NIST AI RMF Profile Template

Executive Summary

- In no more than a couple pages, describe the essential points a reader should come away with.
- If the profile is intended for multiple groups, consider dividing the executive summary into sections catered to each group.

Background

- Describe the objective of the profile, defining what successful risk management or profile implementation looks like.
- Scope the profile. Include the system description, key capabilities, and expected use conditions. Consider clarifying what content is out of scope as well.
- Clarify whether the profile is a "current" or "target" profile. Current profiles reflect the current risk state of the system and active mitigation approaches. Target profiles are the long-range goals and full lifecycle of risk management. They represent the risk management processes that should ideally be implemented.[1]
- Remember to incorporate definitions and background material so that a casual reader can understand the profile.

Intended Audience

- Who should read the profile? For whom is the profile not relevant?
- Clarify how the primary audience will shift throughout the document and change both as the profile matures and as the AI system's lifecycle stage changes.

[1] The National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Washington, D.C.: Department of Commerce, 2023), 33, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

AI System Management and Schedule

- State and describe all stakeholders that are not a decision-making authority, including their responsibilities.
    - If appropriate, clarify intended users of the system and their expectations.
    - Consider stakeholders that are not users or directly part of the AI lifecycle – for example, those indirectly affected by the AI system.
- Clarify who has the decision-making authority to:
    - Sign off on tasks; and
    - Accept risk or a risk mitigation approach.
- Map out the lifecycle stages of the AI system, emphasizing:
    - Decision points at each lifecycle stage;
    - Decision authority and accountability at each decision point;
    - Resources at each lifecycle stage, including:
        - Workforce needs, including any special skill sets
        - Compute
        - Hardware
        - Test harnesses
        - Access to high-demand or rare resources;
    - Entrance and exit criteria at each decision point; and
    - Outputs and documentation at each decision point.

Prioritization of Subcategories

- Recognize that emphasis on lifecycle stages and authority will change for different AI RMF subcategories, and consider using visual cues or a table to indicate this.
- Consider prioritizing subcategories of the AI RMF for different combinations of
    - Audiences
    - AI lifecycle stages
    - Mission objectives
    - Risk tolerances
    - Domains
    - Business drivers

    - Manufacturer priorities
    - Security environments
- Prioritization can be a binary classification of whether a subcategory is relevant or not, or it can provide a more nuanced view of how a subcategory can assist with an objective (for example, by using grades of low, medium, or high relevance). See Table 1 for an example.
- Elaborate on subcategories when possible – for example, by describing the challenges that readers might encounter when implementing a subcategory or clarifying which requirements or needs for a subcategory are immutable and which are not.

Table 1: Example Prioritization of Subcategories for a System Operator

Subcategory	Stakeholder	AI System Lifecycle Stage(s)	Priority
Measure 2.2: Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	System Operator	Design, Evaluation	Low
Measure 2.3: AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.	System Operator	Evaluation, Deployment	Medium

Measure 2.4: The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.	System Operator	Deployment, Monitoring	High

For a given stakeholder and AI system lifecycle stage, the priority of different subcategories may change. Table 1 depicts what the prioritization of subcategories might be for a system operator. Other factors, like mission objectives or risk tolerances, can also affect the prioritization of subcategories.

Source of Measure subcategories: The National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0).[2] The stakeholder, lifecycle stage, and priority for each subcategory are not taken from the NIST AI RMF and were created by CSET for this example.

Use Cases

- A use case is an example implementation of the profile for a given actor(s) and AI system(s).
- Ensure use cases articulate how an actor, or multiple actors, could use the profile to achieve their objectives with an AI system.
- Include a justification for why the use cases were selected. Are they common, and therefore relevant to many people? Are they less common but may present large scale, imminent risks?

[2] The National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (Washington, D.C.: Department of Commerce, 2023), 29, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

Next Steps

- Outline plans to test the profile with users to determine whether changes need to be made.
- Establish a cadence for periodic updates or guidance on when testing results trigger an update to the profile.

When writing the profile, make sure to reference documents from other communities, highlighting synergies between your profile and other resources when feasible. Supplementary resources include references for term definitions and derivations of metrics, reference architectures for the AI system, descriptions of the end-needs and operational conditions of the system, and datasheets and model cards.