OT Cyber Security Frameworks Comparison Tool (CSFCTool)

G. Mùrino[1], M. Ribaudo[1], S. P. Romano[2] and A. Tacchella[1]

[1]DIBRIS, Università degli Studi di Genova, Italy
[2]DIETI, Università degli Studi di Napoli Federico II, Italy

Abstract

This paper proposes a holistic cybersecurity online tool to support implementation activities of the *"National Framework for Cybersecurity & Data Protection"*, one of its contextualizations, as well as the fifteen *"Essential Cybersecurity Controls"*. It also aims at promoting its wide dissemination by SMEs. All the regulations, standards and national/international laws mentioned as *"Informative References"* for each Subcategory in the Framework Core are, in fact, made available through a web application where they can be consulted with a few clicks, guiding even less experienced users in the creation of their cybersecurity compliance projects.

The research and analysis activities conducted with a systematic, global and conceptual approach - consistent with the original document - have been aimed at highlighting the substantial differences between IT/OT cybersecurity requirements in order to increase, through a comparative analysis, the cyber resilience of national critical infrastructures.

Meanwhile, since an important step towards cyberspace security is a global increase in the level of cyber risk awareness, the tool aims to be used for education and training programs too, both at the corporate and academic levels, in order to bridge the skills gap in the job market between job seekers and employers. For this purpose, some of the main reference standards used for auditing, vulnerability assessment and risk management activities have been included.

Keywords

Legal aspects and compliance tool, cyber education and training tool, cyber risk awareness, National Framework for Cybersecurity & Data Protection, Data security and Privacy, Operational Technology, Critical Infrastructures security.

1. Introduction

The publication of Presidential Policy Directive 21 (PPD-21/2013) [1] commissioned by past U.S. President Barack Obama, introduced the concept of resilience as *"the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents"*, which was used to coin the new term of cyber-resilience as *"the ability to continuously deliver the intended outcome despite adverse cyber events"* [2].

ITASEC'21, Italian Conference on Cybersecurity, April 7-9, 2021
giuseppina.murino@edu.unige.it (G. Mùrino); marina.ribaudo@unige.it (M. Ribaudo); spromano@unina.it (S. P. Romano); armando.tacchella@unige.it (A. Tacchella)
0000-0003-0820-983X (G. Mùrino); 0000-0003-0697-2225 (M. Ribaudo); 0000-0002-5876-0382 (S. P. Romano); 0000-0001-9487-331X (A. Tacchella)

To better address these risks, the Cybersecurity Enhancement Act of 2014[1] (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include, identify and develop cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. More specifically, the goal was *"...to identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks"*. This formalized NIST's previous work developing Framework Version 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity"[2] (February, 2013), and provided guidance for the future evolution of the Framework up to the release of version 1.1 (April, 2018).

Meanwhile, at national level, as illustrated in Figure 1, the joint activities of the Cyber Intelligence and Information Security Center (CIS) at Sapienza University of Rome and the Cyber Security National Lab (CINI), led to the publication of the "National Framework for Cyber Security" (version 1.0, 2015) [3] which was followed in 2016 by the publication of the "Essential Cyber Security Controls" [4], until the publication in 2019 of version 2.0 of the "National Framework for Cybersecurity and Data Protection" (FNCS&DP) [5] which integrates the national implementation of EU Regulation 2016/679 (GDPR) on personal data protection.

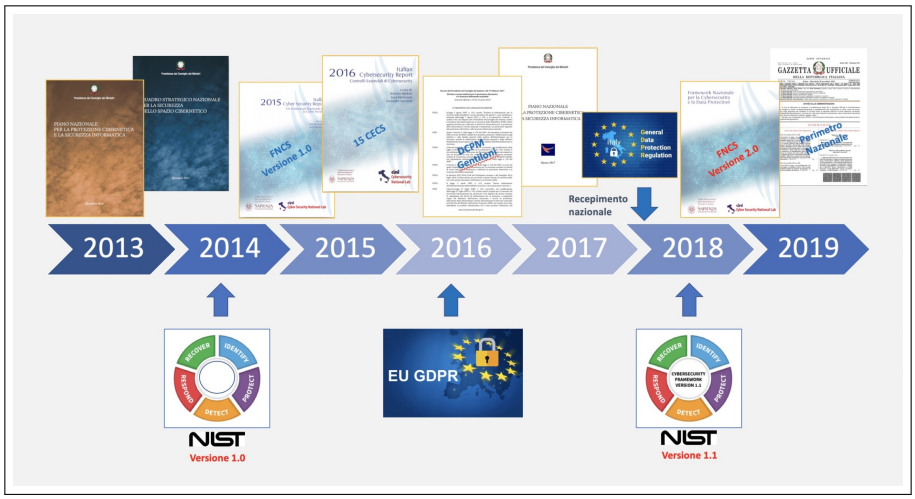

Figure 1: National Framework timeline evolution

As per the NIST Framework, from which our National Framework is derived, the Framework Core includes an *Informative References* section that provides specific standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each *Subcategory*.

Compared to the list initially provided by NIST, the National Framework versions have been extended to national reference laws and regulations (including transposition decrees of EU directives).

[1] https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[2] https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

The use of Informative References is non-compulsory for the implementation of the National Framework. Organizations have the flexibility to mix and match Informative References as best suits their needs. They may use all, some, none, or even choose to map additional practices not included in the Informative References catalog. While this, on the one hand, represents an advantage to the application of the National Framework, on the other hand it represents a major problem for SMEs facing further difficulties as they often do not have the skills and/or economic resources necessary to cope with this complexity.

Having in mind this scenario, this work proposes a web-based tool which has three main objectives:

1. Providing personnel involved in cybersecurity activities with an automatic consultation and design tool able to support their choices based on a selection of documents that are quickly accessible and constantly updated, saving research and selection time in the *mare magnum* of national and international Informative References currently existing.

2. Pointing out the security requirements substantial differences in an Operational Technology (OT) vs Information Technology (IT) environment.

3. Providing a self-learning support for training, at both corporate and academic level, in order to standardize the required cybersecurity best practises and skills.

The paper is organised as follows: in Section 2 we present some related work, while in Section 3 we describe the objectives of the proposed framework. In Section 4 we briefly describe the architecture of the current proof-of-concept and its main functionalities. Finally, Section 5 concludes this work presenting possible future extensions.

2. Related Work

The adoption of a cybersecurity framework may represent a best practice and a way to demonstrate that the organization adopted a well-grounded duty of care. This represents an important step to properly face fines and the legal liability of lawsuits [6].

Unfortunately, nowadays this is no longer enough. The digital transformation of society (intensified by the COVID-19 crisis) has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses to avoid that any disruption, even those initially confined to just one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market, as underlined in the recent EU Proposal for NIS 2.0 (December, 2020)[3].

A significant change of pace is required to rapidly increase cybersecurity awareness overall in SMEs [7]. A change which can only go through a digitization of the tools provided to support this activity. In this sense, a confirmation is also provided by the american NIST which, by publishing its NIST SP $800-53$ rev.5, declares that *"...In the near future, NIST also plans to offer the content*

[3]https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

of SP $800-53$*, SP* $800-53A$*, and SP* $800-53B$ *to a web-based portal to provide its customers interactive, online access to all control, control baseline, overlay, and assessment information"* [8].

In this context, another key element is is represented by the IT/OT convergence. The advent of the 4^{th} industrial revolution, also known as Industry 4.0, introduced cyber-physical systems. Industrial Control Systems (ICS) - such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) - introduced by the third industrial revolution to support and improve operational activity in the industrial sector and in critical infrastructures, traditionally "closed" to the outside world, have been connected to the Internet with unavoidable serious consequences deriving from the need to integrate the Operational Technology (OT) world, on the one hand, with that of Information Technology (IT) on the other hand. The convergence point between these two distinct worlds is a figurative "red dot" that represents the weak point of the entire system.

This new trend in industry to let IT and OT systems converge comes from the need to access real time data and to interconnect all facilities in order to enhance productivity/production. The convergence is driven by the need to obtain quantitative management reporting, assisted by big data and sensor technology, artificial intelligence, physical automation, remote operations, cloud computing, analytics [9]. This requires operators to increase network connectivity and access to both IT and OT systems using Ethernet, Wi-Fi and TCP/IP standards [10] with consequent new challenges to be faced (e.g., network performance considerations related to different latency, jitter, bandwidth and throughput between IT/OT protocols [11]).

Finally, as reported by ENISA *"CyberSecurity Skills development in the EU"*[4] report, published in December 2019, the cybersecurity skills shortage, which refers to the lack of qualified cybersecurity professionals in the labour market [12], represents an issue for both economic development and national security, especially in the rapid digitization of the global economy. It poses threats with a high impact on the data, information technology systems and networks that form the dorsal spine of modern societies.

This skills shortage can be further analysed into two concurrent issues: a *quantitative* one and a *qualitative* one. The quantitative issue is related to the insufficient supply of cybersecurity professionals to meet the requirements of the job market; the qualitative one is related to the inadequacy of professional skills to meet market needs. This report focuses on the status of the cybersecurity education system and its inability to attract more students in the field of cybersecurity. It argues that many of the current issues in cybersecurity education could be ameliorated by redesigning educational and training pathways that define knowledge and skills that students should possess upon graduation and after entering the labour market.

Different causes might be attributed to the skills shortage[5], credited with issues in the workplace or in the education and training system. Two elements that compound the shortage can be attributed to employers or, more generally, to the labour market:

1. The high expectations that employers have about the skill level of candidates that the current labour market can offer.

2. The lack of sufficient and suitable training provided to employees.

[4] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
[5] https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/

The cybersecurity job market is relatively immature and very dynamic, and the job specifications are highly dependent on the organisation size and sector. ENISA report emphasizes that *"...Small and Medium-sized enterprises not specialised in job security tend to prefer generalist IT staff with some understanding of cybersecurity, whereas larger firms and firms specialised in cybersecurity have need of specialised staff focused on one of the sub-disciplines of cybersecurity"*.

Concerning tools availability, to the best of the authors' knowledge, there is no tool featuring the same capabilities as the one proposed in this paper. While several automated tools are available to support technical auditing tasks (i.e., information gathering, penetration, exploitation, forensics [13]) or to support cybersecurity learning activities [14], none is able to simultaneously offer support to regulatory compliance, starting from our FNCS & DP, highlighting differences in OT vs IT worlds. Last but not least, our tool follows up previous proposals (i.e., Cyber Security Framework Tool[6], CRUMBS [15]) intended to disseminate the National Framework.

3. Cyber Security Framework Comparison Tool

As anticipated in Section 1, we present in this section the Cyber Security Framework Comparison Tool (abbreviated with CSFCTool in the following). We first illustrate the implementation of the three main project objectives. Then, we briefly describe the architecture of the tool and some of its main functions.

3.1. Objective 1: Simplifying the use of the National Framework by SMEs

The CSFCTool is based on the assumption that the aforementioned National Framework (in all its versions), for each identified Subcategory, proposes a list of corresponding *Informative References* (see Figure 2), e.g., a list of specific national/international standards, regulations or laws to refer to in order to achieve the outcomes associated with the selected Subcategory.

Appendice A. Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	**ID.AM-1:** Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 1
		ID.AM-2: Sono censite le piattaforme e le applicazioni software in uso nell'organizzazione	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5 · **Misure Minime AgID** ABSC 2
		ID.AM-3: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 · **Misure Minime AgID** ABSC 5.1.4, 13.3.1, 13.4.1, 13.6, 13.7.1, 13.8.1

Figure 2: *Informative References* section example

[6] http://tool.cybersecurityframework.it

The adoption of cybersecurity standards is often a technical challenge for SMEs, where the staff involved in cybersecurity assessment activities has to face daily overlapping of roles, shortage of time, and training gaps or inadequate skills.

The first objective of CSFCTool can be reached thanks to the adoption of four phases, detailed below, which correspond to as many steps within the security assessment process.

- **Step 1 - Automate security assessment activities**
  Through direct access to the consultation of all national/international standards, regulations and law articles listed in correspondence with each selected Subcategory, the CSFCTool allows to automate the use of the National Framework for Cybersecurity and Data Protection (FNCS&DP), one of its contextualization or fifteen Essential Cybersecurity Controls (CEC) in a simple, clear and fast way.

- **Step 2 - Verify regulatory compliance**
  By creating an individual Portfolio, the CSFCTool allows each user to access the various projects created, verify and note their regulatory compliance with the aid of an interactive NOTES section associated with each Subcategory of a selected project.

- **Step 3 - Plan and manage all projects in a unique personal Portfolio**
  Using the CSFCTool users can quickly create projects with different *maturity levels* or *profiles*, collect them in their personal PORTFOLIO and manage them intelligently. In this way they will be able to plan and control the organization's *continuous improvement* in an easy way, always having under control the progress of all transition processes.

- **Step 4 - Save hours of design**
  Within the CSFCTool it is possible to access all national and international references related to the use of the National Framework and to understand their time allocation (and/or updates) in a few clicks. Staff will thus be able to save hours of work lost in collecting, selecting and understanding the rules to be used. For each reference, in fact, there is also a quick self-learning tutorial that can be easily consulted. Furthermore, all attached and linked documents are made available in downloadable format.

3.2. Objective 2: Identification of OT vs IT Cybersecurity requirements

The second main objective of CSFCTtool is to highlight the application differences between OT and IT cybersecurity requirements using the so-called CIA TRIAD paradigm based on *Confidentiality, Integrity* and *Availability* (as illustrated in Figure 3), to arise security of critical infrastructures by increasing the level of awareness of all personnel involved in their operations.

The process consists in a cross-mapping mechanism based on the use of NIST SP $800-82$ rev.2 *"Guide to Industrial Control Systems (ICS) Security"* [16] a document that provides guidance on how to secure ICS, including SCADA systems, DCS, and other control system configurations such as PLC, while addressing their unique performance, reliability, and safety requirements [17]. This document[7] includes (in Appendix G) an overlay based on NIST SP $800-53$ Rev.4 [19]. More specifically, Table G-1 provides a summary of the security controls and control enhancements

[7] Cited also in ECSO Guidelines [18] as reference for ICS in Industry 4.0

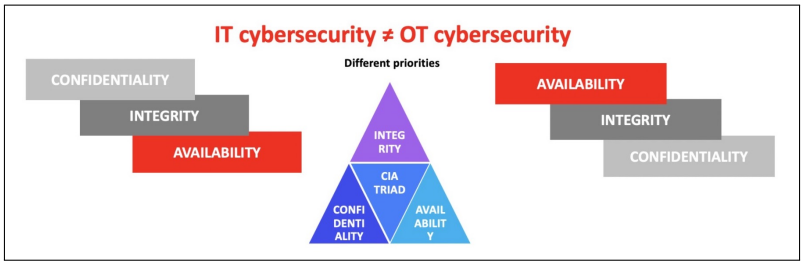

Figure 3: *CIA Triad paradigm* - OT vs IT priorities

from NIST SP 800 – 53 Appendix F that have been allocated to the initial security control baselines (i.e., *Low, Moderate*, and *High*) along with indications of ICS Supplemental Guidance and ICS tailoring. Controls and control enhancements for which there is ICS Supplemental Guidance are **bolded**. If the control baselines are supplemented by the addition of a control to the baseline, the control or control enhancement is underlined. If a control or control enhancement is removed from the baseline, the control or control enhancement is ~~struck out~~.

Example in Figure 4, compares initial control baseline values for NIST SP 800 – 53 rev.4 (above) vs NIST SP 800 – 8 rev.2 overlay (below). It is highlighted how an ICS Supplemental Guidance was added to Control Enhancement 1 of AU-4 (bolded). In addition, Control Enhancement 1 of AU-4 was added to the Low, Moderate and High baselines (underlined).

AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	Audit Storage Capacity	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**

Figure 4: NIST SP 800-82 rev.2 overlay for AU-4 Security Control

3.3. Objective 3: Training and self-training activities

Helping to bridge the skills gap is the third key objective of the CSFCTool project. To support the training and self-learning activities two strictly interconnected actions have been implemented:

- **Extension of standards, regulations and laws list**
  As shown in Figure 5, the *Informative References* of the FNCS & DP have been extended by adding eight new documents which are briefly explained in Appendix A.

- **Creation of eight educational sections**
  Starting from the complete *Informative Reference* list, up to now, eight sections have been created (as shown in Figure 6), which present all documents listed in Figure 5. Each section includes:

	NIST CSF Version 1.1 (2018)	FNCS & DP Version 2.0 (2019)	CSFCTool (2021)
CIS CSC	√	√	√
COBIT 5	√	√	√
ISA 62443-2-1:2009	√	√	√
ISA 62443-3-3:2013	√	√	√
ISO/IEC 27001:2013	√	√	√
NIST SP 800-53 REV.4	√	√	√
D.LGS. 18/5/2018 N° 65		√	√
GDPR		√	√
MISURE MINIME AGID		√	√
ISO/IEC 29100:2011		√	√
NIST SP 800-53 REV.5 (UPGRADE)			√
NIST SP 800-82 REV. 2			√
ISO 19011:2018			√
ISO/IEC 27000:2018			√
ISO/IEC 27001:2017			√
ISO/IEC 27002:2017			√
ISO/IEC 27005:2018			√
ISO 31000:2018			√

Figure 5: *Informative References* comparison

1. A landing page with a brief introductory summary and links to all related standards, regulations or laws.
2. A timeline that allows to contextualize all related documents over time and national vs international panorama.
3. A subsection for each standard/regulation or law previously summarized. Each subsection proposes synthetic content aimed at self-orientation and/or self-learning (which can also be used for face-to-face or online training) and, in compliance with the original document, allows interactive access to all cited crossed contents.

4. Prototype description

CSFCTool is built as a standard web application. Its front-end is developed in HTML and CSS, taking advantage of the Bootstrap[8] framework to improve the look and feel of the user interface. The server-side code is written using the PHP programming language and the back-end data

[8]https://getbootstrap.com/

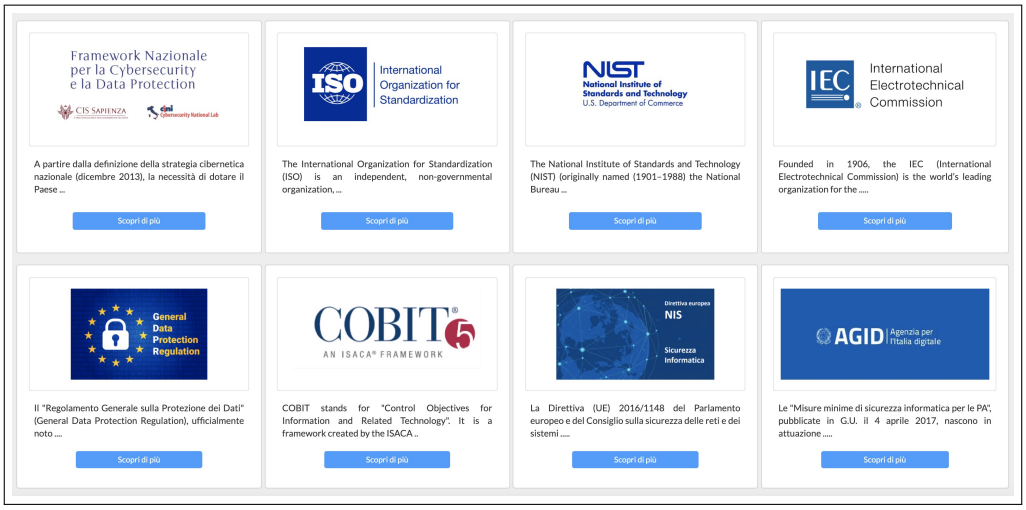

Figure 6: CSFCTool educational sections in the HOME page

storage is handled via a MySQL[9] server using MySQL Workbench, an Oracle unified visual tool that provides data modeling, SQL development, server configuration, user administration and backup. The current implementation is still a proof-of-concept built to demonstrate the potential of such an application. Some refactoring is needed to go online, but the current proof-of-concept version provides a view of all the functions that have been designed and implemented.

A visual sitemap of CSFCTool showing the full website structure is presented in Figure 7. The eight educational sections are available in the HOME page. From the menu bar it is possible to reach the services (SERVIZI) and other resources (RISORSE).

Figure 8 shows a small portion of the back-end relational database, presenting the tables (*Function, Category, Subcategory, Ref*) which allow to map all Subcategories with their corresponding Informative References as discussed in Section 3.1. Thanks to the data stored in these tables, the users can access all Informative References, and find all the details presented in a tabular form. This allows them to have a direct access to specific articles without having to browse the whole document.

In order to use the available services, the users must register to the platform providing their name, surname and a valid e-mail address. After authentication a user can:

1. Consult all articles from regulations, standards and laws listed for each Subcategory in the *Informative References* section, starting from FNCS & DP, CEC or an existing contextualization (e.g., GDPR).

2. Create a new project, e.g., select Subcategories they might decide to implement within their organization starting from FNCS & DP, CEC or from a new contextualization (consultation function for *Informative References* is still available to support choices).

3. Visualize all projects in a personal PORTFOLIO area. All different projects created and

[9]https://www.mysql.com/

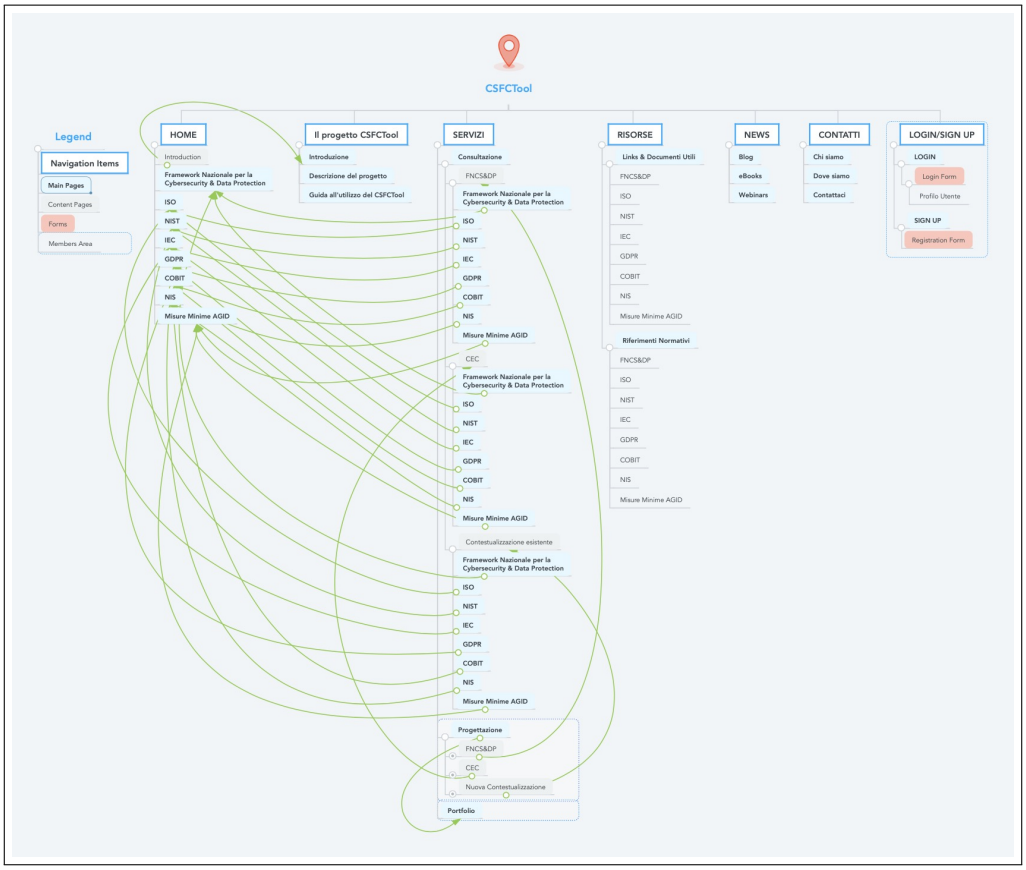

Figure 7: CSFCTool sitemap

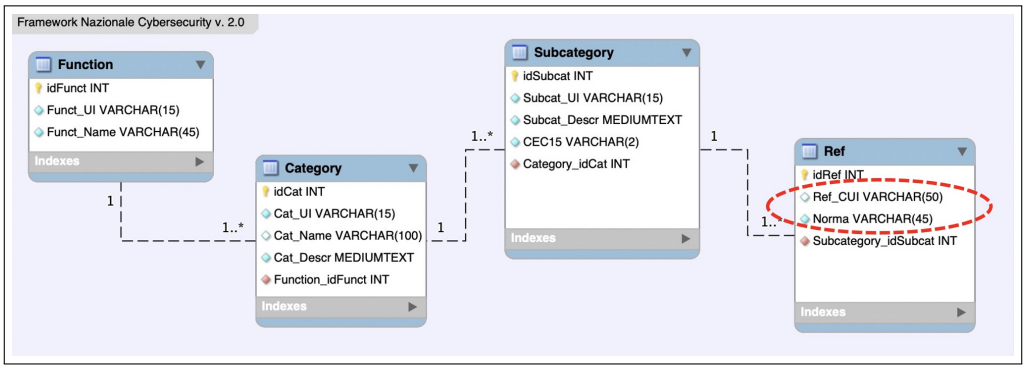

Figure 8: *EER diagram* for FNCS & DP tables

stored are here available in order to be used synergistically, e.g., to monitor continuous improvement when moving from the current to the target profile.

After selecting the starting point users are presented a page with the corresponding Functions, Categories, Subcategories and Informative References to be selected by checking boxes in a

guided procedure.

Figure 9: CSFCTool widget to create a new project starting from FNCS & DP

Figure 9 shows the four steps of this procedure, with the first one highlighted in blue. All projects are reachable from the section PORTFOLIO. Opening a created project makes available two sections. The first one presents a summary of the selected Subcategories while the second, for each Subcategory, provides the user with a section NOTE where to add information obtained from the normative or any other type of comment useful for its implementation. Currently, only textual comments can be added, but the extension to other types of documents, e.g., pdf files or images, can easily be added.

5. Conclusions and future work

This paper presented the main features of CSFTool, a new web-based application with the objective of raising awareness about IT/OT cybersecurity and empowering end users (in particular SMEs) with actionable knowledge on standards, regulations and laws related to protection of critical infrastructure.

We have discussed the main rationale behind the project, as well as provided information about both the design and the implementation of a proof-of-concept prototype of the overall system.

As part of our future work, we plan to refine the current implementation in order to arrive at a fully fledged product. The goal is to enable companies to leverage such a product for implementing effective strategies aimed at increasing the overall resilience level of their critical infrastructures.

A second line of exploitation concerns the use of the CSFCTool as an effective means for carrying out education and training campaigns, both at the academic level and as part of dedicated professional training initiatives tailored to private companies.

Finally, we also plan to integrate the CSFCTool with state-of-the-art monitoring frameworks

like, e.g., the well-known ELK (Elasticsearch, Logstash and Kibana)[10] stack. Namely, our tool might become an ELK component tailored to analyzing and catalyzing information about a company's IT/OT cybersecurity compliance level, as well as optimizing IT/OT data management processes for the long term.

References

[1] B. Obama, Presidential Policy Directive 21 (PPD21): Critical infrastructure security and resilience (Washington, DC (2013)).

[2] F. Bjorck, M. Henkel, J. Stirna, J. Zdravkovic, Cyber resilience–fundamentals for a definition, in: New Contributions in Information Systems and Technologies, Springer, 2015, pp. 311–316.

[3] R. Baldoni, L. Montanari, Un Framework Nazionale per la Cyber Security, 2015 Italian Cyber Security report, 2016.

[4] CIS-Sapienza/CINI, Controlli essenziali di cybersecurity, 2017.

[5] CIS-Sapienza/CINI, Framework nazionale per la cybersecurity e la data protection, 2019.

[6] M. Angelini, C. Ciccotelli, L. Franchina, A. Marchetti-Spaccamela, L. Querzoni, Italian national framework for cybersecurity and data protection, in: Annual Privacy Forum, Springer, 2020, pp. 127–142.

[7] B. Y. Ozkan, M. Spruit, Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda, International Journal of Standardization Research (IJSR) 17 (2019) 41–72.

[8] N. N. I. of Standards, Technology), NIST SP 800-53 rev. 5 - Security and Privacy Controls for federal Information Systems and Organizations (2020).

[9] G. Murray, M. N. Johnstone, C. Valli, The convergence of it and ot in critical infrastructure, in: 15th Australian Information Security Management Conference, 2017, p. 149.

[10] A. Shahzad, M. Lee, N. N. Xiong, G. Jeong, Y.-K. Lee, J.-Y. Choi, A. W. Mahesar, I. Ahmad, A secure, intelligent, and smart-sensing approach for industrial system automation and transmission over unsecured wireless networks, Sensors 16 (2016) 322.

[11] E. D. Knapp, J. T. Langill, Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems, Syngress, 2014.

[12] T. De Zan, Future research on the cyber security skills shortage, Cyber Security Education: Principles and Policies (2020).

[13] O. M. Al-Matari, I. M. A. Helal, S. A. Mazen, S. Elhennawy, Cybersecurity Tools for IS Auditing, in: 2018 Sixth International Conference on Enterprise Systems (ES), 2018, pp. 217–223.

[14] L. Topham, K. Kifayat, Y. A. Younis, Q. Shi, B. Askwith, Cyber security teaching and learning laboratories: A survey, Information & Security 35 (2016) 51.

[15] M. Angelini, S. Lenti, G. Santucci, CRUMBS: a cyber security framework browser, in: 2017 IEEE Symposium on Visualization for Cyber Security (VizSec), IEEE, 2017, pp. 1–8.

[16] N. N. I. of Standards, Technology), NIST SP 800-82 rev. 2 - Guide to Industrial Control Systems (ICS) Security (2015).

[10] https://www.elastic.co/

[17] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, K. Jones, A survey of cyber security management in industrial control systems, International journal of critical infrastructure protection 9 (2015) 52–80.
[18] E. E. C. S. Organization, State of art Syllabus - Overview of existing Cybersecurity standards and certification schemes v2, 2017.
[19] N. N. I. of Standards, Technology), NIST SP 800-53 rev. 4 - Security and Privacy Controls for federal Information Systems and Organizations (2013).
[20] I. I. O. for Standardization), ISO 19011:2018 - Guidelines for auditing management system (2018).
[21] I. I. O. for Standardization), ISO 27000:2018 - Information technology - Security techniques - Information Security Management Systems - Overview and vocabular (2018).
[22] I. I. O. for Standardization), ISO 27001:2017 Information technology - Security techniques - Information Security Management Systems - Requirements (2017).
[23] I. I. O. for Standardization), ISO 27001:2013 Information technology - Security techniques - Information Security Management Systems - Requirements (2013).
[24] I. I. O. for Standardization), ISO 27002:2017 Information technology - Security techniques - Code of practice for information security control (2017).
[25] I. I. O. for Standardization), ISO 27002:2013 Information technology - Security techniques - Code of practice for information security control (2013).
[26] I. I. O. for Standardization), ISO 27005:2018 Information technology — Security techniques — Information security risk management (2018).
[27] I. I. O. for Standardization), ISO 31000:2018 Risk management - Guideline (2018).

Appendix A

The documents listed in Figure 5 are briefly described in the following.

- **NIST SP 800-53 Rev.5** Revision of foundational NIST SP 800-53 rev.4, this publication represents a multi-year effort to develop the next generation of security and privacy controls that will be needed *"...to develop and make available to a broad base of public and private sector organizations a comprehensive set of safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud-based systems, mobile devices, Internet of Things (IoT) devices, weapons systems, space systems, communications systems, environmental control systems, super computers, and industrial control systems"*. It includes changes to make these controls more usable by diverse consumer groups (as enterprises conducting mission and business functions; engineering organizations developing information systems, IoT devices, and systems-of-systems; and industry partners building system components, products, and services).

- **NIST SP 800-82 Rev. 2** which provides the overlay tool for ICS described in CSFCTool objectives of Section 3.2.

- **ISO 19011:2018** ***"Guidelines for auditing management systems"*** [20] This document provides the third edition of ISO standard guidance on auditing management systems,

including the principles of auditing, managing an audit program and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process.

- **ISO/IEC 27000:2018** ***"Information technology - Security techniques - Information security management systems - Overview and vocabulary"*** (fifth edition) [21] This document provides an overview of Information Security Management Systems (ISMS) and describes terms and definitions commonly used in the ISMS family of standards.
- **ISO/IEC 27001:2017** ***"Information technology - Security techniques - Information security management systems - Requirements"*** [22] Review of ISO/IEC 27001:2013 [23] including Cor 1:2014 and Cor 2:2015.
- **ISO/IEC 27002:2017** ***"Information technology - Security techniques - Code of practice for information security controls"*** [24] Review of ISO/IEC 27002:2013 [25] including Cor 1:2014 and Cor 2:2015.
- **ISO/IEC 27005:2018** ***"Information technology - Security techniques - Information security risk management"*** [26] that provides ISO standard guidelines for information security risk management in an organization. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.
- **ISO 31000:2018** ***"Risk management - Guidelines"*** [27] This document provides ISO standard guidelines on managing risk faced by organizations. It provides a common approach to managing any type of risk and is not industry or sector specific. It can be used throughout the life of the organization.