Software Requirements Specification

for

AI Cybersecurity Risk Management Framework Tool

Version 1.5

Prepared by Ripken Stork, Jonathan Ly, Colson Swope, and Slate Colebank

Senior Project 2024-2025 NUWC Division Keyport

11/5/2024

Table of Contents

Revision History

Name	Date	Reason For Changes	Version
Colson Swope, Ripken Stork, Jonathan Ly, Slate Colebank	11/12/2024	Adding more detail to numerous sections, according to feedback from the course instructor (Blake Pedrini)	1.1
Colson Swope, Ripken Stork,	11/22/2024	Specified what types of “data” will be collected and ensuring it is reflected across the	1.2

Jonathan Ly, Slate Colebank		entire document, more information was needed regarding the AI model, as well as security and maintenance with the AI model. Revised performance requirements.	
Colson Swope, Ripken Stork, Jonathan Ly, Slate Colebank	12/9/2024	Changed language in 2.4 to avoid legal implications.	1.3
Colson Swope, Ripken Stork, Jonathan Ly, Slate Colebank	02/07/2025	Added a new section which addresses the risk of a Cyber Range outage.	1.4
Colson Swope, Ripken Stork, Jonathan Ly, Slate Colebank	05/07/2025	Changed system target from Debian 11 to Debian 12	1.5

1. Introduction

1.1 Purpose

This SRS covers the scope of the entire product. The purpose of the Artificial Intelligence (AI) Risk Management Framework (RMF) tool serves to assist human Cyber Security analysts with the RMF processes applied to system updates and patch management. Information will be collected from end-user machines, and sent to an AI model system. This model will process the information and output a document containing a high-level summary of the results, a list of systems included, prioritized list of updates that must be installed for each machine, a generated response of how existing infrastructure is compliant with NIST SP 800-40 Rev. 4, and key recommendations based on NIST SP 800-40 Rev. 4.

1.2 Intended Audience and Reading Suggestions

This document is targeted towards executives, Board of Directors (BoD), and information technology (IT) Specialists. For executives and BoD this is informative for them to understand the reason why this is being implemented. As for IT Specialists this shows the implications of the Artificial Intelligence (AI) tool/model. As this tool will be following the National Institute of Standard and Technology (NIST) both parties will be informed on the policies/standards which will be used.

1.3 Product Scope

The Cybersecurity AI RMF tool serves the purpose of assisting a human cybersecurity analyst through a simplified and expedited RMF process. The targeted domain of the RMF process is patch management planning for enterprises (NIST SP 800-40r4). Update and patching information will be passively sent from client computers to a central machine running an AI model. The AI model will take this information, and process it into a report in accordance with NIST SP 800-40r4. The goal of this report is to be a source

that can be used for the organization to justify that they are capable of maintaining security over the client patching / update data that is being handled, by remaining compliant with the patch management RMF framework.

1.4 References

1. **NIST Special Publication (SP) 800-53 Rev. 5:** Provides a comprehensive catalog of security and privacy controls for information systems and organizations[1].
2. **NIST Cybersecurity Framework (CSF):** Offers guidelines for managing and reducing cybersecurity risks[2].
3. **NIST Special Publication (SP) 800-30 Rev. 1:** Guide for conducting risk assessments, including the identification of threats and vulnerabilities[3].
4. **NIST Special Publication (SP) 800-37 Rev. 2:** Guidelines for applying the Risk Management Framework (RMF) to information systems[3].
5. **NIST Special Publication (SP) 800-40 Rev. 4:** Guidelines for Enterprise Patch Management Planning
6. **ENISA Guidelines:** European Union Agency for Cybersecurity provides comprehensive guidelines on AI risk management and cybersecurity[4].

2. Overall Description

2.1 Product Perspective

The AI RMF tool is a self-contained application that functions independently. It is designed to compile software version information from a set of machines, then determine the system's NIST compliance with patch management. It suggests software version changes to bring the machine into NIST compliance.

2.2 Product Functions

- **Data collection on installed software versions:**
  Target systems will provide access to software version information, which will be compiled by the tool.
- **Data analysis by way of AI model:**
  The AI model determines which system updates / upgrades shall be done in order to bring the system within NIST compliance.

2.3 Operating Environment

The AI software will operate on the current version of Debian 12. We will be collecting information from three virtual machines on the Western Washington University cyber range running both Windows and Debian-based Linux operating systems. A separate machine on the cyber range will run the AI model. Data will be transferred over the network, meaning that the user must first run all machines, including the host, on the same network.

2.4 Design and Implementation Constraints

- The program will handle client patching / update data from both Windows and Debian-based Linux operating systems.
- The AI tool will follow NIST and ENISA regulatory policies.
- The client will be responsible for maintaining the delivered software.
- Once this update data has been compiled, the AI model will produce a correct report within 1 minute.
- Downloading completed reports will take no more than 10 seconds.

2.5 User Documentation

1.Project Wiki Page (Cyber Range GitLab)

1.1 Cyber Range VPN access required
1.2 Email Paul Haithcock (haithcp@wwu.edu) if VPN access to the Cyber Range is needed
1.3 Must log into the general Cyber Range GitLab page first
1.4 Once logged in, email Sally Bass (basss@wwu.edu) for access to the AI Cybersecurity RMF Tool
1.5 Access Wiki here:
https://gitlab.cyberrangepoulsbo.com/nuwc-k-navy-projects/2025-ai-cybersecurity-rmf-tool

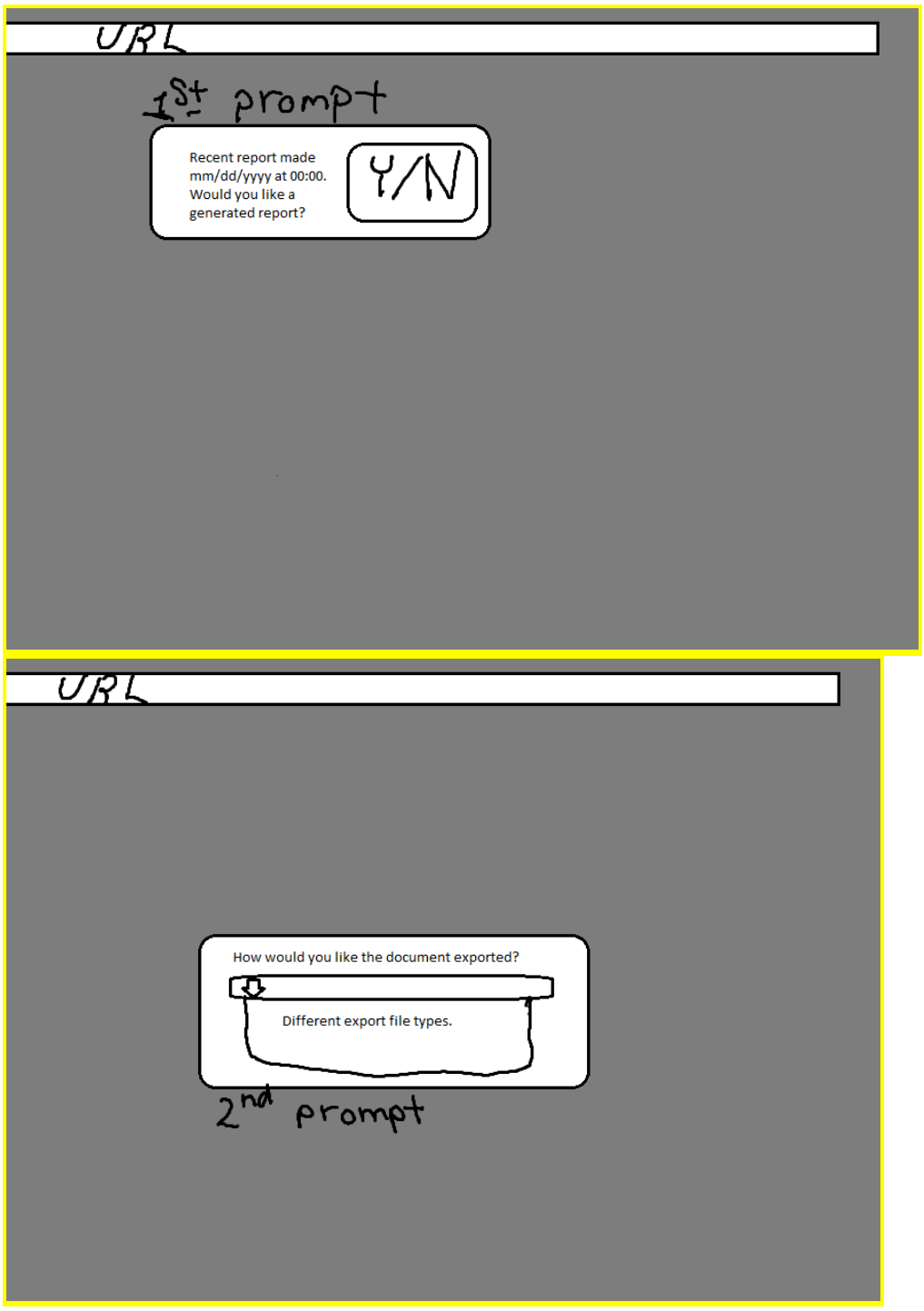
2.6 Assumptions and Dependencies

We are going to assume that the WWU Cyber Range is up and running as the software is held on the Cyber Range. We are also going to assume that the script of collecting information from the machine receives good information from an interval of (12 hours currently.) This information will be stored/logged somewhere safe and secure. Once you want the RMF report it is expected that the information will be securely and efficiently transported into the AI model to generate the RMF report.

3. External Interface Requirements

3.1 User Interfaces

The GUI will essentially be a dashboard. There will be a button to request an RMF, and another button to export results to PDF, DOCX, etc. There will be a place to see the last time the information was requested from the machines.



3.2 Software Interfaces

- **Program Operating System: Debian 12**
  The program will run on the current version of Debian 12.
- **Target Operating Systems: Debian 12, Windows 11**
  The program will be capable of assessing client patching / update data from both Debian 12 and Windows 11 machines.

- **AI Model**
  AI API key:
  OpenAI, Gemini, Hugging Face, Ollama, Claude

Client patching / update data will be collected from target systems, and compiled on the host machine. After compilation, the AI model will be fed the compiled data. Once trained, the AI model will analyze the provided data and output a report detailing the systems' NIST compliance levels. The web GUI will handle control over the program, allowing for the user to start report generation and download reports. Reports will be output in .pdf format to the host system.

3.3 Communications Interfaces

The web GUI will be compatible with Chromium and Firefox browsers.

Chromium versions (Stable):
- Versions 119.0.6045.134 and later

Firefox versions (Official Releases):
- Versions 119.0 and later

4. System Features

4.1 AI Model Trained on NIST Data

4.1.1 Description and Priority

An AI model trained using NIST data, notably NIST 800-40 Rev. 4. It is capable of determining whether or not a system is in compliance.

Priority: High

4.1.2 Stimulus/Response Sequences

Stimulus: User initiated report creation
Response: Generate a report using the NIST 800-40 Rev. 4 and provide it to the user. Use the most recent software version dataset.

4.1.3 Functional Requirements

REQ-1: Processing formatted software version data.

REQ-2: Evaluate software version data in relation to the NIST requirements.

REQ-3: Provide suggestions to the user based on software version data.

REQ-4: Provide suggestions to the dashboard.

4.2 WEB GUI

4.2.1 Description and Priority

A dashboard GUI running in a browser that allows the user to easily manage the generation of reports and displays information about the client patching / update data collected.

Priority: Medium

4.2.2 Stimulus/Response Sequences

Stimulus: Request to generate report
Response: Output the report to the dashboard

Stimulus: Request to download report
Response: Download the formatted report to the system

Stimulus: New report created
Response: Update the report history panel

4.2.3 Functional Requirements

REQ-1: Allow for responsive use of GUI.

REQ-2: Create reports using a button in the GUI.

4.3 Scalability

4.3.1 Description and Priority

The ability to process a surplus of information and handle all the new device's client patching / update data being collected.

Priority: Medium

4.3.2 Stimulus/Response Sequences

Stimulus: Requesting more devices to checked
Response: Allows/Handles more information.

4.3.3 Functional Requirements

REQ-1: Allows for scalability to more devices by continuously collecting information as computers are added or removed from the network.

REQ-2: The program can handle a maximum of 10 devices.

REQ-3: The AI model shall be able to process information from new systems.

4.4 Compile update data in proper RMF layout/Format

4.4.1 Description and Priority

Internal data collection on software patch versions.

Priority: High

4.4.2 Stimulus/Response Sequences

Stimulus: Data collection requested.
Response: Scan systems and compile client patching / update data to be sent to the AI model.

Stimulus: New system added.
Response: Upon next scan, add the new system to the set of current systems.

4.4.3 Functional Requirements

REQ-1: Compile software version information.

REQ-2: Create reports using a button

4.5 Result exports

4.5.1 Description and Priority

Internal functionality to compile the report created by the AI model and export it as a formatted document.

Priority: Medium

4.5.2 Stimulus/Response Sequences

Stimulus: GUI requests report export.
Response: Download report to user machine.

4.5.3 Functional Requirements

REQ-1: Create formatted exportable report as .docx.

REQ-2: Download the report to the user's machine.

4.6 AI model security

4.6.1 Description and Priority

Make sure that the AI model isn't susceptible to attack such as reverse prompt engineering and making sure that the Information that the AI model generates is secure. The AI model shall be restricted to only send information on RMF procedures.

Priority: High

4.6.2 Stimulus/Response Sequences

Stimulus: Request RMF information.
Response: Accurate and secure RMF information.

4.6.3 Functional Requirements

REQ-1: Restricted the output of the AI model to only RMF information.

REQ-2: Make sure that the client patching / update data sent and received is safe.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The program will be run on the WWU Cyber Range, meaning that performance will depend on the usage of the range during execution.

- Data collection related to updates and patching shall take no more than 5 minutes per client machine.
- The website interface shall take no more than 30 seconds to open.
- Collected patching and update data shall take no more than 5 minutes to compile into the appropriate NIST format.
- Once patching / update data has been compiled, the AI model will produce a correct report within 2 minutes.
- Downloading completed reports shall take no more than 1 minute.

5.2 Safety Requirements

The output of the AI model shall be strictly controlled to only output necessary update information. This will prevent any unwanted output of data not applicable to update information according to the NIST SP 800-40r4. If update information were to be leaked, possible reputation loss among clients may occur. This information shall remain internal to the program.

5.3 Security Requirements

As this is an AI tool, it will need to collect client patching / update related data to operate properly. Therefore conversation about acquisition of data from another company or current company is top priority and will need to happen first. As this data can contain personal or proprietary information this data will be kept secure and isolated from other users to null the possible chance of data leakage. One way we will protect data is to use input sanitization in order to make sure that we can not reverse engineer the prompt in order to get information. Another way that we will protect that data is to make sure the AI model is in a secure environment to prevent unauthorized access (the WWU Cyber Range). Then, we will also make sure to use secure authentication methods like using ENV variables to hide API keys within code. Lastly, we will use TLS (Transport Layer Security) to encrypt data transmitted from the VM's to our processing system.

5.4 Software Quality Attributes

Accuracy: The model shall report an accurate analysis of the provided client patching / update data. The analysis shall be in line with the NIST standards that are provided to the model.
Security: The program shall not scan any information about the systems that have not been authorized. It shall store only information regarding software versions.
Usability: The interface shall be easy to use and self explanatory. The GUI shall be responsive.
Maintainability: The program shall include robust error checking and error reporting to the user.

6. Other Requirements

6.1 Maintenance Requirements

AI Model: The AI model will be updated with the API key that is being used.
The OS Running the Model: Automated operating system updates via. CRON job.

7. Risks

7.1 Cyber Range Platform Outage

If the Cyber Range platform is down, there is no current way to access the AI RMF tool. This includes the running product, as well as the development tools for this AI RMF model, including the GitLab repository containing the files associated with this model, as well as the OpenStack Horizon platform. Therefore, if an issue arises, there is potential for some / all of these tools to become unavailable for extended periods of time.

Appendix A: Glossary

RMF: Risk Management Framework
NIST: National Institute of Standards and Technology
ENISA: European Union Agency for Cybersecurity
Link to AI RMF Gantt Chart:
https://docs.google.com/spreadsheets/d/1WSECMaxXFPmFkuYqpYUdb19p6ivmP1hI/edit?usp=sharing&ouid=114767040186885259492&rtpof=true&sd=true

Appendix B: To Be Determined List

Document Conventions
Other Requirements