HIVE SYSTEMS

CYBERSECURITY THAT’S APPROACHABLE

www.hivesystems.com

AGENDA

01 INTRODUCTION

02 DEVELOPMENT PROCESS

03 FEATURES & FUNCTIONALITY

04 RESULTS

05 FUTURE IMPROVEMENTS

06 CONCLUSION

COMPANY OVERVIEW

HIVE SYSTEMS

Hive Systems is a consulting firm focused on making cybersecurity more approachable. They support companies of various sizes with understanding and tackling a full spectrum of cybersecurity issues from simple phishing simulations to FedRAMP authorizations.

HIVE HELPS

Hive Systems offers pro bono services (Hive Helps) to qualified non-profit organizations and communities to ensure that limited resources don’t hinder social progress.

INTRODUCTION

Problem:

Many companies struggle with the intricacy of cybersecurity compliance requirements, finding it difficult to tread through various standards, regulations, and frameworks

Our **objective** is to develop a user-friendly self-assessment CMMC Level 2 tool for all company sizes to make the process simpler and affordable

PURPOSE

Develop Self-assessment Tool

Outreach and Streamline Processes

Reduce the Burden

STAKEHOLDERS

HIVE SYSTEMS (THE COMPANY)

PROSPECTIVE CLIENTS OF HIVE SYSTEMS

DEVELOPMENT PROCESS

RESEARCH

- Conducted interviews and surveys to understand client needs.
- Focused on simplifying manual compliance processes.

DESIGN

- Figma, HTML, CSS
- Implemented intuitive UI/UX elements: progress bars, dropdowns, and navigation buttons

TECHNOLOGY

- Used **Flask** for backend development, incorporating modular functions for scoring logic, form validation, and PDF generation.
- Scoring criteria were centralized in a configuration file (**JSON**), ensuring maintainability and version control. Caching mechanisms (**Flask-Caching**) optimized performance, and asynchronous processing (**Flask-SocketIO**) was implemented for time-consuming tasks.

TESTING & DEPLOYMENT

- Tested front-end and back-end integration.
- Validated compliance logic with unique use cases.

CHALLENGE

- Ensuring accurate compliance logic for diverse and complex use cases.

CONTROLS LOGIC

WE HAVE 14 CONTROL FAMILIES & 110 CONTROLS

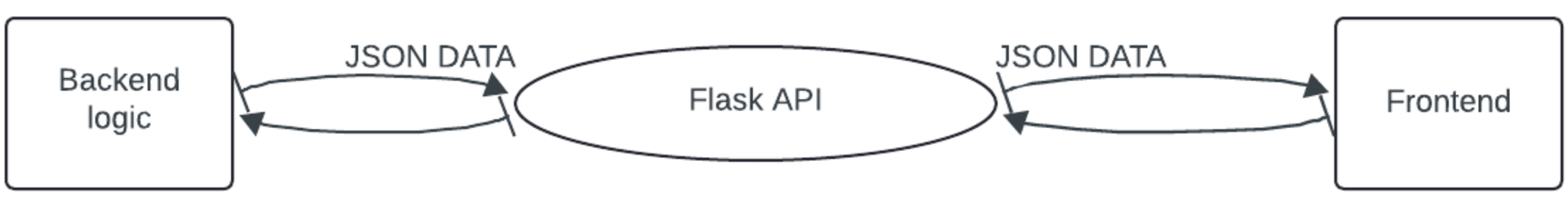
Categorization of Controls:

Base Bucket: Controls with a standard scoring logic.
Special Bucket: Controls with unique conditions for score calculation.

Example Control Scenarios:

- **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.'

TECHNOLOGY



KEY FEATURES

1

DYNAMIC QUESTIONNAIRES WITH CENTRALIZED MANAGEMENT

The web tool dynamically generates questionnaires allowing users to interact with dropdowns for each control family .

2

REAL-TIME PROGRESS TRACKING

The web tool provides a progress bar that updates in real-time as users complete sections, offering immediate feedback on completion status

3

DETAILED RESULTS AND AUTOMATED SUMMARY GENERATION

The tool automatically calculates and displays detailed results, including per-control PASS/FAIL statuses and an overall assessment (PASS or FAIL) based on the cumulative score.

4

PDF EXPORT FOR EASY REPORTING

Users can download a PDF summary of the assessment results directly from the tool, which includes family-wise details and overall scores

FUNCTIONALITY

Structured Data Input and Validation:
Collects user responses through dropdown menus, ensuring standardized inputs for each criterion. Validates completeness before allowing progression to prevent errors.

Dynamic Questionnaire Management:
Automatically organizes questions into distinct control families (e.g., "Access Control") based on predefined datasets, enabling easy scalability and customization.

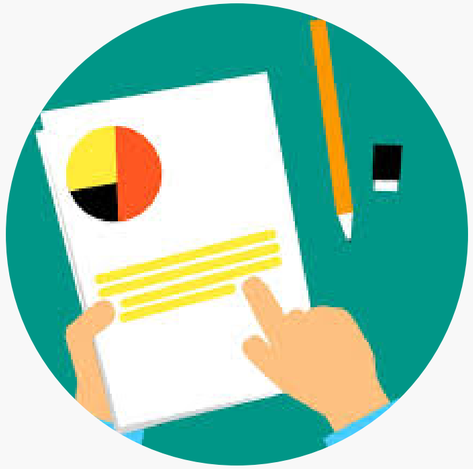
Automated Scoring and Results Generation:
Evaluates each control as PASS or FAIL based on user responses and calculates overall assessment results with a scoring threshold (e.g., 80% of 110).

Real-Time Navigation and Progress Tracking:
Provides intuitive navigation with Next and Previous buttons and a real-time progress bar, ensuring users can track and update their responses effortlessly.

FUTURE IMPROVEMENTS

INTEGRATING DATABASE

As the demand for the tool grows, incorporating a database with login authentication will enhance functionality by allowing users to store their assessments. This feature will enable users to start and complete assessments at their convenience.



REPORT ENHANCEMENTS

Report customization tailored to client companies can be introduced, allowing personalized insights and branding. Additionally, improvements can be implemented by adding charts to enhance readability.

AI AGENT

AI Agent can be integrated into the tool, enabling AI assistance to help users complete questionnaires efficiently and provide intelligent feedback based on their responses.

RESULTS

Streamlined Data Collection: Replaced manual Excel processes with an interactive web tool, reducing errors and improving data consistency.

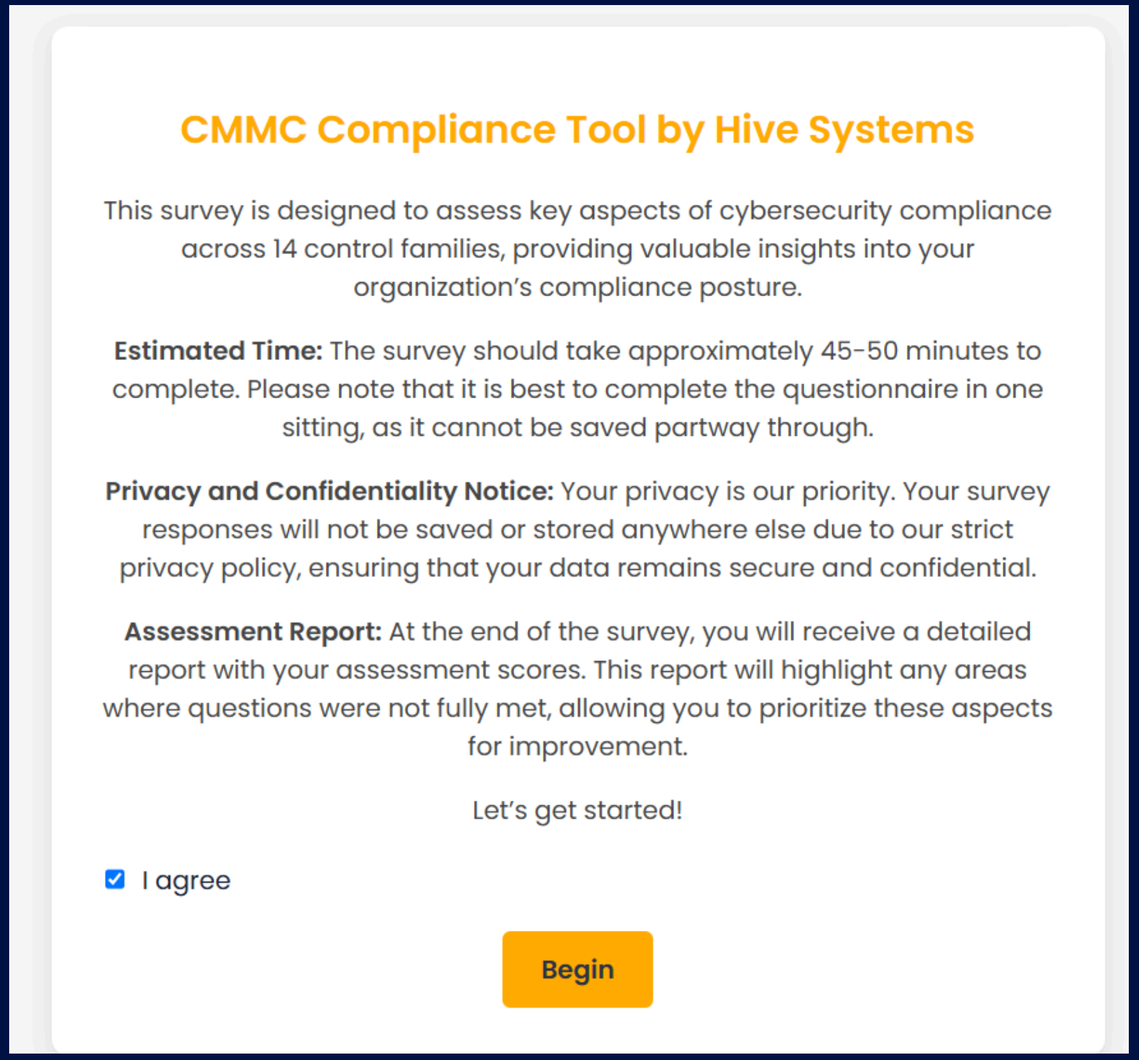
Enhanced User Experience: Introduced real-time progress tracking and intuitive navigation for seamless assessments.

Automated Evaluation: Standardized the scoring process with automated PASS/FAIL evaluations, ensuring objective results.

Simplified Reporting: Enabled professional PDF report generation, making result sharing and documentation more efficient.

THANK YOU!

APPENDIX



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.

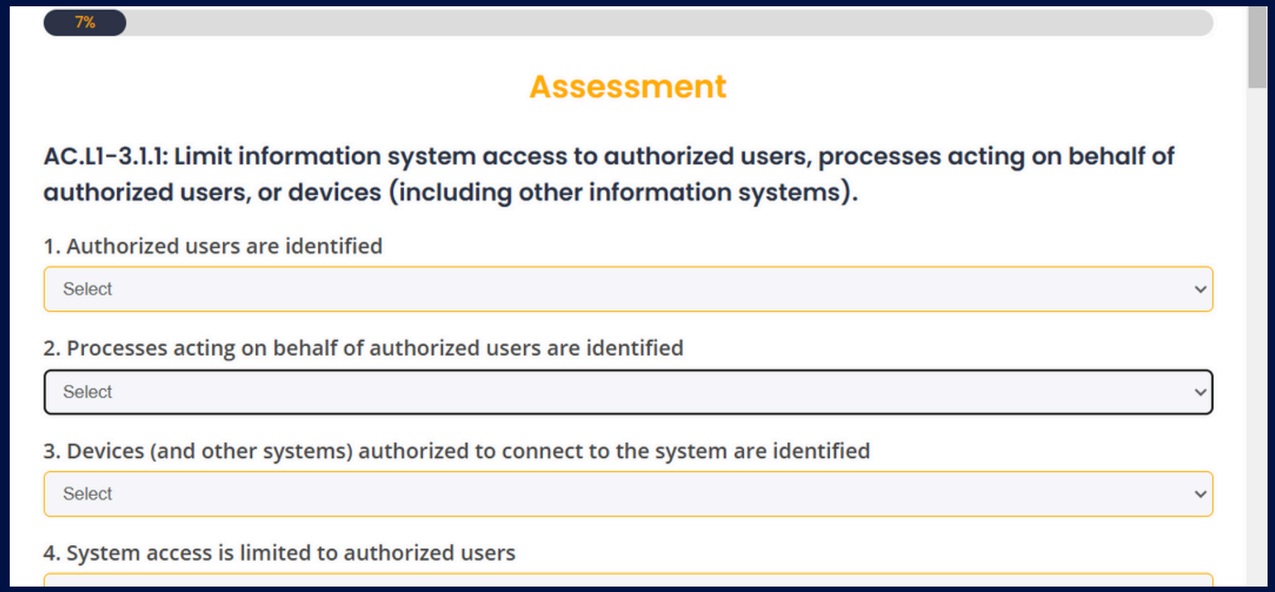
Privacy and Confidentiality Notice: Your privacy is our priority. Your survey responses will not be saved or stored anywhere else due to our strict privacy policy, ensuring that your data remains secure and confidential.

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



7%

Assessment

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

Select

2. Processes acting on behalf of authorized users are identified

Select

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

Select

4. System access is limited to authorized users

Assessment Results

Access Control

AC.L1-3.1.1: FAIL
AC.L1-3.1.2: PASS
AC.L1-3.1.20: FAIL
AC.L1-3.1.22: FAIL
AC.L2-3.1.3: PASS
AC.L2-3.1.4: PASS
AC.L2-3.1.5: PASS
AC.L2-3.1.6: PASS
AC.L2-3.1.7: PASS
AC.L2-3.1.8: FAIL
AC.L2-3.1.9: PASS
AC.L2-3.1.10: PASS
AC.L2-3.1.11: PASS
AC.L2-3.1.12: PASS
AC.L2-3.1.13: PASS
AC.L2-3.1.14: PASS
AC.L2-3.1.15: PASS
AC.L2-3.1.16: PASS
AC.L2-3.1.17: PASS
AC.L2-3.1.18: PASS
AC.L2-3.1.19: PASS
AC.L2-3.1.21: PASS

Awareness and Training

AT.L2-3.2.1: PASS
AT.L2-3.2.2: PASS

new passwords are created

- **IR.L2-3.6.1**: The operational incident handling capability includes user response activities
- **MA.L2-3.7.2**: Personnel used to conduct system maintenance are controlled
- **PS.L2-3.9.2**: The system is protected during and after personnel transfer actions
- **PE.L2-3.10.2**: The physical facility where organizational systems reside is protected
- **RA.L2-3.11.2**: Vulnerability scans are performed on applications when new vulnerabilities are identified
- **CA.L2-3.12.4**: The security requirements identified and approved by the designated authority as non-applicable are identified
- **SC.L2-3.13.1**: Communications are monitored at key internal boundaries
- **SC.L2-3.13.2**: Architectural designs that promote effective information security are identified
- **SC.L2-3.13.4**: Unauthorized and unintended information transfer via shared system resources is prevented
- **SC.L2-3.13.12**: Collaborative computing devices are identified
- **SI.L2-3.14.3**: System security alerts and advisories are monitored
- **SI.L2-3.14.7**: Unauthorized use of the system is identified

---

Cumulative Score: -64 / 110 (-58.18%)

Overall Assessment: FAIL

Download as PDF