny each [**CM-3**]. |

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## ANALYZE GAPS AND CREATE AN ACTION PLAN – PART 1

***Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan for addressing those gaps.*** Using Profiles in this manner helps your organization make better-informed decisions about how to improve cybersecurity risk management in a prioritized and cost-effective manner.



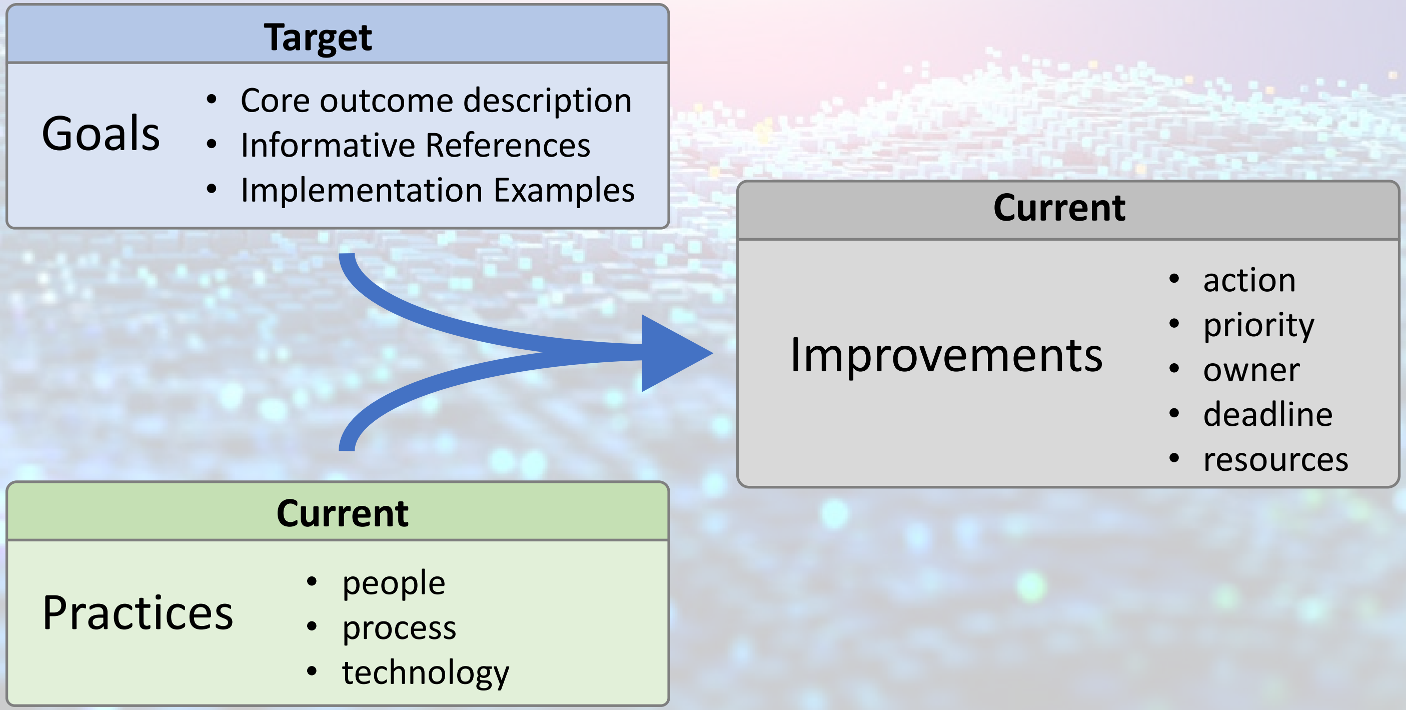
1. Scope the Organizational Profile
2. Gather needed information
3. Create the Organizational Profile
4. **Analyze Gaps and Create An Action Plan**
5. Implement action plan and update Profile

Repeat…

### Step 4a

***How to Analyze Gaps***

Compare and contrast your current **practices**, across people, process, and technology, to the best practices described in CSF outcome descriptions, Informative References, and Implementation Examples. With those **goals** in mind, make observations about differences and document those items as candidate improvements.



**Target**

Goals

- Core outcome description
- Informative References
- Implementation Examples

**Current**

Practices

- people
- process
- technology

**Current**

Improvements

- action
- priority
- owner
- deadline
- resources

### Step 4b

***How to Create Action Plans***

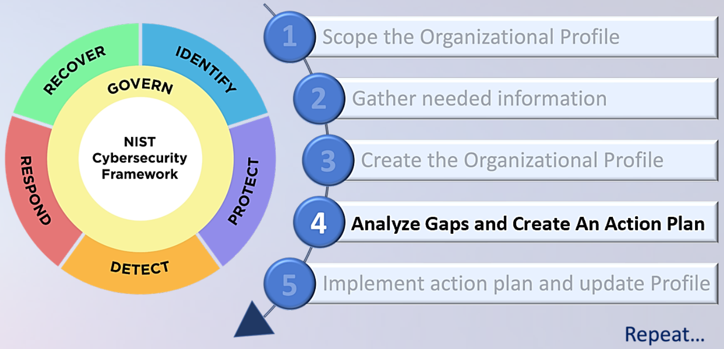
The action plan is a list of pending **improvements** for your cybersecurity program. In addition to the Organizational Profile gap analysis, the action plan should consider mission drivers, benefits, risks, and necessary resources (e.g., staffing, funding). Action plans should have all the essential items in the graphic (left).

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## ANALYZE GAPS AND CREATE AN ACTION PLAN – PART 2

***Identifying and analyzing the differences between the Current and Target Profiles enables an organization to find gaps and develop a prioritized action plan for addressing those gaps.*** The CSF provides links to tools, controls, and implementation resources that will help you with analyzing gaps [**Step 4a**] and creating action plans [**Step 4b**]. A recommended approach for developing action plans is to use the NIST CSF 2.0 Reference Tool to follow the references from your Target Profile's pertinent Subcategories to the associated NIST SP 800-53 controls.



1 Scope the Organizational Profile

2 Gather needed information

3 Create the Organizational Profile

4 **Analyze Gaps and Create An Action Plan**

5 Implement action plan and update Profile

Repeat...

## What Best Practices to Use

***Informative References:*** relationships between the Core and various best practices, including standards, guidelines, regulations, and other resources. References help inform how an organization may achieve the CSF outcomes. They also help connect desired outcomes to other common cybersecurity documents, such as ISO/IEC 27001 and SP 800-53 which provides a catalog of security and privacy controls.

## How to Implement Best Practices

***Implementation Examples:*** notional descriptions of ways CSF outcomes can be fulfilled. The examples are not a comprehensive list of *all* actions that could be taken by an organization, nor are they a *baseline* of required actions; they are helpful ideas to get organizations thinking about concrete steps. The NIST CSF 2.0 Reference Tool allows users to explore the full CSF 2.0 Core and download in Excel and JSON formats.

## Example of an Implementation Example

***An Excerpt from the NIST CSF 2.0 Reference Tool***

Subcategory

**PR.PS-01**: Configuration management practices are applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)

***Implementation Examples***

Ex1: Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality)

Ex2: Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

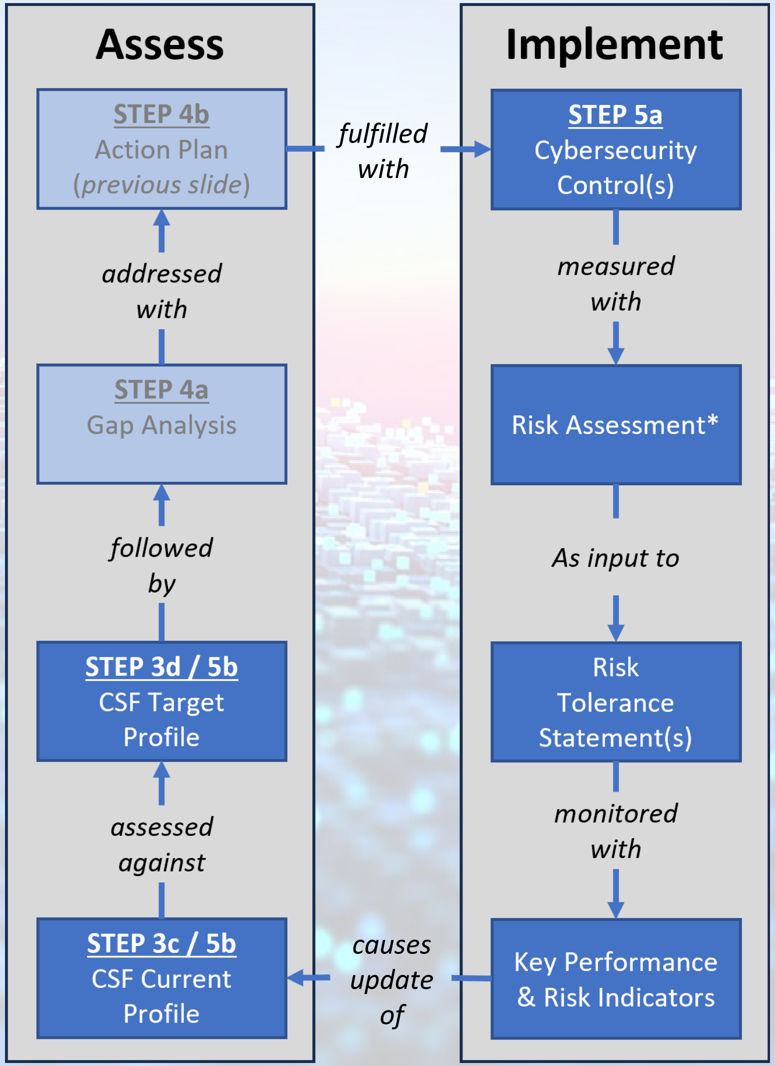
## A QUICK START GUIDE

## IMPLEMENT ACTION PLAN AND UPDATE PROFILE

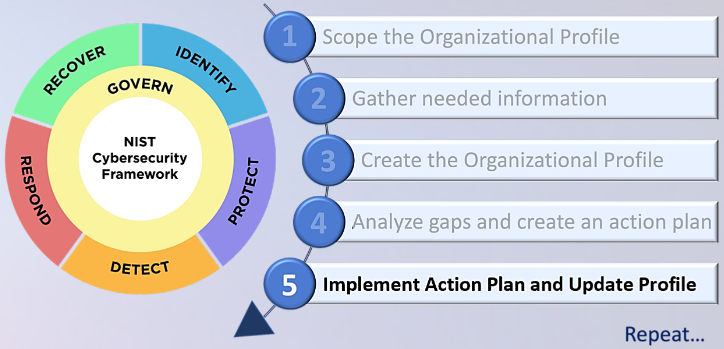
### Step 5a

***Implementing Action Plans***

The Action Plan is fulfilled through any combination of management, programmatic, and technical controls. As those controls are implemented, the Organizational Profile can be used to track implementation status. Subsequently, controls and associated risks can be monitored through Key Performance Indicators (KPI) and Key Risk Indicators (KRI). Cyber risks that fall beyond Risk Tolerance are observed through Risk Assessments. Risks beyond Risk Tolerance may prompt updates to the Action Plan, Organizational Profile, and/or Risk Tolerance statements. Gap Analysis may also result in the creation of POA&M for gaps that will take a longer remediation timeline. More information about KPI, KRI, Risk Tolerance, and POA&Ms can be discovered in IR 8286B and SP 800-37.



* Risk Assessment can occur at any time and can inform any step


RECOVER
IDENTIFY
GOVERN
NIST Cybersecurity Framework
PROTECT
RESPOND
DETECT
1 Scope the Organizational Profile
2 Gather needed information
3 Create the Organizational Profile
4 Analyze gaps and create an action plan
5 Implement Action Plan and Update Profile
Repeat…

### Step 5b

***Updating Your Profile***

**Implement** activities that follow your Action Plan are a part of an ongoing cyber risk management program (feedback loops and lines of communication more nuanced than shown). Risk Assessments, as described in SP 800-30 can leverage Risk Tolerance statements when identifying risks, as well as determining likelihood and impact of those risks. The changing likelihood and impact are a measure of the effectiveness of the Action Plan and the discrete controls. Risk monitoring is also performed using KPI and KRI. Changes in risks, likelihoods, and/or impacts may all result in updates to the Organizational Profile.

# NIST CSF 2.0: CREATING AND USING ORGANIZATIONAL PROFILES

## A QUICK START GUIDE

## NEXT STEPS

## What We Learned.

This QSG explained the following terms:

**Organizational Profile** – CSF Core outcomes relevant for a specific organization

**Community Profile** – CSF Core outcomes that apply to multiple organizations

**Current Profile** – the cybersecurity outcomes that an organization is currently achieving

**Target Profile** – the desired outcomes an organization wants to achieve

**Gap Analysis** – determining the differences between the Current and Target Profiles

**Informative References** – best practices that implement various CSF Core outcomes

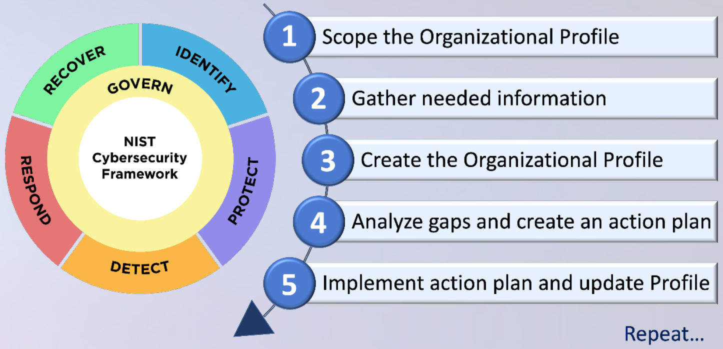
**Implementation Examples** – notional ways organizations can achieve CSF Subcategories

**Action Plan** – address gaps and move toward the Target Profile

## What's Next.

Here's a list of things you can do to move this QSG into practice:

- Familiarize yourself with the NIST CSF Organizational Profile template
- See if there is a Community Profile relevant for you at the NIST Community Profiles site
- Determine how many CSF Organizational Profiles you need [**Step 1**]
- Inventory your cybersecurity requirements
- Prioritize CSF outcomes in your Organizational Profiles [**Step 2**]
- Assess your Current Profile [**Step 3**]
- Read more about Informative References
- Improve your cybersecurity program over time [**Steps 4 & 5**]



1 Scope the Organizational Profile

2 Gather needed information

3 Create the Organizational Profile

4 Analyze gaps and create an action plan

5 Implement action plan and update Profile

Repeat…

## Learning More

### *Reading*

| | |
|---|---|
| IR 8286B | NIST IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management* |
| SP 800-37 | NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems & Organizations* |
| SP 800-53 | NIST SP 800-53 Revision 5, *Security  and Privacy Controls for Information Systems & Organizations* |
| SP 800-30 | NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* |

### *Resources*

Organizational Profile Template

NIST CSF 2.0 Reference Tool

Informative References

Implementation Examples

*A Guide to Creating CSF 2.0 Community Profiles*

*Quick-Start Guide for Using the CSF Tiers*