Analysis and Study of a Cybersecurity Maturity Assessment System for SMEs

Stefano Bistarelli[1,†], Sara Geoli[1,*,†], Chiara Luchini[1,2,†] and Ivan Mercanti[1,†]

[1]Università degli Studi di Perugia, Perugia, Italy
[2]Università degli Studi di Firenze, Firenze, Italy

Abstract

Small and Medium Enterprises (SMEs) are increasingly vulnerable to cyber threats due to limited resources and the absence of tailored cybersecurity frameworks, especially in Italy. This study presents the development of a Cybersecurity Maturity Assessment System designed specifically for SMEs, integrating updates from NIST Cybersecurity Framework (CSF) version 2.0 and the Italian National Framework for Cybersecurity and Data Protection. A refined Framework Core was developed by synthesizing elements from these frameworks, complemented by a simplified methodology derived from official national guidelines. A web-based Cybersecurity Assessment Tool was implemented to guide users through the evaluation process, facilitating the creation of Target and Current Profiles and generating comprehensive Cybersecurity Assessment Reports.

Keywords

SMEs, Cybersecurity Maturity Assessment, Web-based Tool

1. Introduction

Cyber risk awareness is becoming a critical competence for the survival and growth of companies. Any well-executed cyber attack can negatively affect company stakeholders' reliability, revenues, and trust, leading to financial losses and even legal and compliance risks. During the past five years (2019–2023), the Internet Crime Complaint Center (IC3) has received an average of 758,000 cybercrime complaints annually, reflecting a consistent upward trend. The volume of reported incidents peaked at 880,418 in 2023, resulting in an estimated global financial loss of $12.5 billion [1]. This steady increase highlights the growing prevalence and impact of cybercrime worldwide.

The vulnerability to cyber threats does not depend on the size of the company: both multinationals and *Small and Medium Enterprises (SMEs)* are exposed to increasing risks. SMEs often do not have the same resources as large companies and may find it more difficult to defend themselves adequately against cyber attacks [2]. In 2021, 37% of Italian SMEs experienced at least one cyber attack, about ten percentage points higher than the European average [3]. The European Flash Eurobarometer [3] highlighted managerial hypocrisy, particularly in Italy, where 71% of corporate executives claim to be aware of cybercrime dangers, yet only 15% provide proper training to their personnel. The tendency is the same across all European countries. Developing a structured and systematic strategy for SMEs managers is necessary to improve cyber risk management, which is currently inefficient, particularly in Italy, which has the largest number of SMEs in Europe [4], making their protection fundamental as they form the backbone of the country's economic structure.

This paper presents the development of a Cybersecurity Maturity Assessment System tailored for SMEs. We begin by comparing the Italian National Framework for Cybersecurity and Data Protection (which we will call INFS)[5] written by the Research Center of Cyber Intelligence and Information Security at Sapienza University of Rome (CIS) and the National Interuniversity Consortium for Informatics (CINI), based on the NIST Cybersecurity Framework (CSF)[6], with the most recent version of

Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT
*Corresponding author.
†These authors contributed equally.
stefano.bistarelli@unipg.it (S. Bistarelli); sara.geoli@studenti.unipg.it (S. Geoli); chiara.luchini@collaboratori.unipg.it (C. Luchini); ivan.mercanti@unipg.it (I. Mercanti)

the NIST CSF [7], released in February 2024. In Section 2, we address the main differences between the two frameworks and outline the National Methodology. Then follow Section 3 with the description of how the INFS can be enhanced by integrating significant updates from the NIST CSF version 2.0. Also, we focus on the methodological adjustments needed to adapt the scoring and maturity metrics offered by CIS and CINI [8], ensuring they are more accessible and practical for SMEs. Next, in Section 4, we describe the development of our Cybersecurity Assessment Tool designed to facilitate the adoption of the Assessment System. Furthermore, in Section 6, we analyze the current state of the art, highlighting existing approaches and emphasizing the significance of our contribution to cybersecurity maturity assessment for SMEs. Finally, in Section 7, we present our conclusions, summarizing key findings and outlining potential directions for future research.

2. Background on the two Frameworks and the Methodology

This section provides an overview of the key elements inherited by INFS from CSF, with a focus on the elements added in the Italian Framework and the National Methodology, which offers organizations a path to follow when applying the Framework to their "context and measure their cybersecurity posture" [8]. Then, we explain the main updates introduced in the most recent version of the NIST elaborated.

The INFS was published in 2015 by CIS and CINI [9], based on the 1.0 version of the CSF [10], which main goal was to protect critical infrastructure by providing a common organizational structure for different approaches to cybersecurity. To suit Italy's SME-driven economy, CSF v1.0 was readapted. Following the publication in 2018 of version 1.1 of the NIST Framework [6], the adoption of the General Data Protection Regulation (GDPR) in the Europan field, and the profound changes in the National cybersecurity landscape, the CIS updated the Framework to version 2.0 in 2019, renaming it National Framework for Cybersecurity and Data Protection [5]. Adapting and reprocessing the US Framework on national territory initiates an international alignment of cyber threat responses and enterprise cybersecurity management, allowing for an international cybersecurity dialogue [11].

The three main concepts inherited from the CSF in the INFS are Framework Core, Framework Profiles and Tiers, and are introduced the principles of Priority Levels, Maturity Levels and Contextualization.

The *Framework Core* includes industry standards, principles, and practices that help the organization to communicate cybersecurity efforts and results more effectively. It consists of five "concurrent and continuous" [6] functions: Identify, Protect, Detect, Respond and Recover. In a sequential view, the functions represent the life cycle of the organization's cyber risk management, from identifying critical assets and defining protective actions to implementing measures to detect, respond, and recover in the event of a cyber attack. Each function is organized hierarchically into Categories and Subcategories, with Informative References to guidelines, standards, GDPR legislation, and so on. The NIST defines *Tiers* that provide insight into the extent to which IT risk management processes are embedded within the organization. They are not maturity levels but inform risk management decisions, with four assessment levels: Partial, Informed, Repeatable, and Adaptive. More information on the Tiers levels can be found in [6]. Through the opportune selection of specific Subcategories from the Framework Core, organizations can create two *Profiles* tailored to their environment, applicability, and resources. The Current Profile includes all of the cybersecurity outcomes gathered to date, whereas the Target Profile comprises all desired goals. Comparing the obtained profiles may reveal a gap that has to be closed by developing a road map to follow.

One of the key elements introduced in the Italian Framework is the *Priority Levels*, which help enterprises prioritize interventions to bridge the gap between the Current Profile and Target Profile, focusing on the most risk-reducing measures. The goal is to identify essential Subcategories for immediate implementation based on risk mitigation (threat exposure, occurrence probability, and damage impact), costs, and measurable outcomes. The INFS defines three Priority Levels: Low, Medium, and High. A High value is assigned when implementing a Subcategory substantially reduces a cyber risk factor, regardless of cost. A Medium value indicates relatively low-cost risk reduction, while a

Low value applies when the cost is high and risk reduction is minimal. Since CSF Tiers are merely "visionary tools" [12] to help organizations understand cybersecurity risk management, the CSF does not offer mechanisms to measure implementation progress or improvements. To address this, the INFS introduces *Maturity Levels*, enabling organizations to globally evaluate security processes, technological implementations, and resource needs for each Subcategory. These levels must be incremental, and each SME defines them according to its requirements. The INFS also introduces *Contextualizations*, allowing Framework modulation based on sector, employee type, and territorial distribution. Contextualizations are created by selecting Subcategories from the Framework Core to form a new enterprise core. Each element of this core is then assigned a Priority Level and a Maturity Level. The 2015 [9] and 2019 [5] versions presented two contextualizations—one for Italian SMEs and one based on GDPR—which we will integrate into our Cybersecurity Assessment Tool.

To facilitate the adoption of the Framework and assess the extent to which current security measures meet the desired objectives, a National Methodology [8] was published in 2021. It defines three operational phases: *Contextualization, Measure, and Evaluation*, introducing the metrics of *Score* and *Maturity*. The initial phase of Contextualization consists in the selection of specific Subcategories with the corresponding level of Priority and Maturity, defining the new enterprise core. Contextualization prototypes can be used to facilitate and speed up the step. This selective process produces the desired Target Profile and establishes the foundation for the assessment. The consequent Measure phase analyzes the gap between the just-created Target Profile and the Current Profile defined through the administration of customized questionnaires by interviewers to SME's selected employees. The final phase of Evaluation, relying on the results of the precedent phase, evaluates the two profiles' distance from one another using the metrics of *Score* and *Maturity*. To understand the metrics, we first need to explain what a *scope* is. A scope is defined as a set $S = (E, W)$, where E is the collection of relevant assessment elements and W is a matrix assigning relevance values w_{ij} in $[0, 1]$ to each control in the Target Profile. The Score indicates the degree of implementation of an element in E, ranging from 0 to 1. It is calculated by comparing the implementation level (coverage value in [0,1]) of each control in the Current Profile with the Target Profile, weighted by the W matrix. The Maturity metric is expressed as a five-element vector m_j, where each component $m_j[k]$ reflects the proportion of controls implemented at maturity level k (ranging from 0 to 5, based on the CMMI scale[1]), weighted by the W matrix. Each vector value is derived from the maturity level of each control within the Subcategory. Further details are available in [8].

The NIST Framework 2.0, published in February 2024, has expanded its focus beyond critical infrastructures to include organizations of all sizes and sectors [7]. The Framework aims to "enhance risk management by providing a flexible, comprehensive framework for organizations to strengthen their cybersecurity posture and adapt to evolving threats"[7]. To achieve this, NIST CSF 2.0 provides additional support through references to other frameworks [13, 14], online resources [15, 16, 17], useful implementation examples [18] and the Cybersecurity and Privacy Reference Tool (CPRT) [19], which acts as a centralized repository for managing datasets related to guidelines, standards, and informative references. In earlier versions, the five Functions segmented cyber risk management temporally: before (Identify and Protect), during (Detect), and after (Respond and Recover) [20]. However, with the addition of the new central *Govern* function, each element is now integrated and interconnected, emphasizing a unified and coordinated approach to cybersecurity risk management.

Governance in NIST CSF 2.0 aligns cybersecurity with organizational goals, focusing on strategic oversight, roles, policies, and accountability. This elevates cybersecurity as a critical business risk, engaging executive leadership and embedding decision-making within risk management strategies [21, 22]. The Govern function introduces ten Subcategories for *supply chain risk management* (*SCRM*) to address complex third-party ecosystems. These Subcategories promote supplier security standards and continuous monitoring, fostering resilience and proactive collaboration with supply partners [7, 23].

[1]CMMI: https://cmmiinstitute.com/learning/appraisals/levels.

3. Our Cybersecurity Maturity Assessment System

Now, we present our Cybersecurity Maturity Assessment System, a reinterpretation of the phases of the National Methodology [8] that adapts its metrics. This system is built upon our newly developed Framework Core. To develop our system we revised the phases of Contextualization, Measure and Evaluation in [8].

In the initial Contextualization phase of the original Methodology, organizations are permitted to define their own Priority and Maturity Levels. However, these are predetermined to ensure a consistent and robust framework, enabling meaningful comparisons among different SMEs that apply the same contextualization. In this phase, a set of Subcategories must be selected, along with each level of Priority and Maturity to create the Target Profile. Three are the possible Priority Levels: Low, Medium and High, according to what is defined in [5]; while the Maturity Levels are five: Initial, Repeatable, Defined, Managed and Optimised, like the ones exposed as example in [8].

The subsequent Metrics phase generates the Current Profile. To have a more automated, concise, and streamlined process for defining the Profile in question, instead of creating and administering a customized questionnaire to the company's employees (like in the official Methodology), we assess the Coverage Grade and Maturity Level of each control through the compilation of a form. The Coverage Grade is determined by selecting a value between 0 and 1, while the Maturity Level is chosen from a range of 0 to 5, following the previously defined scales. The selection must be done by minimum competing selected employees in cybersecurity matters.

Finally, the metrics of Score and Maturity calculated in the third and last phase of Evaluation are reformulated according to the redefinition of scope, to grant a more general and linear approach. These metrics are essential to the organization to obtain a quantitative analysis on their cyber risk management based on the goal defined in the Target Profile. The element E and W in the scope $A = (E, W)$, are redefined as follows.

- The set of components in E matches in each assessment all of the controls contained in the contextualization C generated during the initial Contextualization phase. The set E has cardinality 1, as it contains only one element (e) that represents all n controls in the contextualization C.
- The weight assigned to each control in the scope (equal to all those contained in contextualization C) is uniform, i.e. 1. As a result, the weight matrix W has a value of one at each position w_{ij}. The matrix W assumes a vector form, with each member w_i having a value of 1.

Therefore, in Equation 1 can be seen the updated metric of Score where x_i^A is the Current Coverage of the i-th control in the Current Profile, x_i^T is the desired Coverage of the i-th control in the Target Profile and n is the total number of controls in the contextualization.

$$score(e) = \frac{\sum_{i=1}^{n}(x_i^A / x_i^T)}{n} \tag{1}$$

While in Equation 2 is reported the Maturity metric where $L_k(C)$ represents the set of controls in the Target Profile to which have been assigned a Maturity Level in the Current Profile.

$$m_e[k] = \frac{\sum_{i \in L_k(C)} 1}{n} \tag{2}$$

The final evaluation, using the indicated metrics and a broader scope, offers a comprehensive assessment for SMEs using the Framework. It compares the organization's IT security posture to the Target Profile without requiring detailed or excessive specialized knowledge. Closing the gap between the Current and Target Profiles simply involves assessing the actions taken and, if necessary, redefining them. Thus, the revised Methodology shown in Figure 1 provides a more extensive yet equally effective approach, giving the organization a clear view of its cyber threat management.

Aligning the Italian Framework Core with the key updates in CSF v.2.0 is indispensable, especially given the expanded emphasis on governance and the increased focus on securing the supply chain. Our

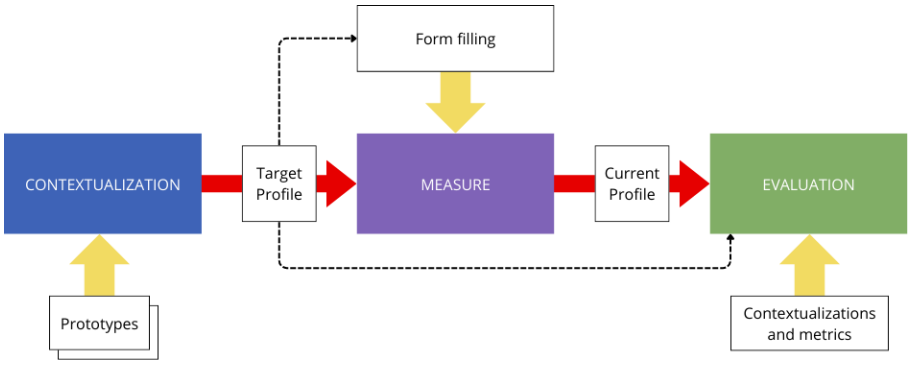


Figure 1: Our Methodology.

new Framework Core has *six* Functions: Govern and Identify from the NIST Core and Protect, Detect, Respond and Recover from the Italian one. Therefore, it is an aggregate (with appropriate adjustment) of the following elements:

- The Italian Framework Core exposed in [5].
- The new function Govern (GV) added in [6] and the relative amendments of the function Identify (ID).
- The implementation examples [18] provided with the CSF updates.

It is worth noting that changes were also made to the other Functions in the CSF v.2.0. However, we deemed them minor, and it was considered essential to avoid extensive modifications to the National Core Framework, as it had been specifically tailored to the Italian socio-cultural context by expert institutions.

Functions	Category	Subcategory	Priority Level	Coverage Grade	Maturity Levels	Informative References	Implementation Examples
GOVERN (GV)							
IDENTIFY (ID)							
PROTECT (PR)							
DETECT (DE)							
RESPOND (RS)							
RECOVER (RC)							

Figure 2: Our Framework Core.

Figure 2 shows the structure of our new Framework Core, which consists of the six Functions. Each Function is divided into Categories and Subcategories. For each Subcategory, must be chosen the Priority Level, the Coverage Grade, and the Maturity Level. Additionally, Informative References and implementation Examples are provided to assist in the process. Furthermore, our evaluation system provides organizations with the contextualization prototypes below as a starting point for initiating the assessment.

- GDPR: A set of controls introduced in the 2019 update of the Framework [5], following the enactment of the General Data Protection Regulation (GDPR), which are considered essential for ensuring proper compliance.
- Essential Controls: A set of basic and fundamental controls for minimal cyber risk management in Italian SMEs, outlined in the report [24] published in 2016 by the same institutions that developed the National Framework.
- Italian SMEs: A set of controls that a typical SME should consider to improve its cybersecurity posture, provided as an example of contextualization in the first version of the Italian Framework [9].
- Italian Public Administration (PA): A set of controls chosen from the INFS generated by the Municipality of Marsciano (Perugia, Italy) in 2018 for local public administration with less than 20.000 inhabitants.
- US SMEs: A set of controls outlined in the Small Business Quick-Start Guide [25], developed by NIST in 2024, specifically for small businesses with minimal or no cybersecurity plans. It references key materials, such as a guide on securing supply chains to manage associated risks [26], the Cyber Resilience Review (CRR) by CISA [27] for assessing and improving operational resilience, and a collection of cybersecurity training resources offering practical education on mitigating cyber threats [28]. Together, these tools support SMEs in strengthening their cybersecurity practices and risk management strategies.

4. Our Cybersecurity Assessment Tool

To facilitate the use of our Cybersecurity Maturity Assessment System, we developed a user-friendly web application, referred to as the *Cybersecurity Assessment Tool*. This tool is designed to streamline the assessment process, enabling users to evaluate their cybersecurity practices and determine their maturity level efficiently. We implemented a RESTful application using Flask [2], a lightweight and flexible Python [3] web framework. To manage the large volume of data associated with our new Framework Core, the official ones and the contextualizations, we chose MariaDB [4] as the relational database management system. The Tool requires registration to be used and handles two kinds of profiles: *Administrator* and *Base User*.

The Administrator must be a qualified individual capable of assessing the cybersecurity needs of the SMEs they work with. After registering, the administrator gains access to a personal area where they can perform various tasks, including: creating Base Users, viewing registered Base Users, developing contextualizations from predefined prototypes or Framework Cores (either ours or official), compiling them with Priority Levels, target Coverage Grades and target Maturity Levels generating the Target Profile, and reviewing both the created contextualizations and the cybersecurity Assessment Reports generated by each user.

A Base User can only be registered in the Tool by an Administrator. Users can access the contextualizations assigned by the administrator and individually complete each one, contributing to the development of the relative Current Profile. These contextualizations can be modified or updated as needed, ensuring the profile remains dynamic and accurate over time. Upon completion, users can view the corresponding Cybersecurity Assessment Report to evaluate their cybersecurity posture. In case of any issues or questions, users can access the informational references of the administrator who created their profile.

The contextualization page of our tool is shown in Figure 3. It features the same structure for both the Administrator and Base User. However, the Administrator can select also the Priority Level, for each Subcategory, in addition to the Coverage Grade and Maturity Levels. It is important to note that the interface is currently in Italian; future enhancements should include an English option to

[2]Flask: https://flask.palletsprojects.com/en/3.0.x/
[3]Python: https://www.python.org/
[4]MariaDB: https://mariadb.org/

Subcategory	Priority Level	Coverage Grade (*Current* Profile)	Maturity Level (*Current* Profile)	Coverage Grade (*Target* Profile)	Maturity Level (*Target* Profile)
PR.DS-2, Data are protected during transmission.	High	0.4 - Initial	4 - Managed	0.8 - Advanced	5 - Optimized

Table 1
Compilation example of Subcategory *PR.DS-2* in a contextualization.

expand usability. Once the contextualization process is complete—the Target Profile is defined by the Administrator and the Current Profile by the Base User—each included Subcategory adopts the structure illustrated in Table 1. The table highlights how the Coverage Grade and Maturity Level apply to both the Target and Current Profiles. These values are critical for calculating key metrics such as Score and Maturity, which are presented in the final report. By analyzing these metrics, the gap between the two profiles becomes evident, providing a clear understanding of the progression needed to align the Current Profile with the Target objectives.

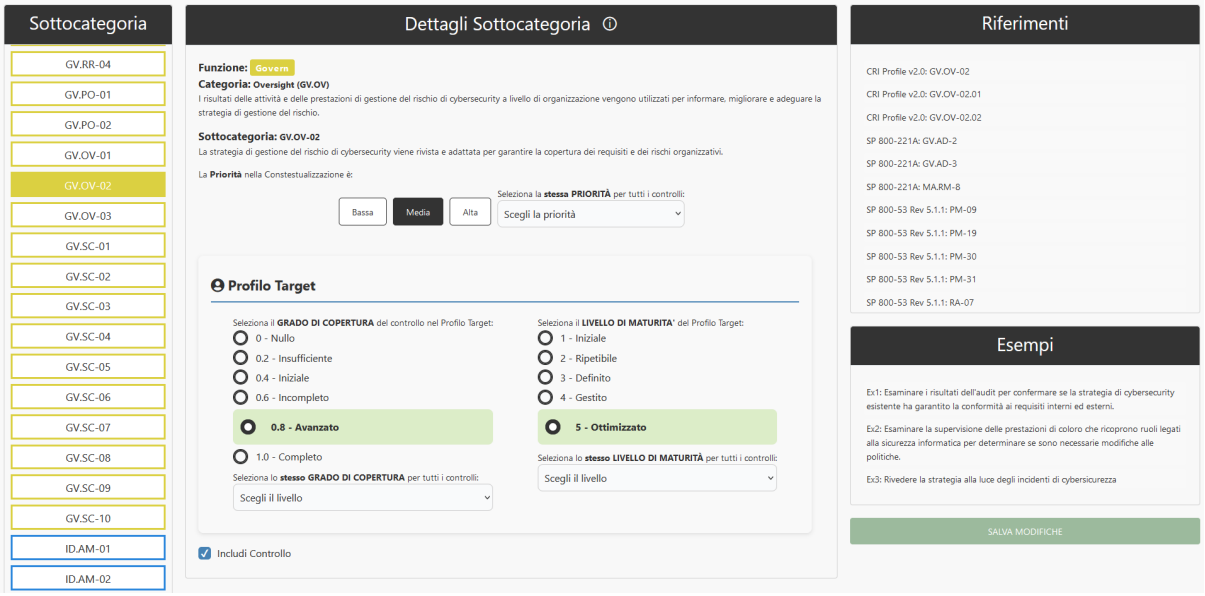


Figure 3: Administrator main interface.

5. Cybersecurity Assessment Report

The Cybersecurity Assessment Report is structured into three main sections. The first section focuses on analyzing the Score. A table is presented, listing the Coverage Grade for each Subcategory within both the Target and Current Profiles. To visually represent the percentage Score, a horizontal bar chart is displayed, as shown in Figure 4. In the provided example, we observe that only 39.71% of the required controls are currently implemented, as compared to the total objective defined in the Target Profile. This indicates that less than half of the expected controls have been developed to date.

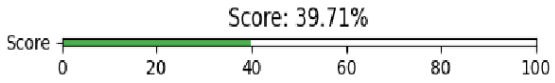


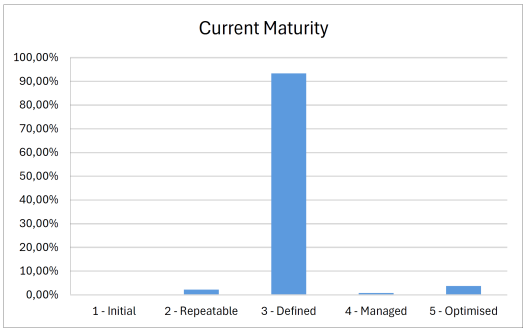
Figure 4: Graphical representation of Score Metric.

The following section of the report presents the calculated Maturity. As in the previous section, it includes a summary table of the Maturity values for each Subcategory in both the Current and Target Profiles within the contextualization. Two separate tables are provided—one for the Current Profile and one for the Target Profile—along with their corresponding column charts (see Figure 5). The Maturity percentage values, as illustrated in Figure 6, show that the majority of controls (93.38%) are currently implemented with a Maturity Level of *3 - Defined* (Figure 6a). However, the objective is to achieve a *5 - Optimised* level for 97.79% of controls (Figure 6b). To identify which controls require more immediate attention, a table has also been included that ranks the Subcategories by Priority Level.

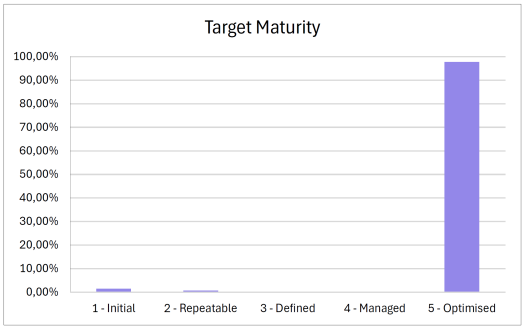
Scale	Current Maturity
1 - Initial	0,00%
2 - Repeatable	2,21%
3 - Defined	93,38%
4 - Managed	0,74%
5 - Optimised	3,68%

Scale	Target Maturity
1 - Initial	1,47%
2 - Repeatable	0,74%
3 - Defined	0,00%
4 - Managed	0,00%
5 - Optimised	97,79%

Figure 5: Table Current and Target Maturity.



(a) Column chart Current Maturity.



(b) Column chart Target Maturity.

Figure 6: Column chart Current and Target Maturity.

6. Related Work

A range of cybersecurity assessment models have been developed to strengthen organizations' ability to measure their cybersecurity maturity. These models typically adapt established frameworks, such as the NIST Cybersecurity Framework (CSF), to meet the specific requirements of SMEs.

Indeed, the Information Security Maturity Model (ISMM) [12] proposes a mechanism to track the implementation of NIST CSF using a five-level maturity scale across 23 assessed areas. While ISMM improves on NIST's Tiers, it is not designed specifically for SMEs and lacks a tool for accessible implementation, limiting its practical use in resource-constrained environments. In contrast, the Methodology we proposed is easily accessible through the Cybersecurity Assessment Tool, encouraging even the most time-poor managers to adopt our Maturity Assessment System. Another notable contribution is the Risk Management Framework for SMEs presented by Nasir et al. [29]. This framework integrates a lightweight approach to risk management, emphasizing practicality and cost-effectiveness, essencial for SMEs with limited resources. However, it does not directly incorporate the latest updates from the NIST CSF, making it less aligned with evolving international standards. In our System, contextualization can be created from various Framework Cores, included the created one based on the NIST updates and the National Framework.

Additionally, numerous cybersecurity tools have been introduced to assist SMEs in evaluating and improving their security protocols, streamlining the assessment process and ensuring efficiency for organizations with limited resources. For instance, the Cybersecurity Evaluation Tool (CET) [30] simplifies cybersecurity assessment for SMEs by evaluating only 35 of the 96 NIST CSF controls. It produces a report card with recommendations when gaps are detected. Although CET is user-friendly, it lacks the flexibility to customize assessments based on the unique needs of individual SMEs, as it uses a static subset of controls for all users. Indeed, to accommodate a broader audience and guarantee a high degree of applicability, different contextualization prototypes are available in our Tool. Furthermore, Armenia et al. [31] make a significant additional contribution by addressing the dynamic nature of cybersecurity risks with the introduction of the SME Cyber Risk Assessment (SMECRA) tool. SMECRA identifies an organization's evolving cybersecurity risk profile, offering continuous evaluation and enabling SMEs to adjust their cybersecurity strategies dynamically. This approach emphasizes adaptability, which is essential for organizations facing ever-changing threats. However, as highlighted in the work of Nasir et al. [29], SMECRA does not integrate the latest updates to the CSF, making it less aligned with the current version of the framework.

7. Conclusion

This study presents the development of a Cybersecurity Maturity Assessment System designed to meet the specific needs of SMEs. By synthesizing key components from the INFS, the CSF versions 1.1 and 2.0, and the National Methodology [5, 6, 7, 8], a refined Framework Core was constructed. This core integrates updates introduced in NIST CSF 2.0 (February 2024) and adapts them to the national context, addressing the gap created by the delayed update of the National Framework. The revised Score and Maturity metrics offer a comprehensive and comparable approach to evaluating cybersecurity risk management practices in SMEs over time. The development of the Cybersecurity Assessment Tool provides a user-friendly interface that guides users through main stages of cybersecurity risk management. The tool facilitates the definition of a Target Profile by expert administrators, the completion of a Current Profile by designated users, and the generation of a Cybersecurity Assessment Report. This report plays a central role in determining the necessary measures to enhance cybersecurity, assess existing controls, and evaluate progress toward achieving cybersecurity objectives.

Future improvements could focus on expanding the integration of updates to encompass additional Subcategories of the NIST Cybersecurity Framework (CSF) beyond the Identify function. Refining the assessment process by developing a customized questionnaire could enhance the precision of coverage and maturity evaluations. Furthermore, automating the response analysis and incorporating a messaging feature to facilitate communication between administrators and users could significantly enhance the tool's usability and overall effectiveness.

Acknowledgments

The authors are member of the INdAM Research group GNCS and of Consorzio CINI. This work has been partially supported by:

- GNCS-INdAM, CUP_E53C23001670001;
- MUR project PRIN 2022TXPK39 - PNRR M4.C2.1.1. "Empowering Public Interest Communication with Argumentation (EPICA)'' CUP H53D23003660006, funded by the European Union - Next Generation EU, Missione 4 Componente 1;
- MUR PNRR project SERICS (PE00000014), funded by the European Union – Next Generation EU;
- EU MUR PNRR project VITALITY (J97G22000170005), funded by the European Union – Next Generation EU;
- University of Perugia - Fondo Ricerca di Ateneo (2020, 2022) – Projects FICO, BLOCKCHAIN4FOODCHAIN, RATIONALISTS, "Civil Safety and Security for Society'';

- Piano Sviluppo e Coesione Salute PSC 2014-2020 - Project I83C22001350001 LIFE: “the itaLian system wIde Frailty nEtwork’’ Linea di azione 2.1 “Creazione di una rete nazionale per le malattie ad alto impatto’’ - Traiettoria 2 “E-Health, diagnostica avanzata, medical devices e mini invasività’’ Codice locale progetto T2-AN-12 CUP J93C22001080001.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT and Grammarly in order to: Grammar and spelling check, Text Translation, Paraphrase and reword and Citation management. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the publication’s content.

References

[1] Internet Crime Complaint Center, Internet Crime Complaint Center Internet Crime Report 2023, Technical Report, Federal Bureau of Investigation, 2023. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. doi:10.1234/ic3.2023.report.

[2] A. Horn, Why cybersecurity should be a top concern for middle-market companies, SmallBizDaily, 2017. URL: https://www.smallbizdaily.com/cybersecurity-middle-market-companies/.

[3] European Commission, Flash Eurobarometer 496: SMEs and Cybercrime Report, Technical Report, European Commission, 2022. URL: https://data.europa.eu/en/euridice/publications/flash-eurobarometer-496-smes-and-cybercrime-report. doi:10.2837/14988.

[4] Statista, Number of SMEs in Europe by Country, 2023. URL: https://www.statista.com/statistics/558308/smes-in-europe-by-country/.

[5] M. Angelini, C. Ciccotelli, L. Franchina, A. M. Spaccamela, L. Querzoni, Framework Nazionale per la CyberSecurity e la Data Protection, CIS Sapienza, Laboratorio Nazionale di Cybersecurity, Consorzio Interuniversitario Nazionale per l’Informatica (CINI), 2019. URL: https://www.cybersecurityframework.it.

[6] N. I. of Standards, T. (NIST), Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1, National Institute of Standards and Technology (NIST), 2018. URL: https://doi.org/10.6028/NIST.CSWP.04162018. doi:10.6028/NIST.CSWP.04162018.

[7] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/NIST.CSWP.29. doi:10.6028/NIST.CSWP.29.

[8] M. Angelini, A. Bruttini, C. Ciccotelli, A. Lucariello, L. Franchina, L. Querzoni, F. Ressa, Metodologia per il cybersecurity assessment con il Framework Nazionale per la Cybersecurity e la Data Protection, CIS Sapienza, Laboratorio Nazionale di Cybersecurity, Consorzio Interuniversitario Nazionale per l’Informatica (CINI), 2019. URL: https://www.cybersecurityframework.it/sites/default/files/2019-09/Metodologia_v1.0.pdf.

[9] R. Baldoni, L. Montanari, 2015 Italian Cyber Security Report, CIS Sapienza, Laboratorio Nazionale di Cybersecurity, Consorzio Interuniversitario Nazionale per l’Informatica (CINI), 2016. URL: https://www.cybersecurityframework.it.

[10] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0), National Institute of Standards and Technology, 2014. URL: http://www.nist.gov/cyberframework/.

[11] S. J. Shackelford, S. Russell, J. Haut, Bottoms up: A comparison of ”voluntary” cybersecurity frameworks, UC Davis Business Law Journal (2015). URL: https://ssrn.com/abstract=2702039.

[12] S. Almuhammadi, M. Alsaleh, Information security maturity model for nist cyber security framework, in: International Conference on Industrial Technology, 2017. URL: https://api.semanticscholar.org/CorpusID:51802617.

[13] National Institute of Standards and Technology, The NIST Privacy Framework: A Tool for

Improving Privacy through Enterprise Risk Management, Technical Report, National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/NIST.CSWP.01162020. doi:10.6028/NIST.CSWP.01162020.
[14] National Institute of Standards and Technology, Integrating Cybersecurity and Enterprise Risk Management (ERM) (NIST IR 8286), Technical Report, U.S. Department of Commerce, 2020. URL: https://doi.org/10.6028/NIST.IR.8286. doi:10.6028/NIST.IR.8286.
[15] NIST, Quick Start Guides for the NIST Cybersecurity Framework, 2023. URL: https://www.nist.gov/quick-start-guides.
[16] National Institute of Standards and Technology (NIST), CSF 2.0 Informative References, 2023. URL: https://www.nist.gov/informative-references.
[17] National Institute of Standards and Technology (NIST), CSF 2.0 Profiles, 2023. URL: https://www.nist.gov/profiles-0.
[18] National Institute of Standards and Technology, CSF 2.0 Implementations Examples, Technical Report, National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/document/csf-20-implementations-pdf.
[19] National Institute of Standards and Technology (NIST), Cybersecurity and Privacy Reference Tool (CPRT), 2024. URL: https://csrc.nist.gov/projects/cprt.
[20] Cybersecurity360, NIST Cybersecurity Framework 2.0: Cambia lo standard della cyber security, ecco come, 2024. URL: https://www.cybersecurity360.it/soluzioni-aziendali/nist-cybersecurity-framework-2-0-cambia-lo-standard-della-cyber-security-ecco-come/.
[21] ISC2, 5 Things to Know Now about NIST CSF 2.0, 2024. URL: https://www.isc2.org.
[22] L. Security, NIST CSF 2.0: Key Updates and Their Impact, 2023. URL: https://lmgsecurity.com/nist-csf-2-0.
[23] Nuspire, NIST CSF 2.0: Changes and Implications, 2023. URL: https://www.nuspire.com.
[24] S. Armenia, R. Baldoni, C. Biancotti, C. Carlini, F. d'Amore, L. Franchina, M. K. Mariam, L. Montanari, L. Querzoni, L. Russo, F. Ruzzi, M. Spada, E. Spagnoli, A. Vitale, Controlli Essenziali di Cybersecurity, Technical Report, CIS Sapienza, Laboratorio Nazionale di Cybersecurity, Consorzio Interuniversitario Nazionale per l'Informatica (CINI), 2017. URL: https://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf.
[25] N. I. of Standards, T. (NIST), Small Business Cybersecurity Quick-Start Guide, NIST Special Publication, 2021. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02162023.pdf.
[26] Cybersecurity and Infrastructure Security Agency (CISA), Securing SMB Supply Chains: Resource Handbook, U.S. Department of Homeland Security, 2023. URL: https://www.cisa.gov/sites/default/files/2023-01/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf.
[27] Cybersecurity and Infrastructure Security Agency (CISA), Cyber Resilience Review (CRR), U.S. Department of Homeland Security, 2023. URL: https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr.
[28] National Institute of Standards and Technology (NIST), Small Business Cybersecurity: Online Training Resources, U.S. Department of Commerce, 2023. URL: https://www.nist.gov/itl/smallbusinesscyber/training.
[29] A. Emer, M. Unterhofer, E. Rauch, A cybersecurity assessment model for small and medium-sized enterprises, IEEE Engineering Management Review 49 (2021) 98–109. doi:10.1109/EMR.2021.3078077.
[30] M. Benz, D. Chatterjee, Calculated risk? a cybersecurity evaluation tool for smes, Business Horizons 63 (2020) 531–540. URL: https://www.sciencedirect.com/science/article/pii/S0007681320300392. doi:10.1016/j.bushor.2020.03.010.
[31] S. Armenia, M. Angelini, F. Nonino, G. Palombi, M. F. Schlitzer, A dynamic simulation approach to support the evaluation of cyber risks and security investments in smes, Decision Support Systems 147 (2021) 113580. URL: https://www.sciencedirect.com/science/article/pii/S0167923621000907. doi:10.1016/j.dss.2021.113580.