



BUDT748

Self-assessment CMMC Level 2 Tool Project Report

Hive Systems



1. Introduction and Context

System Overview

The system developed by Hive Systems is a self-assessment tool designed to simplify the complex landscape of cybersecurity compliance. Its **core functionality** revolves around enabling companies to evaluate their adherence to various standards and frameworks intuitively and efficiently. **Key features** of the system include dynamic questionnaire generation, real-time progress tracking, automated scoring, and PDF export for comprehensive reporting.

The **problem** this tool addresses is the intricacy of compliance requirements, which many organizations, especially smaller ones, find overwhelming. Traditional methods, such as manual evaluations via spreadsheets, are error-prone and inefficient. This tool streamlines the compliance assessment process, reduces the burden of manual data handling, and ensures consistency in evaluations.

The **stakeholders** for the tool include:

- Internal teams at Hive Systems would be involved in developing, maintaining, and improving the system, minimizing the workload, particularly the manual effort involved in the compliance assessment process, by automating tasks and simplifying the workflow.
- Prospective and existing clients of Hive Systems, ranging from small businesses to enterprises.
- Non-profit organizations benefiting from pro bono services through Hive Systems' "Hive Helps" program.

Purpose

The self-assessment tool was created to address the following **client needs** and **goals**:

- Simplification: To make cybersecurity compliance more approachable and manageable for organizations with limited technical expertise or resources.
- Efficiency: To eliminate the inefficiencies of manual processes by automating data collection, validation, and scoring.
- Affordability: To offer a cost-effective solution that reduces reliance on external consultants for basic compliance evaluations.

The **expected outcomes** of the system include:

1. **Improved Accuracy:** Automated scoring and validation reduce errors in compliance assessments.
2. **Enhanced User Experience:** Intuitive navigation, real-time feedback, and simplified reporting improve accessibility for users of varying expertise levels.
3. **Greater Accessibility:** Pro bono access through Hive Helps ensures that resource-constrained organizations can still meet compliance requirements.
4. **Scalability:** The system's modular design ensures adaptability to evolving compliance standards and client needs, with future enhancements such as AI-driven assistance and database integration on the roadmap.

This tool exemplifies Hive Systems' mission of making cybersecurity approachable, empowering businesses to focus on growth while maintaining robust compliance.

2. The Development Process

Research

Interviews and Meetings: The primary research method involved interviews with the client, gathering insights about their existing Excel-based tool and clarifying requirements. This method facilitated effective communication, timely feedback, and fact-checking. The client also shared reference materials like the DoD scoring methodology and relevant controls, which enhanced the team's understanding of the system's context and user limitations.

Brainstorming: Team brainstorming sessions and online research were conducted to explore ideas for improving the Excel tool. These discussions helped identify client pain points and generated solutions to enhance user experience and system functionality.

Workflow Analysis: The team analyzed workflows associated with the Excel tool, focusing on data inputs, processing, and outputs. This method identified inefficiencies and areas for automation, which informed the logic for designing a solution to improve data quality, reduce errors, and streamline processes.

Design Summary

- The Excel tool comprises 14 unique controls and over 100 criteria questions. These controls are categorized into three buckets: **Base**, for standard scoring logic; **Special**, for controls with unique scoring conditions; and **POA&M**, for controls that can be edited within 180 days post-compliance test. This categorization streamlines the scoring process and ensures clarity in handling different control types.
- **Categorization of Controls:**
 - **Base Bucket:** Includes controls with standard scoring logic.
 - **Special Bucket:** Contains controls requiring unique scoring conditions.
 - **POA&M Bucket:** Covers controls editable within 180 days of completing the compliance test.
- **Example Control Scenarios:**
 - **Base Control Logic:**
 - Subtract score if any sub-control is 'NOT MET.'
 - **Remote Access Not Permitted (Special):**
 - Otherwise, subtract score only if all sub-controls are 'NOT MET.'
 - **Absence of SSP (Special):**
 - Deduct 110 points if control is 'NOT MET.'
 - Continue if 'MET' or 'NOT APPLICABLE.'

UI/UX Design Mockup

For the UI/UX, the client provided specific requirements for the overview page, dropdown buttons, and question placements. Key aspects included as below:

Overview of the page:

AC.L1-3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)^①

MET

Assessment Criteria 1: Authorized users are identified

Assessment Criteria 2: Processes acting on behalf of authorized users are identified

Assessment Criteria 3: Devices (and other systems) authorized to connect to the system are identified

Assessment Criteria 4: System access is limited to authorized users

Assessment Criteria 5: System access is limited to processes acting on behalf of authorized users

Assessment Criteria 6: System access is limited to authorized devices (including other systems)



Drop Down List:

AC.L1-3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)^①

MET

Assessment Criteria 1: Authorized users are identified

Assessment Criteria 2: Processes acting on behalf of authorized users

Drop-down for each assessment criteria that allows selection of met, not met, or not applicable

connect to the system are identified

Assessment Criteria 4: System access is limited to authorized users

Assessment Criteria 5: System access is limited to processes acting on behalf of authorized users

Assessment Criteria 6: System access is limited to authorized devices (including other systems)



While implementing these, **adjustments** were made to prioritize functionality and user experience. In maximizing the retention of the client's core requirements, we ensured the tool effectively met its primary purpose of facilitating accurate and efficient compliance assessments.

CRUD Matrix

CRUD models showing when data can be created, read, updated or/and deleted for each entity during every process in the system through the whole research process.

Entity Attributes	Record Client Data	Generate Password	Email Delivery Password	Assessment Logic	Finding Criteria	Evaluate Test Results	Access Controls System	Score Deductions	Calculate Score	Generate Reports
Client	C		RD							
ClientID	C		RD							
Name	C		RD							
Email	C		RD							
Password		C	R							
Assessment		CR								
AssessmentID		CR								
AuditID		CR								
TypeID		CR		U		U				
Score		C								
Control			CR	CR		CR				
ControlID			CR	CR		CR				
ControlName			CR	CR		CR				
Description			CR	CR		CR				
ControType			CR	CR		CR				
TypeID			CR	CR		CR				
ControlID			CR	CR		CR				
TypeName			CR	CR		CR				
Description			CR	CR		CR				
Question			CR	CR		CR				
QuestionID			CR	CR		CR				
TypeID			CR	CR		CR				
QuestionText			CRU	CRU		CRU				
Audit			CRU	C	RU		C	U	R	
AuditID		CR	R		R					R
TimeStamp			CRU	C	RU		C	U		R
Status			CRU	C	RU		C	U		R
TotalScore			CRU	CRU	RU		CRU	U		R

Development

Pseudo code for each specific control:

Initialize page_scores as an empty dictionary
Initialize cumulative_score to 0

For each page in user_input:

Initialize page_score to 0

For each control_id in the page's control data:

 Get control_score for the control_id

 Get sub_control_results (list of results) for the control_id

 If control_id is 'IA.L2-3.5.3':

 If sub_control_results are ['MET', 'MET', 'MET', 'NOT MET']:

 Subtract 3 from page_score

 Else if any sub-control result is 'NOT MET':

 Subtract 5 from page_score

 Else if control_id is 'CA.L2-3.12.4':

 If any sub-control result is 'NOT MET':

 Subtract 110 from page_score

 Else if control_id is 'SC.L2-3.13.11':

 If all sub-control results are 'NOT MET':

 Subtract 5 from page_score

 Else if sub_control_results are ['NOT MET', 'MET']:

 Subtract 5 from page_score

 Else if sub_control_results are ['MET', 'NOT MET']:

 Subtract 3 from page_score

 Else: **# Generic case for other controls**

 If any sub-control result is 'NOT MET':

 Subtract control_score from page_score

Return page_scores and cumulative_score

Testing

Extensively tested the seamless integration between front-end and back-end components to ensure robust system functionality. Rigorously validated the compliance logic against a diverse range of complex and unique use cases, ensuring accuracy and alignment with user requirements and industry standards.

Challenges and Solutions

A key challenge was ensuring the compliance logic accurately addressed diverse and complex use cases while adhering to strict requirements prohibiting any storage of user data in a database or elsewhere. This constraint added complexity to the system design and testing processes, requiring innovative solutions to maintain functionality without data persistence.

The solution to address this challenge was to temporarily store user inputs within the session, allowing the user to answer all 100 questions without persisting data beyond the session. This approach ensured compliance with the requirement to avoid data storage while maintaining functionality and user experience during the assessment process.

3. System Functionality

Our system is a CMMC Level 2 Self-Assessment Tool designed to guide organizations through compliance assessments in a user-friendly and structured manner. It consists of two primary components: Frontend and Backend, which work together seamlessly to ensure an intuitive user experience and accurate assessment scoring. Below is a detailed explanation of the system's core features, frontend-backend interaction, and backend processes.

Frontend Processes

The frontend, built with JavaScript, is designed to dynamically load content and manage user interactions seamlessly. The system utilizes a structured `controlFamilies` array, which categorizes the controls by their respective families. The `loadPageContent` function renders these controls and their criteria dynamically onto the page, ensuring that the assessment interface remains flexible and scalable as new controls are added.

User interaction is facilitated through intuitive features like dropdown selections. Each criterion is paired with a dropdown menu, allowing users to select their responses (MET, NOT MET, NOT APPLICABLE). These responses are tracked in a `responses` object, which maintains the state of user inputs. To ensure completeness, the system validates responses using the `areAllCriteriaSelected` function, which ensures that all dropdowns on a page are filled before the user can proceed to the next section.

Progress tracking and navigation are implemented to enhance user experience. A progress bar, updated via the `updateProgressBar` function, visually reflects the user's progress through the control families. Navigation buttons (NEXT, PREVIOUS) are dynamically enabled or disabled depending on the user's current position in the assessment, managed by the `updateButtons` function.

The system handles submission and PDF generation efficiently. When the user completes the assessment, the `submitResponses` function consolidates and sends all responses to the backend for scoring and analysis. For the final assessment report, the `downloadPageAsPDF` function captures the summary page using `html2canvas` and generates a well-structured, paginated PDF using `jspdf`, ensuring that users can download a professional summary of their results. These processes work together to create a smooth and intuitive assessment experience.

Frontend-Backend Interaction

The frontend communicates with the backend through HTTP POST requests, ensuring a seamless flow of user responses and score calculations. This interaction begins with the submission of page data. When a user completes a page, the `sendPageResponses` function gathers the user's responses using the `constructPageData` function. This data is then sent to the backend API endpoint (`/calculate`), which processes the responses and returns the calculated score for that specific page.

Upon receiving the backend's response, the frontend updates the cumulative score and determines whether to proceed to the next control family. This dynamic interaction ensures that the scoring is both immediate and accurate, providing users with real-time feedback on their progress.

Once all pages are completed, the frontend consolidates the entire assessment data and submits it to the backend for final analysis. The backend processes the data, calculates the final cumulative score, and identifies areas requiring improvement. This final response is displayed to the user in a detailed summary, ensuring transparency and actionable insights into their assessment performance.

Sample Data being sent from frontend to backend in JSON format is below:

```
{  
  
  "AC.L1-3.1.1": { "sub_control_results": ["MET", "MET", "MET", "NOT MET", "NOT  
MET", "MET"]},  
  
  "AC.L1-3.1.2": {"sub_control_results": ["MET", "MET"]},  
  
  "AC.L1-3.1.20": {"sub_control_results": ["NOT MET", "MET", "MET", "MET", "NOT  
MET", "MET"]},  
  
  "AC.L1-3.1.22": {  
  
    "sub_control_results": ["MET", "MET", "MET", "NOT MET", "MET"]},  
  
  "AC.L2-3.1.3": {"sub_control_results": ["MET", "MET", "NOT MET", "MET", "MET"]}}
```

The JSON data structure includes keys that represent the control IDs, such as AC.L1-3.1.1 and AC.L1-3.1.2, corresponding to specific controls within the assessment. Each control contains a field named `sub_control_results`, which is an array holding the user's responses to individual criteria under that control. The responses can have three possible values: "MET", indicating that the criterion is satisfied; "NOT MET", indicating that the criterion is not satisfied; and "NOT APPLICABLE", indicating that the criterion is not applicable in the context. This structured format enables the backend to process each control independently, calculate scores based on the provided responses, and generate detailed feedback for the user.

Backend Processes

The backend, built using Python and the Flask framework, is responsible for processing the assessment data and calculating scores based on predefined control criteria. When the frontend submits user responses for a control family, the backend receives the JSON data at the `/calculate` endpoint. This data undergoes validation to ensure that all necessary information is present and in the correct format.

The scoring process is guided by a predefined `control_scores` dictionary that assigns a score to each control. The `calculate_total_score` function evaluates the user responses for each control. For responses marked as "NOT MET," the assigned score for that control is

deducted. Certain controls, such as IA.L2-3.5.3 and CA.L2-3.12.4, have special scoring rules based on their unique compliance criteria. The backend calculates individual page scores and aggregates them to determine the cumulative score for the assessment.

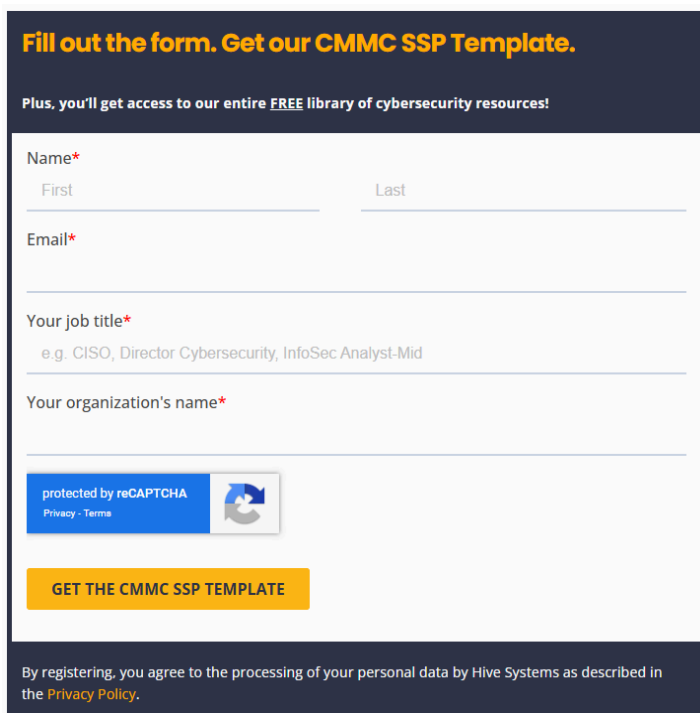
Error handling is an integral part of the backend processes. If issues such as missing data or calculation errors occur, the backend generates a structured error response to ensure clarity and facilitate troubleshooting. Once all pages are processed, the backend evaluates the cumulative score against a predefined threshold, typically set at 80%, to determine whether the user passes or fails the assessment. Additionally, the backend flags controls marked as "NOT MET" and provides a list of areas requiring improvement, which is sent back to the frontend for display.

Input and Output Walkthrough

Inputs :

1. User Authentication:

The tool is accessible when users input their name, email, job title and organization that will be on the Hive Systems website. We make them agree to a disclaimer in the beginning about the tool detailing that we don't hold user data.



Fill out the form. Get our CMMC SSP Template.

Plus, you'll get access to our entire **FREE** library of cybersecurity resources!

Name*

First Last

Email*

Your job title*

e.g. CISO, Director Cybersecurity, InfoSec Analyst-Mid

Your organization's name*

protected by reCAPTCHA
Privacy - Terms

GET THE CMMC SSP TEMPLATE

By registering, you agree to the processing of your personal data by Hive Systems as described in the [Privacy Policy](#).

2. Summary page

Read the Overview: Before beginning the survey, make sure you understand the purpose and estimated time.

Agree to the Terms: Check the box confirming that you agree to the privacy and confidentiality notice.

Click “Begin”: Once you agree, you can click the "Begin" button to start the survey.

CMMC Compliance Tool by Hive Systems

This survey is designed to assess key aspects of cybersecurity compliance across 14 control families, providing valuable insights into your organization’s compliance posture.

Estimated Time: The survey should take approximately 45–50 minutes to complete. Please note that it is best to complete the questionnaire in one sitting, as it cannot be saved partway through.

Privacy and Confidentiality Notice: Your privacy is our priority. Your survey responses will not be saved or stored anywhere else due to our strict privacy policy, ensuring that your data remains secure and confidential.

Assessment Report: At the end of the survey, you will receive a detailed report with your assessment scores. This report will highlight any areas where questions were not fully met, allowing you to prioritize these aspects for improvement.

Let’s get started!

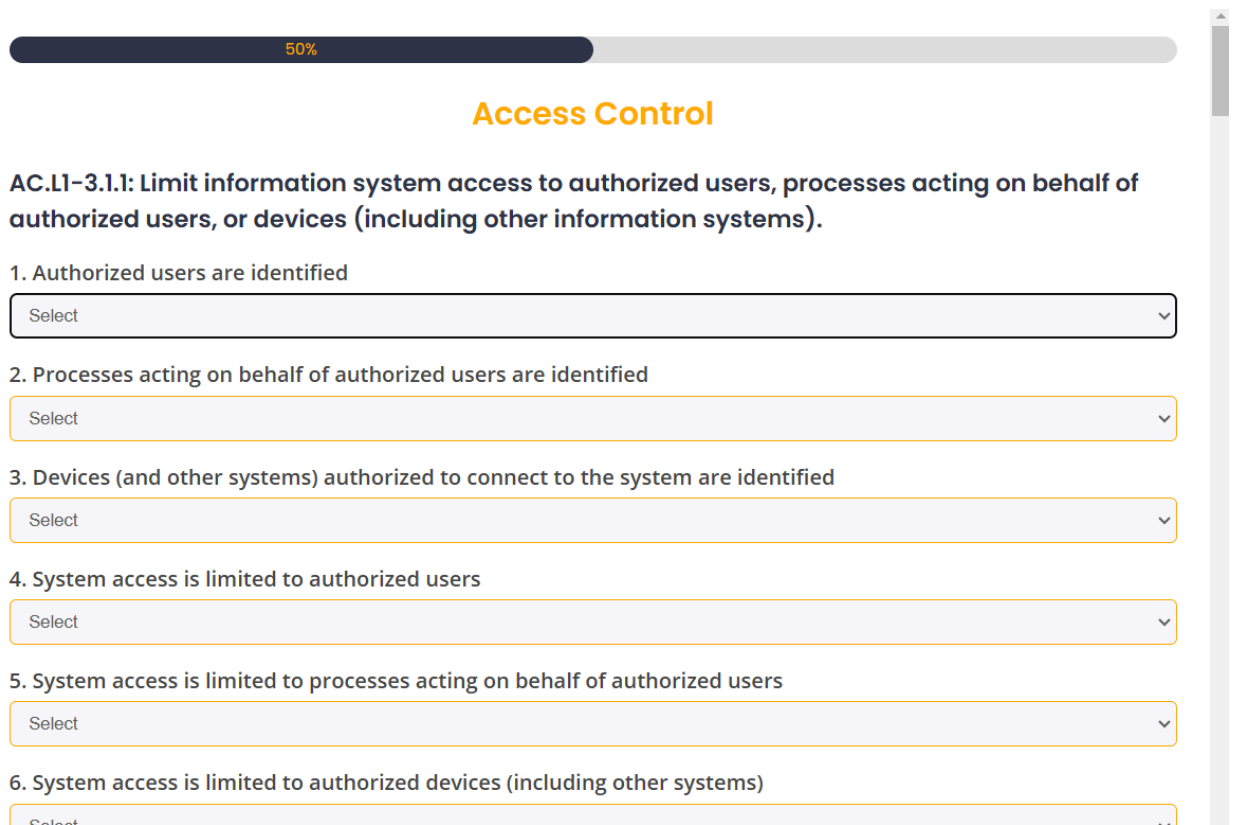
☒ I agree

Begin

3. Overview of the page

The page includes the following elements:

- Progress bar
- Name of control families (e.g. “Access Control”)
- Sub-controls with unique IDs (e.g. “AC.L1-3.1.1”)
- Statements under each sub-control
- Dropdown menus



50%

Access Control

AC.L1-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

1. Authorized users are identified
2. Processes acting on behalf of authorized users are identified
3. Devices (and other systems) authorized to connect to the system are identified
4. System access is limited to authorized users
5. System access is limited to processes acting on behalf of authorized users
6. System access is limited to authorized devices (including other systems)

4. Progress Bar

The progress bar shows the percentage of the survey you have completed. It helps you manage your time effectively and gives you an overview of the survey’s length. By checking the progress, you can see how much you've completed and plan the remaining time accordingly.



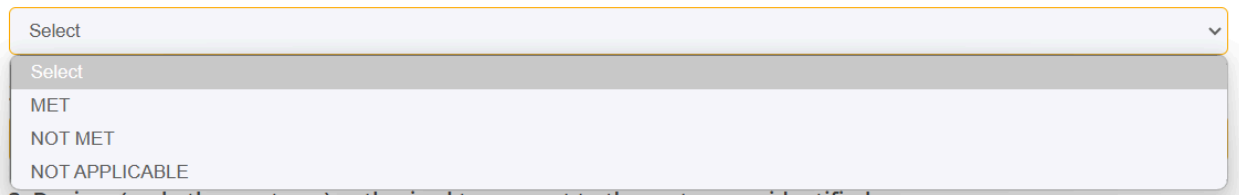
50%

5. Drop Down List

The Drop-Down menu allows the user to select a response for each statement. The user needs to select the most appropriate option based on their actual situation.

AC.LI-3.1.1: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

1. Authorized users are identified



Select

Select

MET

NOT MET

NOT APPLICABLE

3. Devices (and other systems) authorized to connect to the system are identified

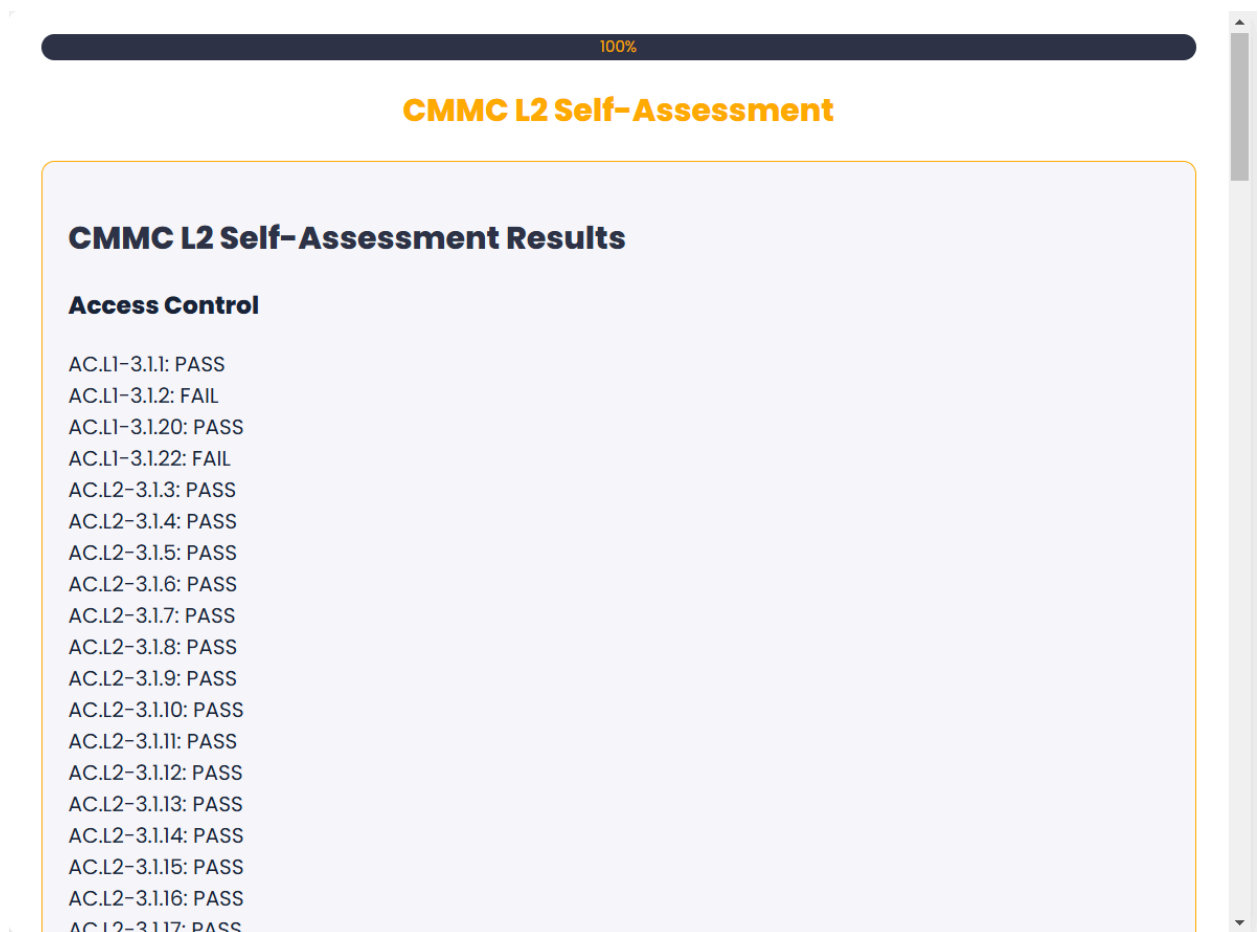
6. Navigation Buttons

By clicking "PREVIOUS" or "NEXT," the user can navigate to the previous page or proceed to the next page.



Outputs:

Outputs are generated in a report form, for each question under each control, and it is downloadable as a PDF for users' reference



The report consists of the cumulative score, overall assessment result, and area of improvement section for the user to understand how they can correct the compliance and the results are as follows in three sections:

- Areas requiring improvement
- Cumulative score
- Overall assessment result(Fail/Pass)

Areas Requiring Improvement

The following objectives were marked as NOT MET:

- **AC.L1-3.1.2:** The types of transactions and functions that authorized users are permitted to execute are defined
- **AC.L1-3.1.22:** Individuals authorized to post or process information on publicly accessible systems are identified
- **CM.L2-3.4.6:** Essential system capabilities are defined based on the principle of least functionality
- **CM.L2-3.4.8:** Allowlisting to allow the execution of authorized software or denylisting to prevent the use of unauthorized software is implemented as specified

Cumulative Score: 94 / 110 (85.45%)

Overall Assessment: PASS

[Download as PDF](#)

Downloadable PDF option:

Users can click “Download as PDF” to save the report locally.

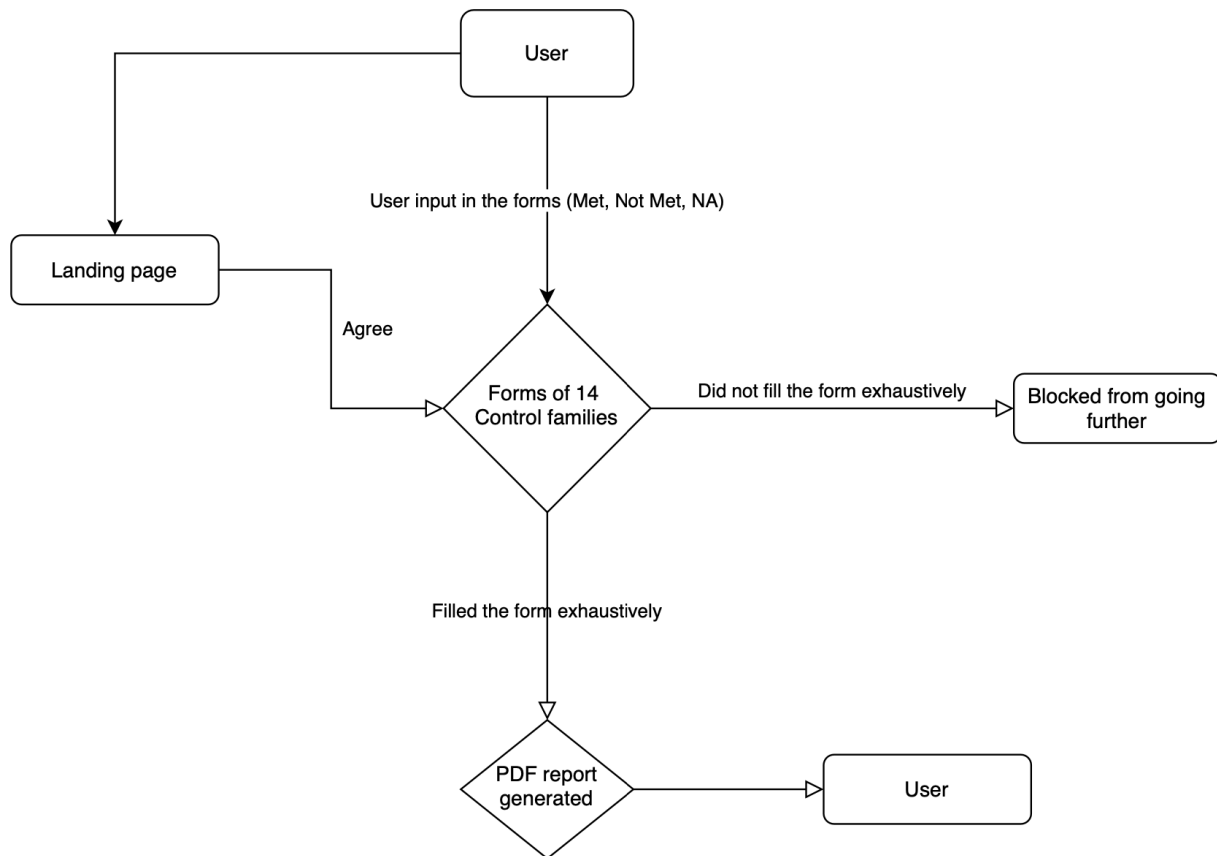
Cumulative Score: 94 / 110 (85.45%)

Overall Assessment: PASS

[Download as PDF](#)

4. Standalone Understanding

Workflows Diagram



CMMC Compliance tool User Flow Diagram

Steps to Use the Tool

1. Access the Tool

- Open the tool via the provided web link or hosted platform.

2. Start the Assessment

- The system dynamically loads the questionnaire, categorized into control families, each containing specific compliance criteria.

3. Complete the Questionnaire

- For each control family:
 - Use dropdown menus to select your responses for each criterion: MET, NOT MET, or NOT APPLICABLE.
 - Ensure all questions on the page are completed before progressing, as incomplete responses will block navigation.

4. Navigate Through Sections

- Use the Next and Previous buttons to move between sections.
- Monitor your progress using the progress bar, which updates in real time as you complete each section.

5. Submit the Assessment

- After completing all sections, click the Submit button to finalize your responses.
- The system will send your responses to the backend for scoring and analysis.

6. Review Results

- Once the backend processes your responses, a Summary Page will display:
 - Detailed results for each control family, showing PASS or FAIL status.
 - Overall assessment score and areas needing improvement.

7. Download the Report

- Click the Download Report button to generate a PDF of your assessment results.
- The PDF will include:
 - A family-wise breakdown of scores.
 - Overall assessment summary.
 - Recommendations for addressing non-compliance.

8. Retake the Assessment if Needed

If adjustments are required, revisit the tool and restart the assessment process to reflect new compliance measures.

By following these steps, users can efficiently conduct assessments and generate actionable insights, even without the ability to save progress between sessions.

5. Deployment Instructions

Repository and File Structure

GitHub Repository Link

- [Hive Control Assessment Tool](#)

Repository Structure

```
hive-control-assessment-tool/
├── css/                # Directory for CSS styles
│   └── styles.css      # Main stylesheet
├── js/                 # Directory for JavaScript files
│   └── script.js       # Main JavaScript functionality
├── index.html          # Main application interface
├── startingpage.html   # Introduction and instructions page
├── main.py             # Flask application backend
└── README.md           # Project documentation
```

Components Explained:

- **HTML Files:**
 - index.html: The main application page users interact with.

- startingpage.html: Provides introductory content or instructions for users.
- **CSS:**
 - styles.css: Provides styling for the HTML pages.
- **JavaScript:**
 - script.js: Contains client-side logic, such as dynamic form handling or DOM manipulation.
- **Backend:**
 - main.py: Flask backend script to serve the HTML files and handle any additional logic.
- **Documentation:**
 - README.md: Includes an overview, setup, and usage instructions.

Setup and Installation

Tools and Software Required

- **Python** (v3.8 or higher)
- **pip** (Python package manager)
- **Flask** (Python web framework)
- **Git** (to clone the repository)
- **Optional:** Docker (for containerized deployments)

Local Setup Instructions

- **Clone the Repository:**

```
bash
Copy code
git clone https://github.com/UMDMSISCapstone/hive-control-assessment-tool.git
cd hive-control-assessment-tool
```

Running the System

1. **Install Dependencies:**

```
bash
Copy code
pip install flask
```

2. Run the Application:

bash

Copy code

python main.py

3. Access the Application:

- Open a browser and navigate to <http://127.0.0.1:5000>.

Troubleshooting Tips

Flask Not Found:

Install Flask:

bash

Copy code

pip install flask

Port Already in Use:

Run Flask on a different port:

bash

Copy code

python main.py --port=8000

- **Static Files Not Loading:**

Verify the directory structure matches Flask's requirements (e.g., `css/` folder path in HTML files).

README Documentation on GitHub

- Here is the README file link: [README](#)

6. Recommendations for Future Improvements

Areas for improvement based on stakeholder feedback:

There have been requests for more user-friendly reports, as the current format lacks the visual appeal and personalization many users desire. Due to time and working knowledge constraints, we were unable to fully accomplish that. Our client also mentioned adding login authentication, but due to constraints of not storing any user data, it could not be achieved. Addressing these issues will ensure the tool's alignment with the business needs and expectations.

Scalability and Performance:

If the tool's user base grows, ensuring scalability and performance enhancements to meet demands are essential. Incorporating a cloud-based database solution can manage data and provide support for concurrent users. Leveraging caching mechanisms and load balancing can improve performance during high-traffic periods. These improvements will prepare our tool to handle future growth without compromising user experience.

New Features:

Our proposed new features include visual reports and AI integration. These reports will allow users to utilize the format to meet organizational needs for better understanding and clarity aiding in decision making and providing actionable insights. Adding charts, graphs, and branding options can further enhance professionalism. Taking one step further, the integration of an AI agent offers another level of sophistication that can guide users through the assessment process with real-time assistance and personalized feedback. These features align with our client needs by improving efficiency, and engagement and ultimately, enhancing the tool's value proposition.

Team and Process Improvements:

Reflecting on our development process, there were opportunities to delegate tasks and enhance collaboration and communication. One key lesson learned was the importance of transparency and accountability which could have avoided delays and miscommunication. The lack of technical background for a few members was a setback, as it placed additional responsibility on others to initiate, manage, teach, and delegate tasks.

To address these challenges, it would have been beneficial to establish a structured onboarding process for team members to familiarize themselves with the technical requirements. Additionally, implementing clear documentation could have bridged skill gaps and empowered all members to contribute effectively. Moving forward, fostering a culture of open communication, regular check-ins, and defined role expectations will be critical to improving team efficiency and ensuring successful project outcomes.

7. Conclusion

Summary

The CMMC Level 2 Self-Assessment Tool developed by Hive Systems exemplifies a practical, user-friendly solution for simplifying cybersecurity compliance. Designed to address the complexity of compliance processes, the tool integrates intuitive frontend features with robust backend functionality. Key highlights include dynamic questionnaire management, real-time progress tracking, automated scoring, and professional PDF reporting. The development process was guided by research and user feedback, ensuring the tool meets client needs while reducing manual errors and improving efficiency.

This system has had a meaningful impact on its intended audience, including organizations of varying sizes and non-profits, by making compliance accessible, efficient, and affordable. By automating traditionally cumbersome processes, the tool has empowered users to focus on their strategic goals without being bogged down by compliance challenges.

Next Steps

To ensure the system's continued growth and utility, the following steps are recommended:

- **Maintenance and Support:** Establish a regular maintenance schedule to address bugs, update compliance frameworks, and incorporate user feedback.
- **Future Enhancements:** Focus on integrating features such as login authentication, personalized visual reporting, and AI assistance to provide a seamless and engaging user experience.
- **Scalability and Deployment:** Transition to a cloud-based database and implement load balancing to ensure the tool can support a growing user base and concurrent access.

- Handover: Facilitate a smooth transfer of the tool to the client's team with comprehensive documentation and training sessions to enable them to manage and update the system independently.

This project underscores Hive Systems' commitment to making cybersecurity approachable and effective, paving the way for broader adoption and stronger compliance practices across industries.