Navigating Cybersecurity Compliance: The Cyber Compass for Medical Device Manufacturers

Andrea Neverdal Skytterholm[1][0000−0001−7507−6366], Adamantios Ntanis[4][0000−0002−1161−4222], Karin Bernsmed[1][0000−0001−9109−5401], Bjørn Magnus Mathisen[1][0000−0002−8063−1835], Egil Wille[2][0009−0004−0113−8594], Christos Androutsos[3][0009−0008−2056−722X], and Martin Gilje Jaatun[1][0000−0001−7127−6694]✉

[1] SINTEF Digital, Trondheim, Norway
{andrea.skytterholm, karin.bernsmed, bjornmagnus.mathisen, martin.g.jaatun}@sintef.no
[2] SINTEF Nordvest, Ålesund, Norway
egil.wille@sintef.no
[3] University of Ioannina, Greece
xristosandroutsos95@gmail.com
[4] PD Neurotechnology Ltd, UK
a.ntanis@pdneurotechnology.com

Abstract. Connected Medical Devices (CMDs) show great potential for improving patients' quality of life, and manufacturers work tenaciously to get such products to the market as quickly as possible. However, to protect the patients, the CMDs need to be developed in accordance with applicable regulations. Therefore, manufacturers must not only identify and implement relevant requirements for their CMDs, but also document their product lifecycle management, their approach to risk management and cybersecurity approach. Inspired by curated lists for cybersecurity management in other domains ("Awesome Lists"), the Cyber Compass tool has been developed to provide a similar overview of relevant cybersecurity resources for the healthcare domain. With its user-friendly interface and crowd-sourced nature, the tool helps manufacturers navigate and filter regulatory resources, alleviating the compliance burden. In addition to identifying the relevant documents and requirements, the tool also addresses the bigger challenge of fully understanding the regulatory requirements and implementing the necessary measures relevant for all stakeholders involved in the lifetime of the CMD. The results from the evaluation of the Cyber Compass tool indicate that stakeholders of CMDs can successfully use the tool for this purpose.

Keywords: Connected Medical Devices · Medical Device Manufacturers · Regulations · Standards · Regulatory Compliance · Best-Practices · Security Requirements · Cybersecurity · Healthcare

1 Introduction

Connected Medical Devices (CMDs) can assist patients in managing a wide range of health conditions and significantly enhance their quality of life. The earlier a medical device reaches the market, the sooner it can be integrated into the healthcare system, enabling its use in patient treatment, enhancing efficiency, and often reducing overall healthcare costs. Consequently, manufacturers face significant pressure to get their products out on the market as quickly as possible. However, in order for CMDs to fulfil their purpose, we need to ensure that they are safe and secure to use. Security vulnerabilities in CMDs can be exploited to harm patients or cause device failures, making it crucial to implement robust security mechanisms to prevent such incidents. Regulation is therefore critical: it protects patient safety, ensures data privacy, maintains the integrity of healthcare services, and provides a legal and ethical framework for manufacturers and healthcare providers. However, identifying relevant regulations, standards, guidelines, and best practices is a complex and resource-intensive task. This challenge is particularly evident under the new European regulations: the Medical Device Regulation (MDR) [15] and the In Vitro Diagnostic Regulation (IVDR) [13]. These regulations require manufacturers to prepare and submit a medical device file to notified bodies and national authorities, and to maintain it for any new or existing device that incorporates software, as well as for stand-alone software that qualifies as a medical device. The file must, among other things, describe the principles of the medical device development life cycle and the manufacturer's approach to risk management, including information security measures as well as the verification and validation processes of the device [16]. Navigating this complex legal and regulatory landscape and identifying the specific requirements for manufacturers is particularly burdensome. This challenge is further compounded by the lack of comprehensive guidance on security mechanisms and best practices during the design phase of medical devices, which can delay development and slow the introduction of products to the market. Large companies and organizations often have in-house expertise to manage and maintain such documentation. However, for smaller companies, particularly small and medium-sized enterprises (SMEs), this can pose a significant challenge due to limited financial and human resources. As a result, manufacturers, especially SMEs, frequently rely on specialized third-party consultants, which can incur substantial costs and divert resources that could otherwise be invested in improving their medical devices.

Thorough legal and regulatory efforts by both governments and organizations are essential for guiding the development of medical devices and protecting patients. However, these efforts tend to increase complexity, which can hinder innovation, especially for SMEs and start-ups that operate at different development speeds and with limited resources (with respect to financial resources, human capital, and technical expertise). In such cases, regulations can act as a barrier to entry, with large established corporations facing little competition from SMEs and start-ups, not due to superior products or services, but simply because the legal and regulatory landscape is too complex and costly for smaller organizations to navigate. Consequently, there is a clear need for a solution that

enables organizations to navigate the complex legal and regulatory landscape, guiding them not only toward compliance but mainly toward the development of safe and secure medical devices.

In previous work [3], we studied common cybersecurity challenges faced by manufacturers of CMDs. Among these, three challenges appear to be particularly difficult to address in order to achieve regulatory compliance.

Purpose Definition – When preparing for the approval (certification) process, defining the *purpose* of the device is crucial from the outset. Determining whether a product qualifies as a medical device might seem straightforward, but in practice, it is often ambiguous and depends largely on the manufacturer's stated intended purpose. For example, the Apple Watch [1] is classified as a "general wellness device" rather than a formal medical device, even though it has received regulatory clearance in the US for specific health features, such as detecting irregular heart rhythms and use in medical research [18].

Regulatory Complexity – Obtaining a comprehensive overview of the many standards, regulations, and guidelines relevant to the target market is notoriously challenging—particularly for the SMEs, which often lack the necessary resources. Manufacturers must navigate numerous documents that are frequently inconsistent. Recommended guidelines often reference other documents that may be outdated, making compliance a difficult and time-consuming task.

Evolving Standards and Practices – Best practices, guidelines, standards, and regulations are continuously evolving, requiring manufacturers to stay up to date to ensure device security and safety. This constant evolution adds a significant burden when preparing a medical device file for certification, particularly for smaller companies with limited resources. Staying compliant not only demands continuous monitoring and adaptation of internal processes but can also extend the time-to-market, potentially causing smaller players to lose their first-mover advantage and limiting their ability to compete effectively in a fast-moving industry.

While these challenges were specifically reported by medical device manufacturers in our study, the data also indicated that other stakeholders in the industry, such as integrators and operators of CMDs, face similar issues when installing and operating new devices within healthcare environments.

To address these challenges, we have developed **Cyber Compass** [21], a tool that assists manufacturers, integrators, and operators of CMDs in identifying relevant security standards and regulations based on a few simple questions about the device and its intended use. The tool was developed as part of the NEMECYS Horizon Europe research project and has been evaluated through two consecutive industry-driven pilot studies (each comprised of 4 case studies) conducted by diverse industry partners. The development process was guided by the requirements identified in these case studies. Cyber Compass is available as an open-source tool on GitHub [20]. This paper presents the first version of the tool, developed as a proof of concept, with the goals of identifying additional user

needs, evaluating its usability, and assessing whether it provides sufficient value to stakeholders, while future work will focus on extending and further utilizing the tool to address more specific needs of medical device stakeholders.

The structure of the paper is as follows: In Section 2, we review relevant previous work. Section 3 explains the main objectives and functionality of the tool. Section 4 details its design and implementation, while Section 5 presents the results from the evaluation of the tool in four case studies. Finally, Section 6 summarises the findings and outlines directions for future work.

2 Related work

Related work relevant to our study can be categorized into three areas: legal and regulatory guidance from official organizations, research reviewing such legal and regulatory frameworks, and technology or tools designed to alleviate compliance and cybersecurity challenges.

Legal and regulatory guidance – A multitude of guidelines exists regarding the cybersecurity of medical devices; however, we focus on the ones from the Medical Device Coordination Group (MDCG) and the American Food and Drug Administration (FDA), as they provide guidance reflecting the regulatory priorities of the European Union and the United States, which are the jurisdictions most relevant to our study. Cyber Compass is designed to assist users in following and implementing the processes recommended in these guidelines. In the EU, the MDCG 2019-16 guidelines titled "Guidance on Cybersecurity for medical devices" [16], provide a structured approach for identifying and implementing the necessary cybersecurity measures throughout the lifecycle of CMDs. Recognising the growing complexity of such devices, and their susceptibility to cyber threats, these guidelines aim to assist medical device manufacturers, integrators and operators in mitigating risks while maintaining compliance with regulatory frameworks such as the MDR and the IVDR. In the U.S., the FDA has issued the guidance documents FDA-2021-D-1158 and FDA-2015-D-5105, titled "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" [11] and "Postmarket Management of Cybersecurity in Medical Devices" [10], respectively. These guidance documents advise the industry on incorporating cybersecurity considerations into device design, labeling, and the required documentation for premarket submissions involving devices with cybersecurity risks. They also provide recommendations for managing cybersecurity vulnerabilities in devices already on the market. Manufacturers are encouraged to integrate cybersecurity measures throughout the entire product lifecycle, from design and development to production, distribution, deployment, and ongoing maintenance. These guidance documents also emphasises that, with the increasing prevalence of networked medical devices aimed at improving patient care, these devices—like other connected computer systems—contain software that can be susceptible to cybersecurity threats.

Legal and regulatory research – Relevant academic work includes the study by Skytterholm et al. [19], which compares the distinct cybersecurity re-

quirements for placing on the market CMDs in the EU and the US. Their analysis is based on the European MDCG 2019-16 guidance and the US FDA premarket and postmarket guidance. The authors examined both the organizational approaches of the MDCG and FDA, as well as the content of their specific guidance documents, identifying key differences and areas of convergence. Bhatt [4] further explored regulatory and compliance considerations for CMDs, addressing both the global regulatory landscape and emerging regulations related to medical device security. The study also highlighted challenges in compliance and enforcement. Biasin et al. [5] focus on the cybersecurity of AI-based medical devices, emphasizing that AI, medical devices, and cybersecurity are closely intertwined but often regulated separately. A key contribution of their work is the comparison of regulatory approaches in the EU and the US. They highlight that both regions adopt risk-based frameworks, yet the US follows a rule-based model, while the EU uses a principle-based system. These differences have significant implications for the regulation of AI medical device cybersecurity. Finally, Biasin et al. [6] reviewed the current EU legal framework for CMD cybersecurity, with particular attention to the European Health Data Space, the Data Act, and the Artificial Intelligence Act. While none of these studies provide tool support, we have begun populating the knowledge database of the Cyber Compass tool using the documents identified in these works.

Technology and tools – In terms of existing tool support, the BSI "Compliance Navigator" [7] serves a purpose similar to the Cyber Compass: it helps medical device manufacturers access and manage regulatory documents, saving time, maximizing resources, and reducing risk. However, while this tool aids in identifying relevant standards and regulations, it is not directly designed towards supporting the creation of the technical documentation needed for cybersecurity regulatory compliance, tailored to the unique needs of different organizations and their regulatory pathways. Additionally, its relatively high cost makes it less accessible for start-ups and small businesses. In contrast, Cyber Compass has been specifically developed to support diverse regulatory pathways, recognizing that effective compliance requires a community-driven approach. As such, it is available as an open-source tool, also making it free of charge. Another relevant tool is the CISO Assistant [9], an open-source platform that facilitates cybersecurity program management. It provides a practical approach to Governance, Risk, and Compliance (GRC), helping cybersecurity professionals manage organizational cybersecurity and comply with applicable laws and regulations. However, the CISO Assistant is not specific to medical devices and focuses on overall cybersecurity management, including internal auditing, risk assessment, and other processes, rather than regulatory compliance for medical devices specifically.

For the design of the Cyber Compass tool, we drew inspiration from curated repositories on other topics, such as "Awesome Machine Learning" [17] and "Awesome Embedded and IoT Security" [2], which are cover machine learning and embedded systems, respectively. A curated repository is a collection of resources that has been carefully selected and organised, and that is maintained by trusted contributors to ensure the quality, relevance, and accuracy of its content. "Awe-

some Lists" are GitHub repositories that provide comprehensive, topic-specific resources, typically curated by the community. To our knowledge, no similar curated lists exist for cybersecurity in the healthcare domain, making the Cyber Compass tool a unique contribution in this space.

3 Tool overview

The main objective of the Cyber Compass tool is to simplify the process of identifying relevant regulations, standards, guidelines, and other up-to-date materials by consolidating all essential information in one place. The ultimate goal is to foster a community of medical device stakeholders who share resources and expertise on legal and regulatory compliance. Given the fast-paced and constantly evolving nature of this field, such a collaborative and continuously updated community is essential to ensure that information remains current. Cyber Compass is built entirely using open-source technologies to ensure freedom from vendor lock-in and the risk of proprietary technology deprecation. The technical implementation of the tool itself can be considered secondary; what truly matters is the community aspect and the capabilities we envision for this community. These include the use of open-source technologies, the promotion of open and accessible knowledge for all, and the adoption of standardized data formats to support effective knowledge sharing.

The target users of the Cyber Compass tool include three main stakeholder groups: manufacturers, operators, and integrators of CMDs. These groups have distinct needs and responsibilities in identifying and maintaining applicable regulatory requirements, as well as relevant standards, guidelines, and best practices throughout the device lifecycle. The tool is therefore designed to accommodate these differences when identifying, organizing, and categorizing relevant documentation.

The tool provides a comprehensive knowledge base of relevant documentation, accessible through an intuitive and user-friendly interface. At present, most documents in the knowledge base are focused on manufacturers. However, the scope will be expanded to include materials relevant to operators and integrators as the tool continues to evolve. Owing to its modular structure, information in the Cyber Compass knowledge base is organized and categorized in a way that is adaptable to various domains, such as services, devices, and operations. Finally, when multiple documents are identified, the tool also maps relationships among them to provide a more comprehensive understanding of the regulatory landscape.

To develop the documentation knowledge base, which forms the foundation of the Cyber Compass tool, we conducted a comprehensive review of current regulations, guidelines, standards, and best practices concerning the cybersecurity of medical devices. The results of this research are reported in [14]. Using this material, we created the first version of the knowledge base, structured in JSON format, and shared it as an open-source resource on GitHub [20]. The JSON file contains detailed information about each document and is organized

to facilitate easy integration with other tools and systems. Beyond serving as the core input to the Cyber Compass tool, this approach allows members of the healthcare community to help maintain and update the knowledge base, ensuring that new and emerging trends in cybersecurity best practices are continuously incorporated.

4 Design and implementation

The design of the Cyber Compass tool was conducted as part of a larger study [14], aimed at extracting in-depth information on the cybersecurity challenges faced by the three stakeholder groups (manufacturers, integrators and operators) involved in the lifecycle of CMDs. This was achieved through a qualitative research approach, combining interviews with a selected group of participants and document analysis, enabling a detailed and comprehensive analysis of the collected data.

The selection criteria for the interviews focused on stakeholders with practical experience in medical device manufacturing, as well as integrators and operators of such devices. In total, six stakeholders were interviewed: three identified as medical device operators, two as medical device manufacturers, and one as a medical device integrator. All participants were affiliated with companies in the European healthcare sector, and five of them were involved in the ongoing Horizon Europe project NEMECYS [14].

Two rounds of interviews were conducted. The first round focused on the overall challenges and needs of the stakeholders. Based on these results, combined with the document analysis, we identified the need for a set of tools to support these three stakeholder groups in their cybersecurity activities. The Cyber Compass was one of these tools, designed to address the specific need for guidance in understanding the regulatory requirements and implementing the necessary measures relevant for all stakeholders involved in the lifetime of the CMD. The second round of interviews then concentrated on the specific requirements for each of the identified tools. Consequently, the design of the Cyber Compass tool is based directly on the requirements derived from the analysis of the second-round interview data.

The following list presents the requirements identified for the Cyber Compass tool. The first six requirements (R1–R6) were derived directly from interviews with stakeholders, reflecting the practical needs of manufacturers, operators, and integrators of connected medical devices. An additional technical requirement (R7) was defined to support integration with other tools developed in the NEMECYS project.

User friendly interface (R1): The tool shall provide an intuitive and user-friendly interface that allows all stakeholders, manufacturers, operators and integrators of CMDs to efficiently navigate through the knowledge base. The interface should minimize learning curves, support smooth interactions, and ensure users can easily access and understand all features and resources. Easy to navigate and responsive across devices.

Up-to-date information (R2): The tool shall continuously incorporate new trends, best practices, and emerging standards in cybersecurity for medical devices. This ensures that users are always accessing the most current and relevant information, reducing the risk of outdated or incomplete guidance. Provides a comprehensive overview of all available resources in a single location.

Categorization (R3): The tool shall organize and categorize information in a flexible and modular way, covering multiple domains such as services, devices, operations, and stakeholder roles. This categorization enables users to quickly locate relevant documents, compare related standards, and explore connections between different regulatory and guidance materials. Supports efficient information retrieval and better understanding of context.

Interoperability (R4): The tool shall support seamless interaction with other procurement, compliance, or cybersecurity management tools. This capability allows for easy data exchange and integration, enabling organizations to incorporate the Cyber Compass knowledge base into existing workflows and digital ecosystems without duplicating effort.

Filtering mechanism (R5): The tool shall provide a robust filtering mechanism that allows users to efficiently narrow down large sets of documents according to multiple criteria, su7ch as stakeholder group, geographic location, regulatory framework, device type, or standard. This ensures that only the most relevant documents are presented, improving usability and saving time when searching for critical information.

Document connections (R6): The tool shall visually and structurally represent the relationships between different documents, such as regulations referencing specific standards or guidelines tied to particular requirements. This relational mapping helps users understand dependencies and context, making it easier to trace compliance requirements and navigate complex regulatory landscapes.

Input format (R7): The tool shall accept a JSON file containing the documentation knowledge base as input. The format should be structured to include all relevant metadata for each document, facilitating integration with other tools, automated updates, and easy maintenance. Ensures compatibility and extensibility for future enhancements or external applications.

The first version of the tool consists of two main components: a knowledge base containing all relevant documentation and a user-friendly web interface for accessing and filtering this documentation. The construction of the knowledge base is described in Section 3. For the user interface, we employed a web application framework originally developed in the European project B-WaterSmart [8] to present the knowledge base in an intuitive and accessible manner. The web application includes filtering mechanisms that allow users to interact with the knowledge base and retrieve only the documents relevant to their needs. Figure 1 shows a selection of pages from the tool.

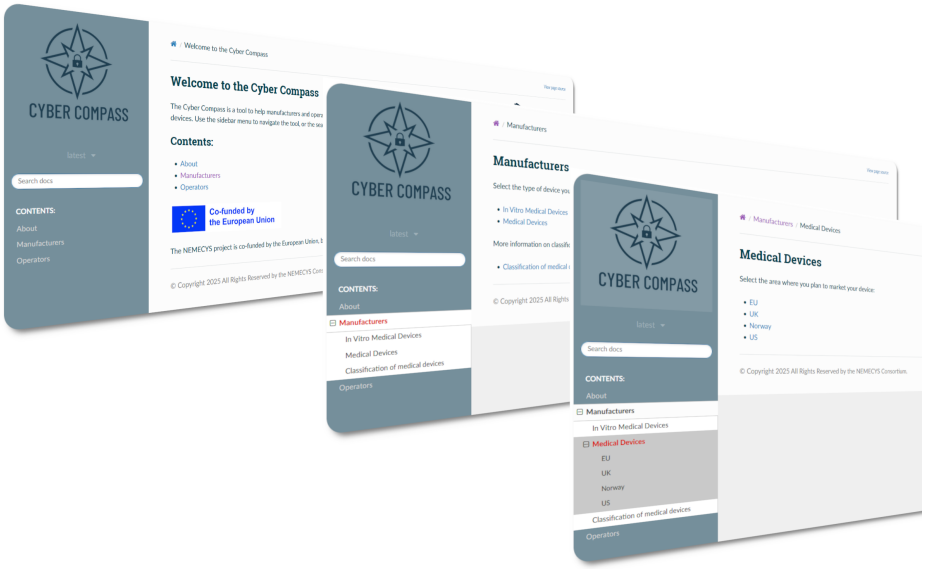

Fig. 1. Three pages of the Cyber Compass showcasing the user interface, the theming, and aspects of the information structure.

5 Evaluation

To evaluate the Cyber Compass tool, we utilised the four case studies being developed in the NEMECYS project, summarised below.

Home dialysis (CS1): In this case study, a medical device manufacturer is developing a non-invasive wearable sensor device that monitors hydration levels in patients with fluid management-related health conditions. The device is intended to provide real-time feedback to patients and healthcare providers, supporting more accurate fluid management and reducing the risk of complications. During the evaluation, the Cyber Compass tool was used as an input resource for checking a comprehensive list of external documents required by ISO 13485:2016-certified companies [12]. This list includes specific regulations, standards, and guidance documents applicable to both the manufacturer and the products being developed. Maintaining and updating this list is critical for regulatory compliance and product safety. The Cyber Compass tool provided a structured and centralized way to ensure that the manufacturer could access the most recent and relevant documents, improving efficiency and confidence in compliance processes.

Wearable devices (CS2): In this scenario, a medical device manufacturer is developing an IoT-enabled wearable device, comprising both Cloud and Edge components, for continuous patient monitoring in home and hospital settings. The device collects sensitive health data and transmits it securely to healthcare providers for analysis. During evaluation, the Cyber Compass

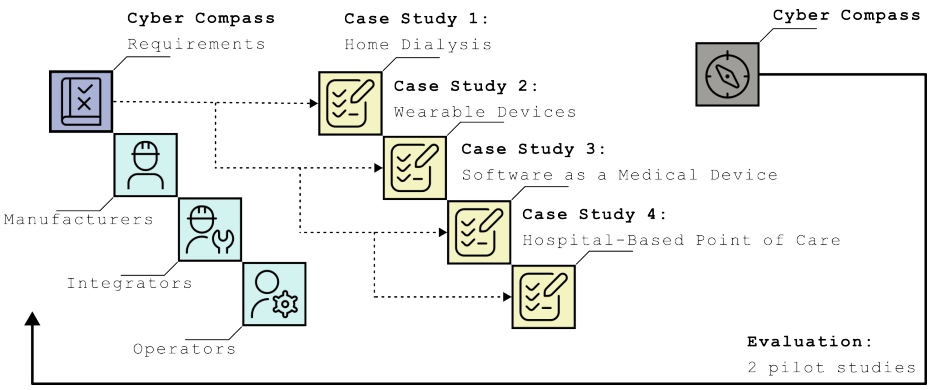

Fig. 2. Structure of the pilot studies and their corresponding case studies, showing how each contributes to the overall evaluation of the Cyber Compass tool.

tool enabled the manufacturer to search through cybersecurity-related documentation in a centralized and user-friendly database. By using the tool, the manufacturer was able to maintain an up-to-date list of relevant cybersecurity regulations, standards, and best practices, ensuring that all critical security considerations were systematically addressed. This streamlined the compliance process, reduced the risk of overlooking important cybersecurity requirements, and supported the safe deployment of the connected device.

Software as a Medical Device (CS3): In this case study, a medical device manufacturer is developing a Class IIb Software as a Medical Device (SaMD) mobile application to help people with diabetes manage their therapy, including monitoring glucose levels, tracking insulin intake, and providing personalized recommendations. The application must comply with strict regulatory standards and guidance for medical software, while ensuring usability and safety for patients. During evaluation, the Cyber Compass tool was employed to cross-check an internal document containing all relevant regulations, standards, and guidelines. This allowed the manufacturer to systematically identify gaps in compliance, update their internal documentation, and ensure that the software development process aligned with regulatory requirements, thereby reducing the risk of non-compliance or delayed approval.

Hospital-based point of care (CS4): This case study focuses on a hospital operator using an in-vitro diagnostic (IVD) device—the Freestyle Libre 2 Continuous Glucose Monitoring (CGM) kit—which is used by both healthcare professionals and patients. The device requires proper integration into the hospital workflow, including staff training, calibration, and data management. During evaluation, the Cyber Compass tool was used to identify all relevant regulations, standards, guidelines, and best practices applicable during device integration and operation. This ensured that the hospital could deploy and manage the device in accordance with current regulatory and safety standards. Additionally, the tool facilitated the maintenance of

Table 1. Cyber Compass feedback matrix

Requirement	CS1	CS2	CS3(1)	CS4	CS3(2)
R1	Pass	Pass	Pass	Pass	Pass
R2	N/A	N/A	N/A	N/A	Pass
R3	Fail	Pass	Pass	N/A	Pass
R4	N/A	N/A	N/A	N/A	Pass
R5	Fail	Pass	Pass	Pass	Pass
R6	N/A	N/A	N/A	N/A	Pass
R7	N/A	N/A	N/A	N/A	Pass

an up-to-date reference of critical documentation, supporting the hospital in maintaining compliance, optimizing operational efficiency, and ensuring patient safety.

The evaluation of the Cyber Compass tool was conducted as part of two broader pilot studies, each implementing the four case studies described above, designed to assess the applicability of all cybersecurity tools developed within the NEMECYS project. Figure 2 illustrates the structure of the two pilot studies conducted to evaluate the Cyber Compass tool. The graph highlights how the pilot studies are organized and how the individual case studies contribute to the overall evaluation process. The primary objective of the pilot studies was to ensure that the tools could effectively address cybersecurity challenges across diverse CMD scenarios while complying with relevant regulatory and compliance requirements, including those outlined in the MDCG 2019-16 guidelines. During the pilots, each case study owner applied the tools within their specific scenarios and provided structured feedback to the tool developers regarding the fulfillment of each predefined tool requirement.

The feedback from the four case studies on the Cyber Compass tool is summarised in Table 1. The table shows whether the tool passed or failed each of the requirements listed previously in Section 4 for each of the case studies. The table also indicates if a requirement was not applicable (N/A) at the time of the evaluation. The reason for this was either that the requirements was not relevant for that particular stakeholder group, or that the requirement had not yet been implemented in the version of the tool that was being used. During the first pilot, all four case studies evaluated requirements R1, R3 and R5 of the Cyber Compass tool. A second pilot has now been launched; however, at the time of writing this paper, it is only case study 3 that has completed the second round of evaluation of the Cyber Compass tool. This case study is therefore represented twice in the table, with "CS3 (1)" for the results from the first pilot and "CS3 (2)" with the results from the second pilot.

The feedback from the first pilot study has already been used to enhance the tool, ensuring it better meets the needs of its users. Although the second pilot is

still ongoing, the initial results indicate that the tool is now likely to satisfy all requirements, as reflected in the updated results from case study 3 (see column "CS3 (2)" in Table 1).

6 Discussion, conclusion and future work

Active engagement with multiple CMD stakeholders (manufacturers, integrators, and operators) revealed the need for collaboration that leverages crowd-sourced legal and regulatory expertise, as well as unique cybersecurity experiences. The Cyber Compass tool has initiated this process, specifically targeting CMDs. The tool is designed to help manufacturers, integrators, and operators of CMDs identify relevant regulations, standards, and guidelines. It consolidates essential information in a single location and is structured as a wiki to facilitate easy access to regulatory documents, standards, and guidance materials related to medical device cybersecurity.

Evaluation results for the tool indicate that it meets the specific requirements identified during interviews with CMD stakeholder groups. However, despite positive feedback, the endeavor is still in its early stages, with the knowledge contained in the knowledge base remaining incomplete. For example, it currently lacks best-practice documentation and metadata for each regulation, standard, and guideline, making it difficult for users to identify the relevant markets and requirements based solely on their titles. Furthermore, the tool currently serves primarily as an index of legal and regulatory knowledge, without guidance on how to apply that knowledge. While maintaining this index is valuable, the crowd-sourced nature of the tool is intended to provide applicability insights, helping stakeholders learn from each other's experiences. Possible applicability insights for the Cyber Compass tool and platform for CMD stakeholders could include:

Guidance on MDR Article 2 – Device manufacturers are required to first determine whether their product qualifies as a medical device. Defining a device's intended purpose is one of the most critical activities during early-stage design, development, and regulatory planning, as it shapes the overall strategic direction. Clear guidance at this stage can help manufacturers make informed decisions on product classification, risk management, clinical evaluation needs, and subsequent regulatory pathways, reducing uncertainty and costly redesigns later in development.

Regulatory compliance requirements – Stakeholders need to understand how to meet obligations under regulations such as the MDR and IVDR. Current guidance documents, particularly the MDCG 2019-16 [16] guidelines, are often perceived as confusing rather than helpful, leading many stakeholders to rely on external consultants. The level of guidance available from notified bodies also varies significantly: some maintain that providing guidance would compromise their impartiality, while others offer recommendations based on experience with similar cases.

Future work includes not only enhancing the Cyber Compass tool itself but also defining a strategy for maintaining its knowledge base over time. The scope of maintenance is expected to grow alongside updates to regulations, standards, and guidance, highlighting the need for continuous collaboration and regular updates. Discussions with representatives from target stakeholder groups indicate that simply hosting the tool on GitHub is insufficient; it is crucial to identify an individual or organization with sufficient interest in keeping it current, whether through a single responsible actor or an appropriate forum or association.

Cybersecurity and compliance can be a complex puzzle, which is why consulting services thrive—especially in sectors like healthcare, where human life is at stake. While compliance may sometimes be seen as a burden, its core purpose is to safeguard the quality of products and services, ultimately contributing to a better world. Cyber Compass is an endeavor toward that goal, but it requires active participation to truly succeed. The participants of the NEMECYS project kickstarted this initiative, yet no matter how much effort they contribute, it will never be sufficient on its own. In this work, we have demonstrated that collaboration among industry and research partners is essential, and that a dedicated community is needed to address both cybersecurity and regulatory challenges. We have also shown that the Cyber Compass tool is on the right track. We invite you to join us in making it even better.

7 Acknowledgement

This work has been performed as part of the NEMECYS project, supported in part by the European Commission Horizon Europe programme, grant number 101094323 and the UK Research and Innovation (UKRI) Horizon Europe funding guarantee under grant numbers 10065802, 10050933 and 10061304, and the Swiss State Secretariat for Education, Research and Innovation (SERI).

References

1. Apple Inc.: Apple watch home page, `https://www.apple.com/watch`
2. Awesome embedded and IoT security, `https://github.com/fkie-cad/awesome-embedded-and-iot-security`
3. Bernsmed, K., Jaatun, M.G.: Security-by-design challenges for medical device manufacturers. In: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference. pp. 155–160 (2024)
4. Bhatt, S.I.: Cybersecurity Risks in Connected Medical Devices: Mitigating Threats to Patient Safety. In: International Journal of Trend in Scientific Research and Development (IJTSRD). vol. 9 (Mar-Apr 2025)
5. Biasin, E., Kamenjašević, E.: Regulatory approaches towards AI-based medical device cybersecurity: A transatlantic perspective. European Journal of Risk Regulation **15**(4), 876–886 (2024)
6. Biasin, E., Yaşar, B., Kamenjašević, E.: New Cybersecurity Requirements for Medical Devices in the EU: The Forthcoming European Health Data Space, Data Act, and Artificial Intelligence Act. In: Law, Technology and Humans. vol. 5 (2023), `https://doi.org/10.5204/lthj.3068`

7. BSI compliance navigator, https://compliancenavigator.bsigroup.com/
8. B-watersmart, https://b-watersmart.eu/
9. CISO Assistant: Open Source GRC Platform (2025), https://github.com/intuitem/ciso-assistant-community, accessed: 2025-10-23
10. FDA: Postmarket management of cybersecurity in medical devices. US Food and Drug Administration (dec 2016), https://www.fda.gov/media/95862/download
11. FDA: Cybersecurity in medical devices: Quality system considerations and content of premarket submissions. US Food and Drug Administration (2023), https://www.fda.gov/media/119933/download
12. ISO: Medical devices – quality management systems – requirements for regulatory purposes. ISO Standard 13485:2016 (2016), https://www.iso.org/standard/59752.html
13. In-vitro Diagnostic Medical Device Regulation. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.) (2025), https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng
14. Jaatun, M.G., Taylor, S., Upstill, C., Farkash, A., Garcia, S., Androutsos, C.: NEMECYS: addressing challenges to building security into connected medical devices. In: Cruz-Cunha, M.M., Domingos, D., Peres, E., Rijo, R. (eds.) HCist - International Conference on Health and Social Care Information Systems and Technologies 2023, Porto, Portugal, November 8-10, 2023. Procedia Computer Science, vol. 239, pp. 1361–1368. Elsevier (2023). https://doi.org/10.1016/J.PROCS.2024.06.307
15. Medical Device Regulation. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.) (2025), http://data.europa.eu/eli/reg/2017/745/oj
16. Medical Device Coordination Group: MDCG 2019-16 - Guidance on Cybersecurity for medical devices (2020), https://ec.europa.eu/docsroom/documents/41863
17. Misiti, J.: Awesome machine learning, https://github.com/josephmisiti/awesome-machine-learning
18. MobiHealthNews: The FDA approves Apple Watch's heart monitoring tool for use in clinical trials, https://www.mobihealthnews.com/news/fda-approves-apple-watchs-heart-monitoring-tool-use-clinical-trials
19. Skytterholm, A.N., Androutsos, C., Ntanis, A., Jaatun, M.G.: Cybersecurity Guidances for Medical Devices: An MDCG and FDA Regulatory Comparison. In: Proceedings of the 2025 IEEE International Conference on Smart Computing (SMARTCOMP) (2025), https://doi.org/10.1109/SMARTCOMP65954.2025.00079
20. Skytterholm, A.N., Mathisen, B.M.: Cyber Compass source code, https://github.com/andreaskytterholm/SOTA-tool
21. Skytterholm, A.N., Mathisen, B.M.: Cyber Compass tool page, https://cybercompass.readthedocs.io/latest/