Scientific Research Publishing

Open Journal of Applied Sciences, 2025, 15(1), 274-284
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

A Web Platform Based on the NIST CSF for Assessing and Monitoring the Cybersecurity of SMEs and Critical Infrastructures

Mohamadou Konate[1*], Pegdwinde Justin Kouraogo[2], Omar Hamidou Harouna[3]

[1]Institut Burkinabe des Arts et Metiers (IBAM), Joseph KI-ZERBO University, Ouagadougou, Burkina Faso
[2]Computer Science Department, Joseph KI-ZERBO University, Ouagadougou, Burkina Faso
[3]Science and Technology Training and Research Unit, New Dawn University, Ouagadougou, Burkina Faso
Email: *mohamadou.konate@ujkz.bf

How to cite this paper: Konate, M., Kouraogo, P. J. and Hamidou Harouna, O. (2025) A Web Platform Based on the NIST CSF for Assessing and Monitoring the Cybersecurity of SMEs and Critical Infrastructures. *Open Journal of Applied Sciences*, **15**, 274-284.
https://doi.org/10.4236/ojapps.2025.151018

Received: November 6, 2024
Accepted: January 27, 2025
Published: January 30, 2025

Abstract

The NIST Cybersecurity Framework (NIST CSF) serves as a voluntary guideline aimed at helping organizations, tiny and medium-sized enterprises (SMEs), and critical infrastructure operators, effectively manage cyber risks. Although comprehensive, the complexity of the NIST CSF can be overwhelming, especially for those lacking extensive cybersecurity resources. Current implementation tools often cater to larger companies, neglecting the specific needs of SMEs, which can be vulnerable to cyber threats. To address this gap, our research proposes a user-friendly, open-source web platform designed to simplify the implementation of the NIST CSF. This platform enables organizations to assess their risk exposure and continuously monitor their cybersecurity maturity through tailored recommendations based on their unique profiles. Our methodology includes a literature review of existing tools and standards, followed by a description of the platform's design and architecture. Initial tests with SMEs in Burkina Faso reveal a concerning cybersecurity maturity level, indicating the urgent need for improved strategies based on our findings. By offering an intuitive interface and cross-platform accessibility, this solution aims to empower organizations to enhance their cybersecurity resilience in an evolving threat landscape. The article concludes with discussions on the practical implications and future enhancements of the tool.

Keywords

Cybersecurity, NIST CSF Framework, Cybersecurity Assessment Tool, Cybersecurity Mitigation, Small and Medium-Sized Enterprises, Critical Infrastructure

1. Introduction

The NIST Cybersecurity Framework (NIST CSF) is a voluntary initiative designed to assist organizations in managing cyber risks effectively. Grounded in a selection of standards, guidelines, and best practices, the NIST CSF remains technology-neutral, aiming to empower critical infrastructure operators and other ICT-related businesses with a structured approach to enhancing resilience against security threats. However, as noted by Wrenn [1], "The NIST Cybersecurity Framework is by far the most comprehensive framework, but it is also the most complex to navigate". This complexity indicates a need for simplification and guidance, particularly for small and medium-sized enterprises (SMEs) lacking extensive cybersecurity resources.

Current tools aimed at supporting the implementation of the NIST CSF can be broadly categorized into two types:

- **Proprietary tools**: Typically designed for complex audit processes within large organizations, these tools can often be overwhelming and costly for smaller entities.
- **Open-source tools**: While generally free, they are often limited to community-sourced toolkits, frequently based on spreadsheets, making them difficult to use effectively in dynamic business environments.

Both categories often neglect the specific requirements of SMEs, which, while frequently representing a weak link in cybersecurity defense, can also serve as entry points for cybercriminals targeting larger corporations. In light of this limitation, our research seeks to simplify the implementation of the NIST CSF through a user-friendly, open-source web platform designed for accessibility by both SMEs and critical infrastructure organizations. This platform addresses a crucial gap by providing a structured approach to cybersecurity assessment and maturity monitoring that is often missing in existing tools.

The choice to test this platform with SMEs in Burkina Faso is particularly significant. SMEs in developing countries, such as Burkina Faso, face unique cybersecurity challenges due to limited financial and technical resources, as well as lower levels of cybersecurity awareness. These conditions make SMEs vulnerable and attractive targets for cyber threats, underscoring the importance of developing tools that are affordable, easy to use, and specifically tailored to their context. Additionally, improving the cybersecurity posture of SMEs in Burkina Faso can contribute to the broader cybersecurity ecosystem, as these businesses often form part of supply chains or support critical sectors within the national economy.

Our primary objective is to enhance the accessibility of the NIST CSF by developing a web platform that offers a tailored experience based on the unique risk profiles and organizational needs of users. The specific functions of the platform include:

- **Risk Exposure Assessment:** Evaluating the level of exposure to cybersecurity risks pertinent to the organization type and generating custom checklists and recommendations for the identified risks.

- **Continuous Maturity Tracking:** This allows organizations to monitor the implementation of recommendations over time and assess improvements in their cybersecurity maturity levels.

By focusing on SMEs and critical infrastructure, this platform aims to bridge a significant gap in cybersecurity tools, providing an adaptable and scalable solution for a wide range of organizations.

This article is structured into several sections to provide a comprehensive overview of the research and methodology employed in developing our NIST CSF-based cybersecurity assessment and monitoring platform. We will begin with a literature review that contextualizes our study by examining existing works and tools for critical infrastructure and SMEs. Next, the methodology section will detail the design process of our platform, the assessment steps, and the benefits it offers in terms of accessibility and simplification for SMEs and critical infrastructure. Following that, we will present the proposed architecture of the platform and the results of tests conducted with several SMEs in Burkina Faso, accompanied by analyses of the cybersecurity maturity levels of these organizations. Finally, the discussion and conclusion will summarize the obtained results, their practical implications, and the prospects for enhancing and expanding our tool for future use, particularly for organizations managing critical infrastructure.

2. Literature Review

2.1. Work and Tools Based on the NIST CSF for Critical Infrastructures

L. Johnson [2] offers a detailed exploration of the NIST CSF's history, core principles, and practical guidance for cybersecurity professionals conducting assessment activities. However, while comprehensive, Johnson's guide is highly theoretical and challenging for smaller organizations without dedicated cybersecurity teams to implement independently. The Federal Office for National Economic Supply (FONES) in Switzerland [3] has developed a minimum ICT standard based on the NIST CSF for critical infrastructure sectors, where system failures are unacceptable due to societal impact. While this tool offers self-assessment in Excel with 106 control measures aligned with the NIST CSF's five functions, it remains limited to Swiss companies. The Excel-based format can also restrict accessibility, making it challenging for SMEs without IT resources to navigate and utilize effectively.

2.2. Work Based on the NIST CSF for SMEs

Chidukwani, Zander, and Koutsakis [4] conducted a survey on cybersecurity in small and medium-sized enterprises (SMEs), revealing that research on SME cybersecurity primarily focuses on the "Identify" and "Protect" functions, with limited guidance on the other three (Detect, Respond, and Recover). This gap leaves SMEs with insufficient guidance on how to respond to and recover from cyber incidents. Benz and Chatterjee [5] developed an SME Cybersecurity Assessment

Tool (CET) as a straightforward, 35-question online survey for IT managers to assess their cybersecurity maturity across all five NIST CSF functions. Although this tool is accessible and tailored for SMEs, it lacks the depth and advanced features needed for more comprehensive assessments, making it less suitable for large companies or critical infrastructure. Another tool, described in [6], is a generic, web-integrated audit information system designed for ISO-27001 compliance, featuring a structured data model adaptable for various audit processes. While robust, this system is primarily designed for ISO-27001 and requires adaptation and expertise to apply NIST CSF controls effectively.

2.3. Summary of Works

Michael Benz and Dave Chatterjee's work on an SME cybersecurity assessment tool [5] is based on 35 essential NIST CSF checks they consider highly relevant for evaluating SME security maturity. For critical infrastructure, Switzerland's Federal Office for Economic Supply's minimum standard for IT resilience offers a self-assessment tool with 106 control measures aligned with the NIST CSF functions, allowing organizations to assess or audit their cybersecurity practices. **Table 1** below provides a comparative summary of key cybersecurity assessment approaches and tools using the NIST CSF, emphasizing their respective strengths and limitations. This situates our proposed platform as a unique solution designed to address the specific needs of SMEs and critical infrastructure, overcoming the limitations identified in previous works.

Table 1. Overview of work in the field.

Reference	Objective	Target Audience	Approach/Tooling	Strengths	Limitations
L. Johnson [2]	A detailed explanation of the NIST CSF creation and components; a practical guide for professionals	Critical infrastructure	Practical guide and general recommendations	Comprehensive methodology for rigorous NIST CSF applications	Complex to implement; lacks specific technological support for SMEs
FONES (Switzerland) [3]	Minimum ICT standard for critical infrastructure resilience, with self-assessment based on NIST CSF	Critical infrastructure	Excel tools with 106 controls for self-assessment	Clear and systematic self-assessment method	Limited to Swiss companies; Excel format restricts accessibility and ease of use
Chidukwani, Zander, and Koutsakis [4]	Identifies gaps in SME cybersecurity research, especially in detection, response, and recovery	SMEs	Qualitative study based on current practices	Highlights specific weaknesses in SME cybersecurity	Lacks specific tools or solutions; limited focus on Identify and Protect functions
Benz & Chatterjee [5]	SME-focused cybersecurity assessment tool with 35 NIST CSF checks for maturity evaluation	SMEs	Online questionnaire for maturity assessment	Easy to use and tailored for SMEs	Limited depth for large companies or critical infrastructure; minimal advanced features

3. Web Platform Based on NIST CSF

The platform we offer is designed to facilitate the assessment and monitoring of the cybersecurity of organizations, based on the security framework of the National Institute of Standards and Technology. This platform was developed to meet the specific needs of small and medium-sized businesses as well as critical infrastructure, which require effective and accessible cybersecurity tools, but are often undervalued by existing solutions. By combining proven security principles and automated monitoring features, our platform aims to overcome the limitations of traditional tools, such as Excel files and proprietary solutions, which can be expensive or unsuitable for SMEs.

The main added value of this platform lies in its intuitive user interface and its cross-platform accessibility, which makes it independent of any operating system. It is compatible with Windows, macOS, Linux, and other web platforms, ensuring that companies and cybersecurity professionals can access assessments and recommendations, regardless of their technical configuration. By adopting a responsive web design approach, our tool offers a solution that is accessible to all, reducing technical barriers and enabling simplified cybersecurity management.

The platform architecture is centered on continuous assessment and automated monitoring of the cybersecurity maturity of organizations. The assessment steps are organized into distinct modules corresponding to the five NIST CSF functions, allowing a targeted assessment of each critical security dimension. This modular approach makes it possible to regularly update the recommendations and dynamically monitor progress in cybersecurity.

3.1. Methodology

Figure 1 below shows the assessment process in 3 main stages:

- Stage 1: Fill in the form to select the type of organization;
- Stage 2: Automatic processing of data and analysis of results;
- Stage 3: Monitoring and updating the organization's level of maturity.

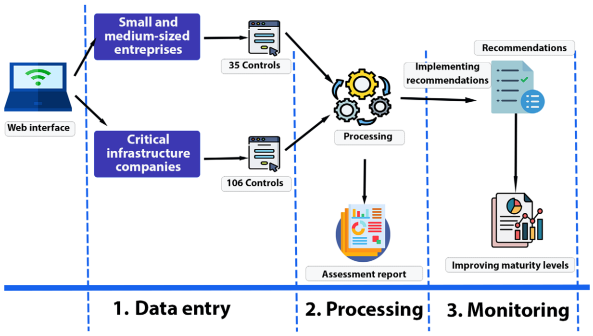

Figure 1. Assessment process.

By integrating the NIST CSF-specific assessment categories, this first step customizes the initial assessment and aligns the organization's priorities with appropriate cybersecurity standards.

This analysis module generates an assessment of the five NIST CSF functions to identify security gaps and hardening priorities.

The final stage of the process allows for continuous monitoring of the organization's cybersecurity progress. This automatic update is a major asset for the sustainability of the approach, ensuring that the organization remains aligned with evolving cybersecurity standards.

3.2. Proposed Architecture

The proposed tool is a web-based platform designed to be highly accessible and user-friendly, providing operating system independence so that users can interact with it across various environments. This flexibility allows any user, regardless of their operating system, to benefit from the platform's capabilities.

The application comprises three architectural and conceptual layers based on the Model-View-Controller (MVC) design model: a data layer that defines the data model, a logic layer that defines the business processes that can be executed, and a visualization layer that implements the functionalities for reporting data to the user. Figure 2 below shows the separation of roles between the three layers, as well as the different technologies used. The PHP Laravel Framework and MySQL are used as the programming language and database management system respectively.

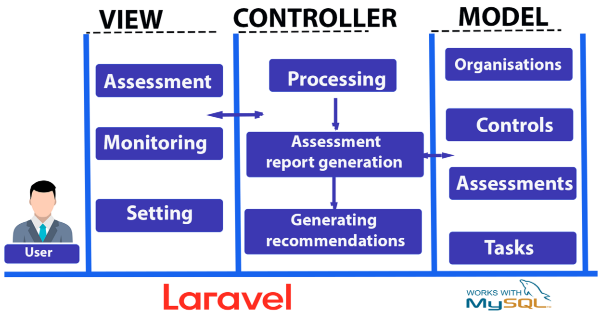

Figure 2. Architecture of the web platform.

- **Scalability Considerations**

The platform has been designed with scalability in mind, allowing it to grow and adapt to increasing data loads and expanding user needs. Leveraging a modular architecture, the platform can integrate new features and functionalities as they are developed, ensuring continued alignment with industry standards and emerging technologies. For instance, the back end infrastructure utilizes containerization and microservices, making it easier to scale specific components independently without impacting the overall system. This modular setup enables the platform to accommodate a growing number of users and increase data volumes seamlessly.

- **Addressing Evolving Cybersecurity Threats:** To handle the constantly changing cybersecurity landscape, the platform includes real-time monitoring and

threat intelligence capabilities. It uses regular updates from threat intelligence feeds to adjust security assessments dynamically, ensuring that it accounts for the latest known vulnerabilities and attack patterns. By maintaining an up-to-date database of potential threats, the platform can evaluate cybersecurity maturity in the context of current risk scenarios, thereby providing organizations with actionable insights that are relevant to the latest threat landscape.

- **Future Improvements:** As part of its roadmap, the platform has the potential to incorporate advanced analytical features, such as machine learning algorithms, to predict and adapt to emerging threats proactively. Additionally, it could integrate with external systems and APIs to allow for automatic updates in line with industry standards, such as the latest NIST CSF or ISO-27001 revisions. In future versions, the platform may also offer customization options, allowing organizations to tailor security evaluations based on their unique requirements and industry-specific challenges.

3.3. Technical Challenges and Mitigation

During the development of the web platform, several technical challenges arose, each requiring specific mitigation to ensure that the tool functions effectively across different organizational environments. Below, we outline key challenges and the solutions implemented to address them:

- **Cross-Platform Compatibility:** Ensuring the platform's functionality across different operating systems and browsers was critical, as the tool is designed to be OS-independent. To address this, we utilized responsive web design principles and cross-compatible development frameworks (e.g., Node.js for the back end and React.js for the front end). We conducted extensive testing across major browsers and operating systems, allowing us to achieve consistent user experiences regardless of the environment.
- **Real-Time Cybersecurity Maturity Tracking:** Integrating real-time tracking required robust data handling to avoid latency and ensured that security assessment data could be processed instantly. This challenge was mitigated by implementing an optimized MySQL database structure with indexed tables for quick data retrieval and caching techniques to reduce the server load. Additionally, asynchronous JavaScript functions were used to handle real-time updates without affecting the platform's performance.
- **Modular Design and Scalability:** The platform needed to accommodate future enhancements and adjustments for evolving cybersecurity standards. To achieve scalability, we structured the platform as a modular system, where each major function (e.g., risk assessment, maturity tracking) operates as a standalone module. This design allows easy integration of new features or updates without impacting the existing architecture. We also adopted RESTful APIs to enable secure communication between modules and ensure future extensibility.

This mitigation collectively enhances the tool's resilience, scalability, and efficiency, making it adaptable to varied organizational needs and ready for further development.

3.4. Data Privacy and Security

Given the sensitivity of cybersecurity assessments, ensuring data privacy and protection for SMEs using the platform is paramount. The following measures have been implemented to uphold high standards of confidentiality and data security:

- **Data Encryption:** All sensitive data transmitted between the user and the platform is encrypted using SSL/TLS protocols, protecting information from potential interception. Within the database, we apply AES-256 encryption to particularly sensitive fields, such as user credentials and cybersecurity assessment details, to secure data at rest.
- **Access Control and Role-Based Permissions:** The platform employs a role-based access control (RBAC) system, ensuring that only authorized users can access specific data and functionalities. Each user role is assigned specific permission that limit access to only the necessary information, reducing the risk of unauthorized data exposure.
- **Regular Security Audits and Compliance Checks:** To ensure ongoing security, the platform undergoes regular security audits and vulnerability assessments. These audits identify potential weaknesses in the platform's security framework, which are promptly addressed. Additionally, the platform is designed with compliance with data protection standards in mind, adhering to industry best practices, such as GDPR principles, to protect SME data.
- **User Data Minimization and Anonymization:** The platform collects only the minimum amount of data necessary to perform cybersecurity assessments, thus reducing the risk associated with data storage. Whenever feasible, anonymization techniques are applied to sensitive information, further safeguarding user privacy.

By integrating these security measures, the platform ensures that SMEs can confidently assess and monitor their cybersecurity maturity without compromising the confidentiality and integrity of their data.

4. Tests and Results

4.1. Data Collection Methodology

In this study, we engaged 15 small and medium-sized enterprises (SMEs) to participate in an online survey aimed at assessing their cybersecurity practices across the 35 controls outlined in the NIST Cybersecurity Framework (CSF), as proposed by Benz and Chatterjee in their cybersecurity assessment tool for SMEs. The selected companies predominantly operate within the service sector, specifically in information technology, transportation, and research within Burkina Faso.

Out of the 15 SMEs approached, 12 responded, yielding a response rate of 80%. Notably, all respondents answered every question in the survey, and 10 expressed

interest in receiving the results pertaining to their organization's cybersecurity assessment. The primary reasons cited for non-participation included time constraints, lack of interest, and apprehensions regarding the disclosure of organizational vulnerabilities.

4.2. Results

The analysis of responses yielded valuable insights into the cybersecurity levels achieved by participating SMEs across the five NIST CSF functions. As illustrated in the graphs below, each function was rated on a scale from 0 to 4, with the colored lines representing individual scores. The dashed red line denotes the average score, established at 2.6.

Figures 3-5 present a detailed breakdown of the scores obtained for each of the five functions.

FONCTION NIST CSF	NOTE	NOTE MOYENNE
Identifier (ID-Identify)	2.58	2.60
Protéger (PR-Protect)	2.23	2.60
Detecter (DE-Detect)	1.66	2.60
Réagir (RS-Respond)	1.66	2.60
Recupéré (RC-Recover)	2	2.60
Moyenne	**2.03**	**2.60**

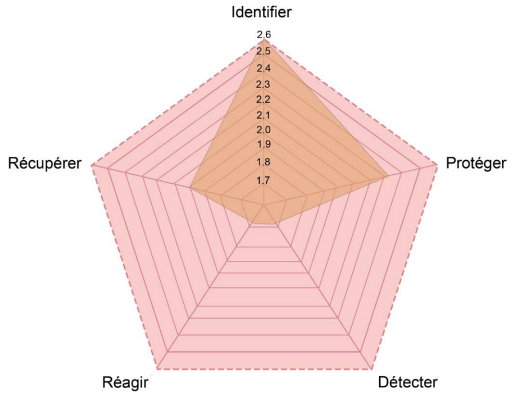

Figure 3. Screenshot of the overall assessment result for one of the SMEs.

The overall average score across these functions was calculated to be 2.02. This result indicates that the participating SMEs exhibit a level of cybersecurity maturity that falls below the recommended threshold. Consequently, it is imperative for the IT security managers of these organizations to develop and implement strategic measures informed by the assessment findings to enhance their cybersecurity posture and increase overall maturity.

FONCTION NIST CSF	NOTE	NOTE MOYENNE
Identifier (ID-Identify)	2.58	2.60
Protéger (PR-Protect)	2.23	2.60
Detecter (DE-Detect)	1.66	2.60
Réagir (RS-Respond)	1.66	2.60
Recupéré (RC-Recover)	2	2.60
Moyenne	**2.03**	**2.60**

Figure 4. Screenshot of the table of evaluation averages by function.

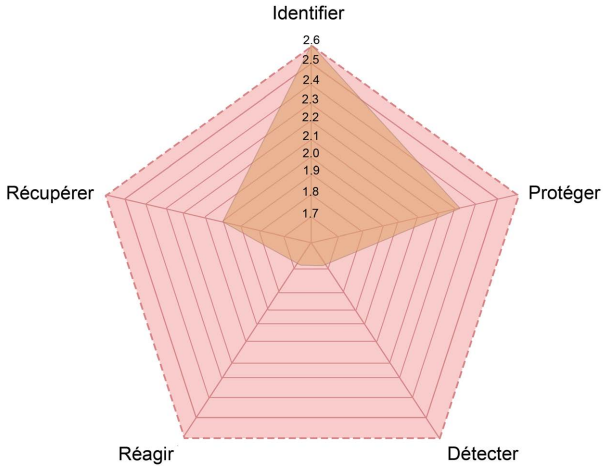

Figure 5. Screenshot of Plot of evaluation averages by function.

4.3. Discussion

In developing our solution, we drew upon established and validated methodologies, particularly the framework provided by Michael Benz and Dave Chatterjee in their cybersecurity assessment tool designed for SMEs, as well as the Minimum Standard for IT Resilience established by the Swiss Federal Office of Economic Supply for critical infrastructure. This foundational approach not only facilitates the evaluation of SMEs and critical infrastructure within a unified platform but also mitigates errors commonly associated with manual data manipulation in spreadsheets, such as Excel, by employing a MySQL database along with user-friendly web interfaces.

Subsequently, we conducted an online survey to collect data intended for case studies that would allow us to test our solution effectively. The results of these tests were promising, as they empowered respondents to evaluate their organization's maturity level, pinpoint vulnerabilities, and receive tailored recommendations for enhancing their cybersecurity posture. This feedback indicates that our solution is effective in providing SMEs with valuable insights and actionable strategies for improving their cybersecurity resilience.

5. Conclusion and Outlook

This article presents the methodology and tools employed to develop a web platform designed to facilitate the assessment of risk exposure and monitor the cybersecurity maturity of two distinct types of organizations: small and medium-sized enterprises (SMEs) and those operating critical infrastructure. The tool has been piloted with approximately 15 SMEs, yielding promising results.

However, there remains significant scope for enhancements. The case study was limited to SMEs, necessitating the use of a 35-task assessment form tailored specifically for this group. Organizations with critical infrastructure tend to be particularly cautious about disclosing details related to their vulnerabilities for security reasons.

In the next phase of our research, we aim to test our solution in evaluating organizations within the critical infrastructure sector. This step will enhance the reliability of our tool and facilitate substantial improvements. To this end, we are focusing on the IT Services Department (DSI) of Joseph KI-ZERBO University in Burkina Faso as a potential partner for this evaluation. By expanding our scope, we hope to refine our assessment tool further and broaden its applicability across various organizational contexts.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Wrenn, G. (2017) CSO Online. https://www.csoonline.com/article/3239968/how-can-my-cyber-program-benefit-from-a-standards-based-approach.html

[2] Johnson, L. (2020) Cybersecurity Framework. In: *Security Controls Evaluation, Testing, and Assessment Handbook*, Elsevier, 537-548. https://doi.org/10.1016/b978-0-12-818427-1.00012-4

[3] Federal Office for Economic Approvals (2018) Minimum Standard for IT Resilience. Bern (Switzerland).

[4] NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

[5] Benz, M. and Chatterjee, D. (2020) Calculated Risk? A Cybersecurity Evaluation Tool for SMEs. *Business Horizons*, **63**, 531-540.

[6] Antunes, M., Maximiano, M. and Gomes, R. (2022) A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing. *Procedia Computer Science*, **196**, 36-43. https://doi.org/10.1016/j.procs.2021.11.070