International Journal of Information Security (2025) 24:90
https://doi.org/10.1007/s10207-025-01009-z

REGULAR CONTRIBUTION

A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain

Kitty Kioskli[1,2] · Elisavet Grigoriou[3] · Shareeful Islam[4] · Andrianos M. Yiorkas[3] · Loizos Christofi[3] · Haralambos Mouratidis[1,5]

Accepted: 23 February 2025 / Published online: 10 March 2025

Abstract

In recent years, the healthcare sector has undergone a significant digital transformation, driven by the rise of the Internet of Medical Things and the exponential use of connected medical devices in healthcare service delivery. This transformation offers numerous benefits, including enhanced patient data collection, processing, and informed treatment decisions. Despite these advantages, digital adoption brings several security challenges that pose considerable risks to overall healthcare service delivery. Additionally, connected medical devices must comply with sector-specific regulatory requirements to ensure trustworthiness and facilitate their broader adoption in the healthcare sector. There is, therefore, a pressing need to understand and manage these risks and compliance issues to secure and strengthen the resilience of healthcare systems. This work addresses these needs by introducing a novel Risk and Conformity Assessment Framework and Certification Scheme, implemented within an agile Information Security Management System context to enhance the security and resilience of healthcare systems. The framework leverages Artificial Intelligence (AI) in risk management practices, improving security assessments, risk prediction, security control implementation, and continuous monitoring. AI algorithms analyze large data volumes from various sources, enabling efficient processing and the identification of potential risk patterns. Additionally, AI-driven automation tools ensure consistent deployment of security controls, while continuous AI monitoring detects abnormal activities and enables rapid response to security incidents. The proposed Cybersecurity Certification Scheme incorporates AI-based security assessments into the certification process, facilitating efficient conformity assurance. This scheme also promotes a collaborative approach with relevant regulatory bodies to achieve compliance. While this work introduces a conceptual framework, its implementation and potential refinements remain subjects for future research. Further studies are necessary to validate its effectiveness, enhance its components, and evaluate its practical application in real-world healthcare environments.

Keywords Cybersecurity · Risk · Conformity assessment · Medical device · Artificial intelligence · Healthcare information infrastructure

1 Introduction

The healthcare sector is continuously evolving, and technology plays a key role for the massive digitalization across the sector. Emerging technologies like connected medical devices, cloud computing and IoT reshape the whole healthcare sector in terms of sharing healthcare data, treatment plans and overall healthcare service delivery. There are over 500,000 different types of connected medical devices, incorporating software and artificial intelligence (AI) tools, which use network infrastructure to transfer, manage and analyse health data for prevention, treatment, monitoring, diagnosis,

Elisavet Grigoriou shares joint first co-authorship for this work.

✉ Kitty Kioskli
kitty.kioskli@trustilio.com

Shareeful Islam
shareeful.islam@aru.ac.uk

1 School of Computer Science and Electronic Engineering, Institute for Analytics and Data Science (IADS), University of Essex, Essex, UK

2 Trustilio BV, Amsterdam, Netherlands

3 eBOS Technologies Ltd, Nicosia, Cyprus

4 School of Computing and Information Science, Anglia Ruskin University, Cambridge, UK

5 Security Labs Consulting, Cork, Ireland

and recovery from both chronic and non-chronic diseases [1]. Patient implantable devices such as holters, pacemakers, insulin pumps, cochlear implants, brain stimulators, etc. as well as wearables or pressure holters and glucose monitors, are connected medical devices that interact with the Healthcare Information Infrastructure (HCII) [2]. The devices themselves, the digital infrastructure that supports them, and the data collected are creating the Internet of Medical Things (IoMT)—a connected infrastructure of medical devices, software applications, and digital health systems and services [3]. In the meantime, specific processes are in place involved in the production, distribution, and delivery of medical devices to the healthcare facilities, providers, and ultimately to patients. The COVID-19 pandemic highlighted the importance of strong and resilient medical supply chains, as the global demand for essential medical supplies surged [4].

Despite significant research effort for developing smart medical devices, existing cybersecurity challenges are hurdling the digitization of the healthcare sector. The ability to compromise devices and networks and the possibility of monetising patient data have led to significantly increased and sophistication of catastrophic cyberattacks targeting healthcare organisations [5]. The result is a perfect storm that puts the importance of healthcare cybersecurity more front and centre than ever before, particularly for IoMT [6], which are connected medical devices that couple IoT technologies with healthcare services to support real-time, remote patient monitoring and treatment [7]. Emerging new technologies such as AI, blockchain, and cloud technologies have been widely adopted in medical devices, but their software has revealed new cybersecurity challenges [8]. Also, the interoperability, security, and resilience levels of connected medical devices are low, which is a widely acknowledged concern [9]. Moreover, cybersecurity threats can pose significant risks to the integrity, availability, and confidentiality of medical supply chains, potentially impacting patient safety and the overall functioning of healthcare systems. There is an urgent need to provide a solution where manufacturers, supply chain stakeholders and users can easily identify, estimate, mitigate, and audit all cybersecurity risks of connected devices (hardware, software, integrated medical frameworks consisting of various modular components) by design, ensuring their security and resilience, towards a resilient and trustworthy healthcare ecosystem.

Another challenging dimension is the regulatory compliance for these connected medical devices. In the EU, the first piece of guidance was issued in July 2019 by the Medical Devices Coordination Group (MDCG) [10]. The EU included the health sector among its critical information infrastructures developing cybersecurity legislation and directives which impose cybersecurity and privacy risk management (e.g., GDPR, NIS), supply chain security (e.g., NIS 2), secure authentication and access of healthcare e-services (e.g., eIDAS), and cybersecurity certification (e.g., Cybersecurity Act, Liability Act, Chip Act) [11]. Medical devices will enhance their trustworthiness, interoperability, and marketing opportunities if the manufacturers assess the risks of their devices, agree upon a cybersecurity schema defining the security requirements, functions, and controls, and pursue a cybersecurity security certification. Only then will the single digital market and the medical industry gain the necessary public trust that their medical devices provide a certain level of cybersecurity. In fact, the healthcare industry is regulated as a critical sector by Directive (EU) 2016/1148, in which cybersecurity certification is of the utmost importance.

In this context, this work presents a unique set of security management services within the context of an agile information security management system, including the introduction of a Risk and Conformity Assessment (RCA) framework that aims for an effective risk management and compliance assurance practice for the healthcare sector. The key contributions of this paper are summarized as follows:

- A novel, dynamic, and evidence-based Risk and Conformity Assessment (RCA) Framework for manufacturers and healthcare organizations to conduct their risk assessments and for auditors to assess the conformity of the claims reported in the security profiles of medical devices.
- A Certification Scheme adapted from ENISA certification (EUCC), tailored for medical devices and their supply chains.
- An agile, extended Information Security Management System (ISMS), through which the RCA and certification are implemented as a bundle of security management services.

The proposed framework and certification scheme and their integration into an agile ISMS aim towards the implementation of the EU Cybersecurity Act [12], promote relevant regulatory requirements (e.g., ISO/DTR 22696, (EU) 2017/745, (EU) 2017/746, NIS, (EU) 2019/881, GDPR Regulation (EU) 2016/679), security standards (e.g., ISO/DTR 22696, ISO/AWI 22697, ISO15408, ISO18045, ISO2700x series), guidelines, and best practices (e.g., ENISA 2020, MDCG 2019–16) by: (i) Supporting manufacturers to certify the security of their connected medical devices and increase their trustworthiness and preparedness; (ii) Improving their cooperation with each other; (iii) Adopting appropriate steps to manage security risks; (iv) Advancing ways to report and handle security incidents; and (v) Enabling them to analyze relevant privacy concerns. Finally, this framework aims to establish an environment of trust and confidence for European consumers, including healthcare organizations and stakeholders such as providers, suppliers, and integrators,

paving the way for a competitive and trustworthy Digital Single Market (DSM).

The structure of this paper is as follows: Sect. 2 outlines the State-of-the-Art in the healthcare domain, specifically healthcare devices, and its supply chains; attack vectors and attack types in medical devices; attacks in medical supply chains; cybersecurity frameworks; risk assessment frameworks; standards for both medical devices and supply chains; certification schemes. Sections 3, 4 and 5 describe the scientific, technical, and research methodology of the RCA Framework, the proposed Cybersecurity Certification Scheme for medical devices and supply chains, and the high-level architecture of the agile ISMS. Section 6 concludes with final thoughts and suggestions for future work, including practical, real-life applications that the framework is designed to cover.

2 Background

This section provides background information on the healthcare and supply chain domains, discusses specific cybersecurity attacks affecting the healthcare sector, and reviews relevant frameworks for this work.

2.1 Healthcare domain and its supply chain

This section provides an overview of various categories of legacy medical devices used in healthcare. These devices serve different purposes, including treating diseases, diagnosing ailments, controlling conditions, conducting in vitro diagnostic tests, and incorporating medical IoT and wearable sensor technologies. These advancements in medical technology have significantly improved patient care and healthcare outcomes, offering personalized and connected healthcare solutions [13].

- *Legacy medical devices to treat diseases* Surgical instruments, implantable devices, prosthetic devices, infusion pumps, ventilators and respiratory devices, dialysis machines, radiation therapy devices, diagnostic imaging equipment.
- *Legacy medical devices to diagnose diseases* Diagnostic Imaging Equipment (X-Ray machine, computed tomography, magnetic resonance imaging, ultrasound machines), Laboratory testing devices (blood analyzers, microscope, point-of-care testing), Endoscopes (gastroscopes, colonoscopes), Electrocardiography devices (ECG, EKG), diagnostic analyzers (immunoassay analyzers, genetic sequencers), spirometers, blood pressure monitors, etc.
- *Legacy Medical devices to control diseases* Drug delivery devices (inhalers, insulin pumps, autoinjectors), Pain Management Devices: (Transcutaneous Electrical Nerve Stimulation Devices), implantable Pain Pumps, neurostimulators, Therapeutic devices (pacemakers, implantable Cardioverter Defibrillators, deep Brain Stimulation (DBS) Devices, continuous Positive Airway Pressure (CPAP) Machines), rehabilitation and Assistive Devices (Prosthetic Limbs, orthotic Devices, Mobility Aids), remote monitoring Devices (Remote Cardiac Monitors, Remote Glucose Monitors, Telehealth Devices).
- *Legacy* In vitro*diagnostic devices* Clinical Chemistry Analyzers, Immunoassay Systems, Molecular Diagnostic Devices, Point-of-Care Testing (POCT) Devices, Hematology Analyzers, Microbiology Culture Systems, Coagulation Analyzers, Urinalysis Analyzers.
- *Medical IoT devices* Wearable health trackers, remote patient monitoring devices, smart pill bottles, connected insulin pumps, telehealth devices, smart implantable devices, connected medical equipment, smart beds, and monitoring systems [14].
- *Wearable sensors* Motion detection sensors, pressure sensors, temperature sensors, chest straps (ECG sensor), glucose level monitoring, smart soles (GPS-based), wireless fetal monitoring, and smart clothing.

2.2 Cyber-attack in the healthcare sector

There are primarily three (3) attack vectors similar to other infrastructures through which connected medical devices can be compromised [15]:

1. *Devices* Device vulnerabilities in their memory, firmware, physical interface, web interface, and network services are exploited by cybercriminals. Furthermore, other factors like unsecured default settings, outdated components, and insecure update mechanisms can also be manipulated. Legacy devices that are outdated and lack necessary patches are particularly targeted due to their vulnerable state.
2. *Communication channels* Device compromises can occur when the communication channels connecting it to other devices are targeted. This vector often involves common attacks such as spoofing and Denial-of-Service (DoS). Traditional Wireless Sensor Networks (WSNs) consist of wireless nodes equipped with antennas that transmit radio signals in all directions, making them vulnerable to eavesdropping attacks. By intercepting this data, an attacker can masquerade as an authorized member and launch an impersonation attack. Consequently, eavesdropping becomes a straightforward task for the attacker when patient data is being transmitted from the body area network to the caregiver device, resulting

in a breach of patient privacy. Examples: Wi-Fi, Bluetooth, cellular networks, Zigbee, NFC, Ethernet, MQTT, LoRaWAN.
3. *Applications and software* Malicious cybercriminals have the ability to exploit weaknesses found in web applications and the associated software used for connected devices. For instance, these web applications can be specifically targeted with the intention of pilfering user credentials or injecting malware.

Cyber-attacks are a growing concern in the healthcare sector and the overall medical supply chain, as they involve deliberate and targeted breaches that exploit vulnerabilities within the supply chain of healthcare systems, devices, or pharmaceutical products. These attacks aim to compromise the integrity, availability, or confidentiality of medical supplies, posing significant risks to patient safety and privacy. By infiltrating the supply chain, cybercriminals can introduce counterfeit or compromised products, manipulate the distribution process, or gain unauthorized access to sensitive information. Such attacks not only disrupt the seamless flow of medical supplies but also undermine the trust and reliability of the entire healthcare system. It is imperative for healthcare organizations to implement robust security measures and collaborate with supply chain partners to mitigate these risks and safeguard patient well-being. Examples of medical supply chain attacks:

1. *Counterfeit products* Involves the introduction of counterfeit or substandard medical products into the supply chain. Attackers may create fake pharmaceuticals, medical devices, or supplies that mimic genuine products, posing risks to patient health and treatment outcomes [16].
2. *Unauthorized modifications* Unauthorized modifications to medical devices or components during the manufacturing or distribution process. This can involve tampering with the hardware, firmware, or software of medical devices, potentially compromising their functionality or introducing vulnerabilities [17].
3. *Supply chain data breaches* Breaches of sensitive data within the supply chain, including personal, medical, or financial information. Attackers may target suppliers, distributors, or logistics companies to gain unauthorized access to confidential information or exploit it for malicious purposes [18].
4. *Software or firmware attacks* Malicious modification or insertion of software or firmware into medical devices during the manufacturing or distribution process. This can include the introduction of malware, backdoors, or other malicious code that compromises the security or functionality of the devices [19].
5. *Supply chain disruption* Attacks aimed at disrupting the supply chain of critical medical supplies, devices, or pharmaceuticals. This can involve physical attacks on warehouses, transportation networks, or production facilities, leading to delays, shortages, or compromised availability of essential medical resources [20].
6. *Supply chain interception or diversion* Interception or diversion of medical supplies during transportation or distribution. Attackers may steal or redirect shipments, leading to supply shortages, compromised product integrity, or delays in healthcare delivery [21].

2.3 Cybersecurity certifications, schemes, acts and standards

Cybersecurity act (CSA): The CSA (Regulation (EU) 2019/881 [22]) was enforced as part of a wide-ranging set of measures to deal with cyber-attacks and to build strong cybersecurity in the EU. It strengthens the ENISA by granting the agency a permanent mandate, reinforcing its financial and human resources, and overall enhancing its role in supporting the EU to achieve common and high-level cybersecurity. CSA establishes the first EU-wide cybersecurity certification framework for products and services to ensure a common cybersecurity certification approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g., IoT) and services.

ENISA European cybersecurity certification scheme (EUCC): Given the large diversity and many uses of ICT products, the European Cybersecurity Certification framework [23] enables the creation of tailored and risk-based EU certification schemes. The European Cybersecurity Certification Scheme on Common Criteria, the first scheme, targets ICT products such as hardware and software products and components. ENISA, with the support of an Ad-Hoc Working Group and the Member States, developed the candidate scheme, which received a positive opinion from the Member States represented at the ECCG (The European Cybersecurity Certification Group). The scheme was passed to the European Commission to be transformed into an Implementing Act. Once done, the certification scheme enters into force. EUCC serves as a template in order to propose security certification schemes for ICT products. Based on Article 54 of the CSA, a European cybersecurity certification scheme shall include at least the following elements: the subject matter and scope of the certification scheme, including the type or categories of ICT products covered. Using the EUCC, any ICT product can serve as a Target of Evaluation (TOE) and be the subject of a security evaluation, also known as a Conformity Assessment (CA), in which it is assessed against security requirements described in the security profile. Conformity assessment is based on ISO 15408 and ISO 18045

standards for the use of the concepts of Protection Profile (PP) and Target of Evaluation (TOE), as well as the Vulnerability Analysis (VA) assurance family, AVA_VAN. It also consults the Security Functional Requirements (SFRs) that are defined in CC as a translation of the security objectives for the Target of Evaluation (TOE) into a standardized language, the implementation of which addresses the threats of counterfeited or tainted products and components. ISO/IEC 15408 also provides a methodology to help an IT security evaluator conduct a CC evaluation by defining the minimum actions to be performed.

Cyber resilience act (CRA): The CRA [24] is the first-ever EU-wide legislation of its kind: it introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. It will ensure that wired and wireless products that are connected to the internet and software placed on the EU market are more secure and that manufacturers remain responsible for cybersecurity throughout a product's life cycle. It will also allow the customers of these products to be properly informed about the cybersecurity of the products they buy and use.

Network and information security (NIS) and NIS2: The NIS Directive imposes cybersecurity obligations on essential service operators, including healthcare providers, within EU member states. It mandates the implementation of measures to manage cybersecurity risks, ensures preparedness for incidents, and report significant cyber incidents to the relevant authorities. The NIS2 Directive is an updated EU-wide legislation that enhances cybersecurity measures to keep pace with increased digitization and evolving cyber threats. NIS2 [25] expands the scope of the directive to include new sectors and entities, strengthening the resilience and incident response capabilities of public and private entities, competent authorities, and the EU as a whole. Unlike the previous version (NIS1), NIS2 applies to a wider range of essential service operators and digital service providers, such as energy, transport, banking, healthcare, online marketplaces, and search engines. The objective is to establish a consistent level of security across the EU by requiring organizations to implement appropriate security measures and report significant incidents. NIS2 extends the directive's coverage to additional industries, including water supply, food supply, and digital infrastructure. The expansion reflects the increasing importance of digital infrastructure and the need to enhance the resilience of networks and information systems in various sectors.

ISO/IEC 15408 (particularly the common criteria—CC): ISO/IEC 15408 [26], commonly known as the Common Criteria (CC), is a widely recognized international standard for evaluating and certifying the security of information technology products and systems. It provides a framework for assessing the security functionality and assurance of these products and systems. While the CC itself is not specific to any particular industry or domain, it can be applied to various sectors, including the healthcare domain. Healthcare organizations can use the CC as a basis for evaluating and selecting secure IT products and systems to protect sensitive patient information and ensure the security of their infrastructure. It is important to note that ISO/IEC 15408 and the CC provide a standardized methodology for security evaluation and certification, but their application and adoption within the healthcare domain may vary depending on specific regulatory requirements and organizational needs. Healthcare organizations should consider their unique security requirements and applicable regulations when utilizing ISO/IEC 15408 and the CC in their IT procurement and security processes.

2.4 Healthcare standards

MDCG 2019-16—Guidance on cybersecurity for medical devices MDCG**Error! Bookmark not defined.** offers cybersecurity guidance for medical devices in the healthcare domain. It addresses unique risks, safeguards sensitive data, and ensures safe device operation. The aim is to assist manufacturers and healthcare organizations in implementing effective cybersecurity measures throughout the device lifecycle. Compliance enhances device cybersecurity and supports overall healthcare domain security and privacy.

ISO 13485: ISO 13485 [27] is an international standard for quality management in medical devices, covering the entire lifecycle. It ensures safety, effectiveness, and compliance with regulations. Implementing it establishes a robust QMS, producing reliable devices and demonstrating adherence to standards. Certification provides assurance to healthcare providers and patients, but it's not mandatory everywhere, as requirements vary.

ISO 14971: ISO 14971 [28] is an international risk management standard for medical devices. It's vital for manufacturers and healthcare organizations to ensure device safety and regulatory compliance. Following ISO 14971 enables stakeholders to identify, evaluate, and control risks throughout device lifecycles, minimizing potential harm. Widely recognized, this standard supports the goal of providing high-quality healthcare services.

IEC 62304: the IEC 62304 [29] is a standard for medical device software in the healthcare domain. It guides the entire software lifecycle, covering development, maintenance, and risk management. It ensures safety and effectiveness by providing a structured framework for design, verification, and validation. Compliance with IEC 62304 is crucial for regulatory approvals of medical devices with software components.

IEC 62366-1: IEC 62366-1 [30] is an international standard for usability engineering in the healthcare domain.

It emphasizes considering user experience during medical device development. Essential for manufacturers, healthcare organizations, and stakeholders, it ensures user-centered devices, reducing errors and hazards. Compliance is usually required by regulators to demonstrate human factors integration in device design, ensuring safe and usable medical devices in the healthcare domain.

IEC 80001-1: IEC 80001-1 [31] is an international standard for integrating medical devices into healthcare IT systems. It focuses on safe and effective integration, providing risk management guidance for IT networks. Relevant for healthcare organizations and IT professionals, it ensures proper functioning, interoperability, and cybersecurity of medical devices within these networks. Compliance aligns IT infrastructure with international standards, ensuring seamless integration while considering patient safety and regulatory requirements.

IEC/TR 80002-1,-2,-3: The IEC/TR 80002-1, -2, and -3 standards apply to healthcare and offer guidance on using ISO 13485 for medical device software. IEC/TR 80002-1 focuses on software as a medical device (SaMD), IEC/TR 80002-2 covers agile software development, and IEC/TR 80002-3 addresses software life cycle processes. These standards help align software practices with ISO 13485, ensuring quality and regulatory compliance for safe and effective healthcare use. Following them enables organizations to develop high-quality software that promotes patient safety and meets industry standards.

ISO 13482: ISO 13482:2014 [32] is a standard for safe design and use of personal care robots, aiming to improve users' quality of life. It addresses hazards, provides risk reduction measures, and focuses on physical contact applications. It excludes specific robot categories like high-speed, toy, industrial, and medical robots. The standard primarily deals with human care hazards, including domestic animals and property where relevant. It covers significant hazards and situations but notes the lack of internationally recognized data on impact-related hazards.

2.5 Healthcare supply chain standards

GS1 healthcare supply chain standards (GS1): GS1 [33] is a non-profit organization that develops and maintains standards across industries, including healthcare. In healthcare, GS1 has created the GS1 Healthcare Supply Chain Standards to improve the efficiency and traceability of the healthcare supply chain. These standards provide a unified framework for identifying and sharing data on healthcare products. Implementing these standards helps healthcare organizations optimize inventory management, reduce errors, streamline product recalls, and ensure product safety. Other industry-specific standards, like HSCA, HIDA, and EFPIA, also exist to address unique healthcare supply chain challenges and promote best practices.

Fig. 1 AI-based risk assessment and conformity (RCA) framework

NIST SP 800-161: supply chain risk management practices for federal information systems and organizations. It primarily targets federal information systems and organizations, and its principles and guidelines can be extended to the healthcare domain. Healthcare organizations can apply the practices outlined in NIST SP 800-161 [34] to effectively manage and mitigate supply chain risks, particularly concerning the security and integrity of medical devices, software, and other technology components. By implementing robust supply chain risk management practices, healthcare organizations can enhance the security, reliability, and trustworthiness of their information systems and the products and services they rely on. However, it's essential for healthcare organizations to also consider industry-specific standards, guidelines, and regulations that specifically address cybersecurity and supply chain risk management in the healthcare sector.

3 Risk and conformity assessment (RCA) framework

This section introduces the proposed RCA framework, which integrates AI models to assess and manage risks while supporting continuous conformity assessment. The use of AI in the RCA framework offers numerous benefits, including enhanced data processing capabilities and the ability to forecast potential risk scenarios. Additionally, AI-based solutions are scalable and adaptable, effectively handling the increasing complexity and volume of data in today's digital landscape. Figure 1 illustrates the RCA framework, which comprises seven key components, each sequentially linked

to support comprehensive risk and conformity assessment. An overview of each component is provided below:

- *Data collection* Utilize AI algorithms to collect and analyze relevant data from various sources, such as system logs, network traffic, and security incident reports. AI can automatically process large volumes of data and identify patterns, anomalies, and potential security risks**.**
- *Risk assessment with AI* Employ AI techniques, such as machine learning and data analytics, to perform advanced risk assessments based on analysing large data. AI algorithms can analyze historical data, identify emerging threats, and predict potential security risks more accurately and efficiently. This enables organizations to proactively address security vulnerabilities and informed decision making to prioritize risk treatment measures.
- *Automated security control implementation* AI-driven automation tools facilitate the streamline the implementation of security controls. AI can assist in automating the deployment and configuration of security solutions, such as firewalls, intrusion detection systems, and encryption mechanisms. This reduces human error and ensures consistent implementation across the organization's IT infrastructure.
- *Continuous monitoring with AI* Implement AI-powered monitoring systems to continuously analyze security events and detect potential threats in real-time. AI algorithms can analyze network traffic, system logs, and user behavior to identify abnormal activities or indicators of compromise. This enables organizations to respond quickly to security incidents and minimize the impact of potential breaches.
- *AI-enabled security evaluation* Enhance the security evaluation process by incorporating AI capabilities. AI algorithms can analyze the effectiveness of implemented security controls, identify weaknesses or gaps, and provide recommendations for improvement. AI can also assist in automating the evaluation process, reducing manual effort and accelerating the certification timeline.
- *Adaptive security controls* Leverage AI techniques to develop adaptive security controls that can learn and adapt to evolving threats and changing environments. AI algorithms can continuously analyze and assess the effectiveness of security controls, making adjustments and optimizations based on real-time data. This ensures that the security posture remains robust and up to date.
- *Intelligent reporting and documentation* Utilize AI technologies to generate intelligent reports and documentation for security certification purposes. AI algorithms can automatically extract relevant information, analyze evaluation results, and generate comprehensive and standardized reports. This saves time and effort for auditors and facilitates the certification process.
- *AI-driven compliance monitoring* Employ AI-powered tools to monitor and ensure ongoing compliance with security standards and regulations. AI algorithms can assess the organization's adherence to security policies, detect policy violations, and recommend corrective actions. This helps maintain a continuous state of compliance and reduces the risk of security breaches.

3.1 Mapping the RCA components with the existing standards

The main innovation of the RCA Framework is the integration of AI technologies throughout its various components for risk assessment, conformity assessment, and security evaluation processes. By leveraging AI capabilities, this framework enhances the efficiency, accuracy, and effectiveness of these processes in both ISO 27001/27002 and ISO/IEC 15408 contexts. Figure 2 depicts how the existing standards can be mapped with different components of the RCA. Below, there is a description of the aspects considered in each step with respect to the ISO standards:

1. *Data collection* Relevant data about assets, threats, vulnerabilities, and impacts need to be collected for comprehensive risk assessment. In security evaluation, data collection is essential to evaluate security functions, vulnerabilities, and assurance measures of a product or system.
2. *Risk assessment with AI* AI can analyze the collected data to identify patterns, assess likelihoods, and evaluate potential impacts of risks. It also highlights the use of AI in risk assessment for ISO/IEC 15408, where AI can analyze historical data, identify emerging threats, and predict potential security risks with higher accuracy.
3. *Automated security control implementation* AI-driven automation tools are used to streamline the implementation and configuration of security controls ensuring consistent and efficient deployment of security solutions, as well as adherence to security standards.
4. *Continuous monitoring with AI* Continuous monitoring is crucial for effective risk management, and the RAC framework analyses security events, network traffic, and system logs in real-time, AI can help detect potential threats promptly. AI-powered continuous monitoring can assess the effectiveness of implemented security controls, identify weaknesses or gaps, and provide recommendations for improvement.
5. *AI-enabled security evaluation* AI can assist in evaluating the effectiveness of implemented security controls, identifying weaknesses, and providing recommendations for improvement by automating the evaluation process and

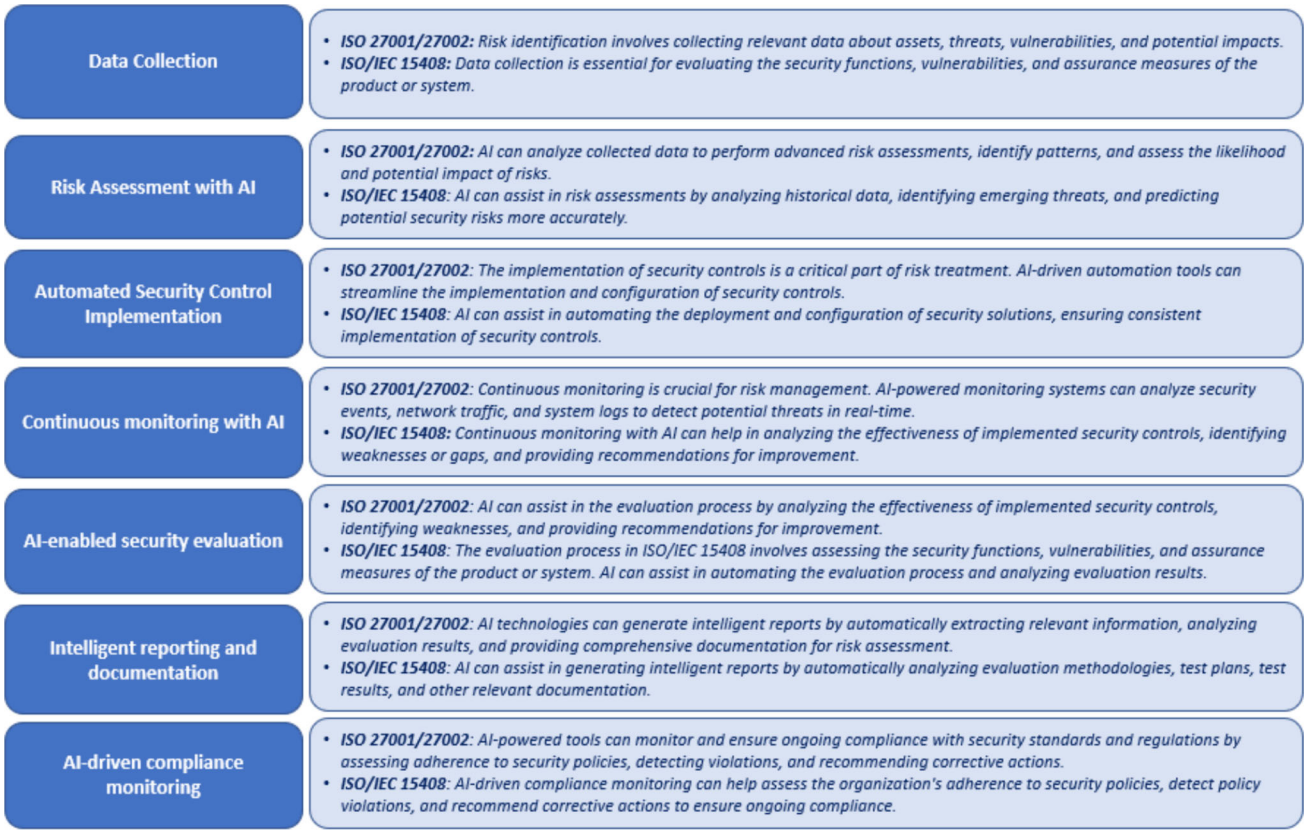

Fig. 2 Mapped standards to the AI-based RCA framework

analyzing evaluation results, AI streamlines the assessment of security functions, vulnerabilities, and assurance measures of a product or system.

6. *Intelligent reporting and documentation* AI technologies are used in generating intelligent reports and comprehensive documentation for risk assessment and security evaluation by automatically extracting relevant information and analyzing evaluation results, AI can assist in creating insightful reports.
7. *AI-driven compliance monitoring* AI-powered tools are leveraged to ensure ongoing compliance with security standards and regulations. AI can monitor adherence to security policies, detect violations, and recommend corrective actions enabling organizations to maintain a proactive approach to compliance and address potential policy violations promptly.

3.2 Incident report and handling

The RCA framework enables cyber-security for medical devices and healthcare systems with sophisticated incident reporting and handling capabilities. It also uses AI-driven continuous real-time monitoring. This section however breaks down in details the technical parts of those features.

AI-Powered continuous monitoring and real-time incident detection [35]**:** The RCA framework includes an advanced AI-driven continuous monitoring system that utilises sophisticated machine learning algorithms for the real-time detection and classification of potential security problems. This system initiates with extensive data ingestion, gathering information from several sources such as network traffic logs, system and application logs, security device logs, and medical device telemetry data. The imported data undergoes feature extraction, isolating important characteristics such as network connection patterns, user behaviour metrics, system resource utilisation, and medical device operational parameters for study. This extracted feature set serves as the foundation for the ensuing anomaly detection and threat classification procedures.

Integration with existing incident response processes and tools [36]**:** The anomaly detection phase uses unsupervised machine learning methods, notably Isolation Forests and Gaussian Mixture Models (GMMs), to detect anomalies in behavior patterns in the extracted features. In this context, these algorithms work well because of their ability to identify

outliers in high-dimension spaces, which is crucial for detecting rare instances in complex healthcare settings. At the same time, a supervised machine learning model that has been pre-trained with historical incident data and known threat patterns, categorises these detected anomalies under specific threats. Advanced classification algorithms like Random Forests, Support Vector Machines or Deep Neural Networks have been employed in this model to classify potential threats with higher accuracy resulting in swift and accurate incident response. The system performs automated prioritization and alerting of detected threats, so that incidents are addressed in the order they should be using real-time notifications based on the severity and confidence level of threat detection.

Automated incident reporting features [37]**:** This is imperative for the RCA framework to fit within present incident response processes in a smooth fashion. RESTful APIs for integration with SIEMs, ticketing systems and incident response platforms. The framework adopts common data formats of industry (e.g., STIX, TAXII) so as to be compatible and expediate information sharing with current tools in security space. The solution provides a configurable workflow engine that automatically manages important incident response procedures: ticket creation, escalation, and initiation of predefined responses. It also offers customisable incident response playbooks to fit your organisations specific needs. The framework also comes with an extensive reporting that uses NLP techniques to generate detailed incident reports, dynamic notification of stakeholders, and regulatory-based compliance reporting suitable for healthcare regulations. Using this, you can create interactive dashboards and visualizations that are paired with reporting features powered by machine learning (ML) designed to give your stakeholders the important insights they need and time them at scale so that your security and operations teams can continually improve incident response procedures.

Asset management and supply chain visibility [38]: The framework incorporates Software Bill of Materials (SBOM) as a critical component of asset identification and management, particularly for addressing supply chain-related security risks. An SBOM provides a detailed, machine-readable inventory of software components, dependencies, and supply chain relationships within medical devices and healthcare systems. By integrating SBOMs, organizations can gain visibility into the software makeup of their systems, identify vulnerabilities, and ensure the integrity of their software supply chain.

To ensure the framework aligns with industry standards and regulatory requirements, we plan to integrate widely adopted SBOM formats, such as SPDX (Software Package Data Exchange), CycloneDX, or SWID (Software Identification Tags). These standardized formats are supported by numerous tools and frameworks, enabling interoperability and seamless integration into existing workflows. SBOMs will be created using automated tools capable of extracting software component data, including dependencies, libraries, and package versions, directly from source code repositories, build environments, or deployed applications. Tools such as dependency scanners, binary analyzers, or SBOM generation tools (e.g., Syft or SBOM generators from CI/CD pipelines) will ensure accuracy and efficiency in compiling these inventories.

The integration of SBOMs into the framework will occur during the asset identification phase, where they will serve as a foundational data source for subsequent assessment phases. SBOMs will be linked to vulnerability databases (e.g., NVD or private vulnerability feeds) to facilitate automated vulnerability scanning, enabling the identification of known risks in software components. Furthermore, the SBOM data will be correlated with risk analysis and compliance assessment phases, ensuring that vulnerabilities and dependencies identified in the SBOMs are evaluated in the context of organizational security policies and regulatory requirements.

This linkage between SBOMs and other assessment phases will also support enhanced incident response capabilities. For example, in the event of a newly discovered vulnerability or a supply chain attack, SBOMs can be referenced to quickly determine which systems or components are impacted and require remediation. Additionally, SBOM data will feed into the risk modeling and prioritization processes, enabling organizations to focus on high-risk components or dependencies with significant potential impact.

By incorporating SBOMs into the framework, we align with modern cybersecurity best practices, including those outlined in regulatory guidelines such as the U.S. Executive Order 14,028 on Improving the Nation's Cybersecurity, which mandates SBOM usage for transparency in the software supply chain. This integration empowers healthcare organizations to maintain a robust security posture by fostering transparency, enabling automated security assessments, verifying compliance, and responding promptly to emerging threats in their software ecosystems. Through this approach, SBOMs become a cornerstone of a comprehensive risk and conformity assessment process, directly contributing to enhanced security, resilience, and trust in healthcare systems and their software supply chains.

3.3 Detailed implementation of RCA components

3.3.1 Data collection and anomaly detection

The RCA framework enhances data collection and analysis by leveraging a combination of machine learning (ML) algorithms designed to efficiently gather and examine data from multiple sources. It employs Natural Language Processing (NLP) algorithms, such as BERT, to process unstructured text data found in system logs, security incident reports,

and other sources. BERT's contextual understanding enables the extraction of meaningfully relevant information from complex security reports. The framework also deploys Convolutional Neural Networks (CNNs) to analyze real-time network traffic and detect deviations from normal patterns. Although CNNs are commonly used for image recognition, here they identify spatial dependencies within traffic flows, enabling the detection of anomalies like Distributed Denial of Service (DDoS) attacks and malicious packet signatures. For identifying long-term temporal anomalies, the framework utilizes Long Short-Term Memory (LSTM) networks. LSTMs, a type of recurrent neural network, are well-suited for analyzing system logs over extended periods, allowing for the detection of slow-developing anomalies that may indicate stealthy, persistent attacks. This approach improves the accuracy of anomaly detection processes. Additionally, Isolation Forests are used to detect point anomalies in high-dimensional datasets, One-Class Support Vector Machines (SVMs) identify novel patterns in network traffic, and Autoencoders facilitate unsupervised anomaly detection within system logs. These models work in ensemble, and their predictions are aggregated using a weighted voting mechanism. Model weights are adjusted based on performance metrics, allowing the framework to evolve and improve over time. All data and model outputs are stored in a distributed NoSQL database, providing scalable, real-time data access for swift anomaly detection and analysis.

3.3.2 Risk assessment and analysis

The risk assessment process in the RCA framework is even multifaceted and brings together different advanced machine learning algorithms and probabilistic models to optimally identify a profile of security risks. The framework uses Bayesian Networks to model relationships between different components in the system, and quantitatively determine probability of potential security compromises. These networks help to model conditional probabilities, causing one to have a more detailed insight into how things like mobile phone exposure or network frailties end up in complete fledged incidents. At the same time, Random Forest classifiers are used to estimate the probability of various security incidents based on historical data. These classifiers examine information related to previous attacks, flaws, and system conditions to determine which types of incidents are the most likely. Then they use Gradient Boosting Machines [39] (GBMs) to recognize which are the key features contributing towards security risk. Mitre's model is set up to focus on remediation of a limited number of vulnerabilities, hopefully the ones that have the largest impact. These have been trained off a vast dataset of past incidents as well as vulnerability reports and risk scenarios that experts in the security domain annotated. Transfer learning techniques [40] are integrated into the training process, by using pre-trained models from a related domain to improve the accuracy and generalisation of healthcare risk assessments.

3.3.3 Continuous monitoring and adaptive security controls

The RCA framework has a continuous monitoring system fuelled by a real-time streaming analytics pipeline with Apache Kafka and Apache Flink. With these tools, security events and system logs are processed in real-time to keep the anomaly detection models up-to-date with fresh data. The pipeline works in real time, ensuring that threats are detected very soon after they occur so mitigation can take place in a timely manner. Further, online learning algorithms are used to update and refine the anomaly detection model so that they stay efficient in tracking new and changing threats. It could leverate adaptive security controls using Reinforcement Learning [41] (RL) to make the system more resilient. By studying historical data and simulating attack scenarios, Deep Q-Networks (DQNs) can automatically adapt firewall rules so as to effectively block hostile traffic without causing inconvenience to security respecting users. Policy Gradient methods [42] also allow for dynamic access control policy tuning. These tools alter security policies according to continued evaluations of the risk scenarios, which is in sync with the changes made to access controls at any point in time due to movement between perceived risk levels. Keep training the reinforcement learning agents in the simulation tool, based on both historical incident data and synthetic scenarios generated by adversarial ML models to resemble the real system as close as possible. These adversarial models resemble the attack vectors, i.e., they provide a wide variety of scenarios for the RL agents to be trained and tested. This learning method is in place to ensure the responsiveness of current security policies and controls against emerging threats, which ultimately translates into enhanced threat detection with naturally less false positives.

3.4 Automated security control implementation

The RCA framework employs AI-driven automation tools to streamline the implementation of security controls. This process is designed to be both efficient and safe, with multiple layers of checks and balances to prevent unintended consequences. Here's a detailed explanation of how this system operates:

3.4.1 System access and integration

The RCA framework can be integrated with existing systems of IT infrastructure management through secured APIs and Professional Access Management (PAM) vendor solutions. With this model, the AI-based system can continue

to interact safely with vital network devices, servers and applications. Integration lets the system read in required configuration state, logs and live network data without access to make any changes within control being rigidly maintained. When enabling a change, the system checks if it is permitted to make changes through PAM before making any security alterations. This method of secure access is used to prevent unauthorized tampering with system configs and keep the risk-free IT environments from being potentially misused / vulnerable through excessive privileges.

3.4.2 Security control selection and configuration

AI systems guide organizations in selecting security controls based on a comprehensive knowledge base of security practices, vendor configuration guides, and regulatory requirements. They consider factors like device type, current threat environment, organizational security policies, and regulatory requirements. For example, a firewall setup involves analyzing network traffic patterns and focusing on essential services. The system then customizes predefined rule templates based on industry guidelines and best practices, ensuring firewalls balance security and performance requirements, meeting both organizational and statutory obligations.

3.4.3 Staged implementation and testing

The AI system implements new security settings through a phased approach. The system simulates proposed controls in a virtualized manner, allowing for changes to be evaluated without impacting live nodes. Issues are captured and tested before being put into use. After a controlled rollout, changes are pushed to a small percentage of devices, monitored for performance and security metrics. The system then incrementally expands, touching larger network portions, continuously validating and monitoring each step.

3.4.4 Safeguards and human oversight

The process contains multiple safeguards that would block accessing functions that may be lethal, especially those shutting down key infrastructure operations. The utility comes with a predefined set of safety checks, in which it would analyze the intended plan and warn the user against doing something risky like blocking all outbound network connections or disabling some important services. These become a failsafe mechanism—simply forcing the AI system not to act in manners already known ahead that significantly compromise its organizational operation. The entire process is accompanied by a human approval flow to help release more critical changes. Individuals need to review and approve changes that involve high-impact security measures before they are made by the system. The proposed changes are highlighted to the IT security staff who can then accept, modify, reject them based upon their knowledge/understanding of the current operational environment. Ongoing monitoring is also carried out after deployment for any performance or security exceptions that arise and if so the system will notify human operators to take further action.

3.4.5 Tool selection and vendor integration

The framework uses an AI system to evaluate security tools based on their capabilities and interoperability. It assesses the effectiveness of each tool in addressing security requirements and determines if it is more beneficial in the current situation and can provide long-term value. The system uses vendor-provided APIs and management interfaces to deploy and manage these tools, including intrusion detection systems, firewalls, and encryption methods. The framework ensures its connection protocols are always current, minimizing manual updates and reducing security vulnerabilities. This integration facilitates efficient tool deployment and maintenance across infrastructure, ensuring uniform and seamless security management.

3.5 Detailed risk management process

3.5.1 Asset inventory identification and management

The RCA framework is a dynamic asset identification system that focuses on understanding the security landscape of the healthcare environment. It uses AI-powered network surveillance tools to automatically identify and log all connected devices and systems, covering everything from medical devices to IoT. The system ensures an up-to-date inventory of all assets, which is crucial for building a correct security profile. Assets are classified based on their purpose, kind, and essentialness for the healthcare operation, prioritizing high-risk and mission-critical assets. Graph-based AI models are used for dependency mapping, allowing visual depiction of asset connections and identifying crucial dependencies. AI-based monitoring systems in healthcare provide real-time asset inventory with regular updates, ensuring the system remains up-to-date.

3.5.2 Risk analysis and categorization

Once the assets are identified, a complete risk identification, analysis and categorization process is carried out by the RCA framework based upon unique vulnerabilities and threat actors linked to each asset. It initiates with AI-backed Threat Modelling, a targeted intelligence platforms that analyses historical attack data, current thread landscapes and future

probability of threats specific to each kind of asset. The system processes the data using machine learning models and is able to discern patterns denoting potential threats, which are thereafter cross-referenced with industry-wide data to provide a full threat profile. Having conducted the AI-driven vulnerability assessment [43], the system uses automated vulnerability scanners to check software packages, configuration settings and known vulnerabilities for each asset. Even more so in medical devices and other systems that incorporate proprietary software that may not be patched as regularly, leading to potential security holes. The task is further followed by impact analysis, where the system makes use of ML models to predict the eventualities in case security attacks occur. The analysis takes into account factors including patient safety, data protection, regulatory standards and financial costs of system downtime. Moreover, the multi-factor risk scoring algorithm calibrates risk scores based on real-time threat intelligence and zero-day discovered vulnerabilities. AI-driven visualization tools interpret risk analysis output through production of heat maps, risk matrices and trend analyses that provides decision makers with a powerful view to prioritize risk mitigation efforts.

3.5.3 Risk treatment and mitigation strategies

Utilizing AI-assisted tools, our RCA framework provides risk treatment and mitigation strategies. AI algorithms recommend automated controls and analyzed investment and risk features of each asset. All the recommendations which are according to standard industrial standards and regulatory policies will make sure that however apparently ideal a strategy is, it must be practical as well. Based on effectiveness, costs/time and implementation difficulty Machine learning models rank the actions and Security team saves many efforts focusing only high impact risks Artificial intelligence (AI) simulation models forecast the efficacy of mitigation strategies and thus highlight where to allocate resources efficiently. The framework iteratively assesses the effectiveness of controls as they are implemented, and adjusts in response to new threats which continuously adapt security posture based on changing risk.

3.6 Real-world implementation of the RCA framework

To demonstrate the practical application of the RCA framework in a real-world scenario, we implemented a prototype system at a mid-sized regional hospital. This implementation focused on securing the hospital's network of connected medical devices, including infusion pumps, patient monitors, and imaging equipment.

3.6.1 Data collection and AI integration

The system collects data to be analyzed and identify security threats, but with combinations of both supervised and unsupervised machine learning strategies during the process. To conduct network traffic analysis, we replaced the intrusion detection system (IDS) with a deep learning (DL) approach to build up IDS using LSTM networks [44]. To build the LSTM model, the researchers trained it on normal network activity and known attack signatures for medical devices. By recognizing changes from the baseline, they trained the system to detect a security incident in real-time. Extensive experiments show that the LSTM-based IDS manages to detect important portion of anomalous traffic patterns with an accuracy rate of 97% by leveraging which it could increase hospital's capability for identifying and responding against target one traffic, thereby enhancing all cyber security lines of defense in healthcare networks.

To handle the logs, Natural Language Processing (NLP) techniques with a Bidirectional Encoder Representations from Transformers (BERT) model [45] could be used to parse system logs generated by medical devices. BERT was then fine-tuned on a custom corpus of medical device logs, thus enabling it to extract the meaningful security events as well as properly distinguish potential threats. This method achieved an F1 score of 0.92, signaling a high degree of precision and recall in detecting security incidents. LSTM on network traffic coupled with BERT on log analysis resulted in a powerful machine-learning and natural-language processing data ingestion framework that was ideal for real-time threat detection and monitoring from multiple data sources.

3.6.2 Risk assessment with AI

A study developed a hybrid AI model to improve risk assessment accuracy and efficiency. It used a Random Forest classifier for initial risk categorization and a Gradient Boosting Machine (GBM) [46] for risk quantification. The Random Forest classifier was trained using historical security incident data and per-device attributes, classifying risks into pre-defined categories like data breaches and device malfunctions. The GBM model assessed risk levels based on factors like device criticality and potential patient safety impact. Combining these models improved accuracy by 23% compared to traditional manual methods.

3.6.3 Automated security control implementation

An AI-driven system was developed to implement security controls, utilizing reinforcement-learning and optimization algorithms to eliminate human intervention and mitigate

misconfigurations. The Deep Q-Network (DQN)-based reinforcement learning agent [47] optimized firewall rule configurations, reducing misconfigurations by 78%. A genetic algorithm (GA) [48] was used for scheduling security updates on hospital network devices. The GA reduced the median photovoltaic for critical vulnerabilities by 62%, reducing disturbances within medical center operations. The AI-driven optimization technology enabled the hospital to respond more effectively and timely to new threats.

3.6.4 Continuous monitoring with AI

A range of AI models were implemented to enable the continuous real-time monitoring of security incidents with anomalies and possible threats identified at every stage of the hospital network, from access to information systems. For point anomaly detection an Isolation Forest algorithm was used to flag anomalies in behavior of devices which could indicate a security incident. To traceback possible unknown attack paths or abnormal traffic, the method also combines a One-Class Support Vector Machine (SVM) [49] for network to capture the novelties in network behaviors at the same time. In addition, we also used a Variational Autoencoder (VAE) [50] for unsupervised anomaly detection on the system logs to detect any deviations from the normal log patterns without relying on predefined rules. In detecting security incidents, this ensemble achieved a 91% true positive rate with only a 3% false positive rate over the traditional rule–based monitoring systems. The AI-based automatic monitoring system analyzes the information it collects in real-time on a massive scale, to detect and respond quickly to security issues.

4 Cybersecurity certification scheme

The section presents another one of the key contributions of the paper related to the Cybersecurity Certification Scheme and its key features, describing how AI is leveraged, the type of AI models that could be used and their usage in each feature. Figure 3 shows the certification scheme for the RCA method.

Fig. 3 Cybersecurity certification scheme adapted on the AI-based RCA methodology

1. *Integration of AI-based security assessments* Incorporate AI algorithms and techniques into the certification process to enhance the efficiency and effectiveness of security assessments. This integration would enable a more thorough and automated evaluation of ICT products' cybersecurity. AI models are employed to enhance the efficiency and effectiveness of security assessments. Machine learning algorithms, anomaly detection models, and natural language processing (NLP) models are utilized for this purpose. AI algorithms analyze extensive datasets, including network logs, system behavior, and security events, enabling accurate identification of patterns and potential vulnerabilities. Anomaly detection models help detect abnormal activities, while NLP models extract relevant information from security policies and reports, streamlining the certification process and providing valuable insights for auditors and stakeholders by leveraging these AI models, healthcare organizations can conduct more comprehensive and automated evaluations of their ICT products' cybersecurity, ultimately leading to improved security and trustworthiness of medical devices and technology components.
2. *AI-driven risk analysis* Utilize AI technologies, such as machine learning and data analytics, to perform advanced risk analysis. AI algorithms can assess historical data, monitor emerging threats, and predict potential risks, allowing organizations to proactively address security vulnerabilities and prioritize risk treatment measures. Key AI models, such as machine learning algorithms and data analytics models, can be utilized in this feature. Leveraging these AI technologies enables organizations to perform advanced risk analysis by assessing historical data, monitoring emerging threats, and predicting potential risks. This proactive approach empowers healthcare organizations to address vulnerabilities effectively and prioritize risk treatment measures, enhancing the overall security posture of medical devices and ensuring safer and more reliable healthcare technology by utilizing machine learning and data analytics, the certification process gains valuable insights and data-driven decision-making, resulting in a more robust and resilient healthcare IT environment.
3. *Continuous AI-based monitoring* Implement AI-powered monitoring systems that continuously analyze security events and detect potential threats in real-time. AI algorithms can analyze network traffic, system logs, and

user behavior to identify abnormal activities or indicators of compromise. This enables organizations to respond promptly to security incidents and reduce the impact of potential breaches. Incorporate AI-powered monitoring systems that continuously analyze security events to promptly detect potential threats in real-time. AI algorithms analyze diverse data sources, including network traffic, system logs, and user behavior, to identify abnormal activities or indicators of compromise. This real-time threat detection empowers organizations to respond swiftly to security incidents, minimizing the impact of potential breaches. The automated monitoring ensures a proactive approach to cybersecurity, enhancing the overall resilience of healthcare IT systems and medical devices.

4. *AI-assisted compliance monitoring* Leverage AI-powered tools to monitor and ensure ongoing compliance with security standards and regulations. AI algorithms can assess adherence to security policies, detect policy violations, and recommend corrective actions. This helps maintain a continuous state of compliance and reduces the risk of security breaches. Harness the potential of AI-powered tools to ensure ongoing compliance with security standards and regulations. AI algorithms assess adherence to security policies, diligently detect policy violations, and recommend corrective actions by continuously monitoring and analyzing compliance, healthcare organizations can maintain a robust state of regulatory adherence and minimize the risk of security breaches. The incorporation of AI-driven compliance monitoring streamlines the certification process and supports healthcare providers in meeting industry-specific cybersecurity requirements.
5. *AI-enhanced security control implementation* Utilize AI-driven automation tools to streamline the implementation of security controls. AI can assist in automating the deployment and configuration of security solutions, ensuring consistent and effective implementation across ICT products. Utilize AI-driven automation tools to optimize the implementation of security controls across ICT products. AI can efficiently assist in automating the deployment and configuration of security solutions, ensuring consistent and effective implementation. This standardized approach to security control implementation enhances the overall security posture of medical devices and healthcare IT systems, mitigating potential vulnerabilities and strengthening protection against cyber threats by leveraging AI-driven automation, healthcare organizations can streamline security practices, ultimately fostering a safer and more reliable healthcare environment.
6. *Intelligent reporting and documentation* Integrate AI techniques to develop adaptive security controls capable of learning and adapting to evolving threats and changing environments. AI algorithms continuously analyze and assess the effectiveness of security controls, dynamically making adjustments and optimizations based on real-time data. This dynamic adaptation ensures that certified ICT products maintain a robust and up-to-date security posture, effectively countering emerging cyber threats. By employing AI-driven adaptive security controls, healthcare organizations can enhance the resilience of their medical devices, promoting a safer and more secure healthcare ecosystem.
7. *Adaptive security controls* Incorporate AI techniques to develop adaptive security controls that can learn and adapt to evolving threats and changing environments. AI algorithms can continuously analyze and assess the effectiveness of security controls, making adjustments and optimizations based on real-time data. This ensures that the certified ICT products maintain a robust and up-to-date security posture. Integrate AI techniques to develop adaptive security controls capable of learning and adapting to evolving threats and changing environments. AI algorithms continuously analyze and assess the effectiveness of security controls, dynamically making adjustments and optimizations based on real-time data. This dynamic adaptation ensures that certified ICT products maintain a robust and up-to-date security posture, effectively countering emerging cyber threatsy employing AI-driven adaptive security controls, healthcare organizations can enhance the resilience of their medical devices, promoting a safer and more secure healthcare ecosystem.
8. *Collaboration with European cybersecurity certification group (ECCG)* Establish a systematic cooperation framework with the European Cybersecurity Certification Group (ECCG) to create guidance documents supporting the certification scheme. This collaborative approach ensures that the scheme aligns with industry best practices and benefits from the expertise and insights of cybersecurity professionals. By working closely with ECCG, the certification process can incorporate the latest cybersecurity knowledge and recommendations, improving its relevance and effectiveness in addressing healthcare-specific cybersecurity challenges. The partnership with ECCG fosters a robust and trustworthy certification framework for medical devices and technology in the healthcare domain.

4.1 Cybersecurity certification scheme for medical devices

This section provides an overview of the certification scheme for the medical devices by following a number of steps based

Fig. 4 Cybersecurity certification scheme for medical devices

on the certification process. As presented in Fig. 4, it triggers from scope definition to understand the possible areas and out of scope context for an audit, followed by the remaining steps of audit.

1. *Scope definition* Define the scope of the certification scheme for medical devices, specifying the types of devices, software, and components that fall under its purview. This may include implantable devices, monitoring systems, diagnostic equipment, and software applications used in healthcare settings and identifies possible out of scope areas for the certification. AI technologies, such as natural language processing (NLP) and data analytics, enable the comprehensive analysis and categorization of various medical devices, software applications, and components that fall within the scheme's purview. By efficiently processing vast amounts of information from diverse sources, including regulatory guidelines and device specifications, AI-driven data analysis ensures a holistic approach to cybersecurity certification. This innovation facilitates a thorough evaluation of the interdependencies between different medical devices and software components, allowing for a tailored and effective certification scheme that addresses the unique risks and challenges prevalent in the healthcare domain. The AI-powered scope definition guarantees the security and reliability of certified medical devices and their associated software, instilling confidence among stakeholders and enhancing overall healthcare cybersecurity.
2. *Compliance requirements* The focus is on establishing comprehensive and tailored cybersecurity requirements specifically designed for medical devices. AI models, such as machine learning algorithms and data analytics, play a pivotal role in this process. These AI technologies are utilized to analyze vast amounts of data from various sources, including historical security incidents, device behavior, and regulatory guidelines. By leveraging AI-driven data analysis, the cybersecurity requirements are meticulously crafted to address the unique challenges and risks associated with medical devices, with a strong emphasis on ensuring patient safety, safeguarding data privacy, and maintaining compliance with relevant industry standards like the IEC 62443 series and FDA guidelines. The integration of AI-powered insights ensures that the cybersecurity requirements are adaptive and continually updated to stay abreast of emerging threats, ultimately fostering a resilient and secure environment for medical devices and the healthcare ecosystem as a whole.
3. *Risk assessment and management* Cutting-edge AI-driven risk assessment techniques are employed to conduct a comprehensive evaluation of potential threats and vulnerabilities in medical devices. Utilizing sophisticated AI algorithms, historical data is analyzed to gain insights into past security incidents and trends. Moreover, the AI models continuously monitor emerging cybersecurity risks and utilize predictive capabilities to anticipate potential attack vectors. This dynamic approach enables the early identification of potential risks specific to each device, leading to the development of tailored risk treatment measures. By leveraging the power of AI-driven risk assessment, healthcare organizations can proactively safeguard medical devices, mitigate potential threats, and enhance the overall security posture of their healthcare IT environment.
4. *Security control implementation* Advanced AI-driven automation tools are integrated to streamline the implementation of robust security controls. These AI tools play a pivotal role in automating the configuration of essential security features, encryption mechanisms, access controls, and secure software development practices across a wide range of medical devices. Leveraging AI algorithms, the implementation process becomes not only efficient but also consistently effective, ensuring that each device adheres to the highest security standards. By utilizing AI-driven automation, healthcare organizations can expedite the deployment of security controls, reducing potential human errors and ensuring a uniform and robust security posture for all certified medical devices. The seamless integration of AI in this process enhances the overall cybersecurity resilience of medical devices, ultimately contributing to a safer and more secure healthcare ecosystem.
5. *Continuous monitoring and threat detection* Cutting-edge AI-powered monitoring systems are implemented to conduct continuous analysis of security

events, enabling real-time threat detection. By utilizing advanced AI algorithms, these monitoring systems meticulously scrutinize network traffic, system logs, and user behavior to identify anomalies and indicators of compromise swiftly. The real-time detection of potential security incidents empowers healthcare organizations to respond promptly, minimizing the impact of any potential breaches. The integration of AI-driven monitoring ensures a proactive approach to cybersecurity, enhancing the overall resilience of medical devices and healthcare IT systems, and fostering a safer and more reliable healthcare environment for patients and healthcare professionals alike.

6. *Vulnerability management* Comprehensive processes are established to identify and effectively manage vulnerabilities in medical devices. To achieve this, collaboration with device manufacturers, software vendors, and security researchers is essential to promptly address any identified vulnerabilities. AI technologies play a crucial role in this context, aiding in the identification of vulnerabilities through advanced analysis of device behavior, code review, and historical security data. Moreover, AI-driven automation facilitates efficient patch management processes, ensuring timely updates and fixes to address vulnerabilities. By leveraging AI models, healthcare organizations can proactively secure medical devices, reducing the potential for exploitation and enhancing the overall cybersecurity resilience of the healthcare ecosystem.The certification scheme for medical devices includes a vulnerability management process supported by mature AI-driven tools and integration with existing vulnerability databases. The system uses static and dynamic analysis techniques to provide a comprehensive picture of the security state of Medical Device Software and Firmware. It analyzes firmware using tools for detecting vulnerabilities in embedded systems of medical devices. The system is fed from various vulnerability databases, including the National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE) effort, and MDVIP, Medical Device Vulnerability Intelligence Framework, FDA cybersecurity alerts for medical device-specific vulnerabilities, CISA's Industrial Control Systems advisories for critical infrastructure concerns, and manufacturer security bulletins for device-specific updates and patches. This multi-source approach ensures thorough coverage of potential vulnerabilities and enables healthcare organizations to maintain an up-to-date understanding of their risk landscape. The integration of these authoritative sources allows for timely identification and assessment of vulnerabilities that could impact medical devices and healthcare operations.AI-based natural language processing (NLP) algorithms will constantly track and process updates from these databases to detect new vulnerabilities for immediate response against emerging threats. The certification also includes a mature risk-based scoring and prioritization system that prioritizes vulnerabilities based on potential patient safety or data-security impacts. The automated patch management system handles the remediation process, identifying, testing feasibility, and deploying patches for known vulnerabilities. The system provides real-time status of patch effectiveness and device performance, ensuring proper drug delivery without putting the safety or functionality of a therapy at risk.
7. *Secure software development lifecycle* Secure software development practices are seamlessly integrated to ensure robust cybersecurity measures. This encompasses incorporating stringent security requirements and testing procedures throughout the entire software development lifecycle. Code reviews and implementation of secure coding practices are emphasized to minimize potential vulnerabilities. AI technologies play a pivotal role in this process by assisting in automating security testing and code analysis. AI-driven testing frameworks can efficiently scan and analyze code, identifying potential vulnerabilities with remarkable precision and speed. By leveraging AI models, healthcare organizations can strengthen the security posture of medical device software, proactively addressing potential risks, and bolstering the overall resilience of the healthcare IT environment.
8. *Documentation and reporting* AI technologies are harnessed to produce comprehensive and standardized documentation crucial for the certification process. Advanced AI algorithms are employed to automatically extract relevant information from various stages of the certification, encompassing risk assessments, security controls, and vulnerability management. By leveraging AI-driven data extraction, the documentation process becomes efficient and accurate, simplifying the task for auditors and regulators. The use of AI models ensures that the certification documentation is thorough and consistent, providing valuable insights into the cybersecurity measures implemented and facilitating a smoother and more transparent certification process for all stakeholders involved in ensuring the security and integrity of medical devices.
9. *Collaboration with regulatory bodies* Close collaboration with regulatory bodies, such as the FDA, is established to harmonize the certification process with existing regulations and guidelines. AI models can be employed to facilitate this alignment by analyzing relevant regulatory documents and guidelines to identify

the specific requirements that need to be met during the certification process. By leveraging AI-driven analysis, healthcare organizations can ensure that their certification scheme adheres to all necessary regulatory standards, making the approval process for medical devices more seamless and efficient. This collaboration with regulatory bodies reinforces the credibility and trustworthiness of the certification, assuring stakeholders that the certified medical devices comply with all relevant industry regulations, ultimately contributing to a safer and more reliable healthcare ecosystem.

10. *Training and awareness* Comprehensive training programs and awareness campaigns are developed to educate all stakeholders involved in the medical device ecosystem. AI models can be utilized to analyze the cybersecurity landscape, identifying prevalent threats and vulnerabilities specific to medical devices. By leveraging AI-driven insights, these training programs are tailored to address the unique challenges and risks faced in the healthcare domain. The education efforts encompass device manufacturers, healthcare providers, and end-users, emphasizing the critical significance of cybersecurity in medical devices. The campaigns foster a culture of cybersecurity awareness and promote the adoption of best practices in device deployment and usage, empowering stakeholders to proactively safeguard medical devices and enhance the overall security posture of the healthcare IT environment. Our proposed framework will contribute to Training and Awareness by leveraging AI-driven insights to develop targeted training programs. These programs will educate all stakeholders, including device manufacturers, healthcare providers, and end-users, on the specific cybersecurity risks and challenges within the medical device ecosystem. The framework will analyze the latest threats and vulnerabilities, tailoring training to the needs of each group and fostering a proactive cybersecurity culture. This ensures that all participants are equipped with the knowledge to safeguard medical devices and enhance overall system security.

The innovation in the healthcare domain lies in tailoring the certification scheme to address the unique challenges and risks associated with medical devices. The integration of AI technologies enables more accurate risk assessment, continuous monitoring, vulnerability management, and the application of secure software development practices. This innovation promotes patient safety, data privacy, and regulatory compliance in the context of medical devices and contributes to improving cybersecurity within healthcare systems.

4.1.1 Regulatory framework and international cooperation

The European medical-device market will mandate the assent of any medical device that seeks to enter did reach the EU with the certification system since it is set to be deeply interwoven with The structure of The EU Medical Device Regulation [51] (MDR). This link ensures its economic conductibility and operation with extant regulatory frameworks. The certification process enables manufacturers to integrate cybersecurity right into their standard overall device certification workflow. The framework will provide a broad, but legally binding approach to medical device cybersecurity that must be met before putting them on the market. In addition, when the certification program is expanded globally, the European Union will endeavor to conclude International Mutual Recognition Agreements with key regulatory partners including FDA and Health Canada. The pacts will also facilitate mutual recognition of certification processes, thus streamlining the alignment of cybersecurity standards among major markets, ameliorating the issue of non-EU suppliers and facilitating market access for manufacturers working in multiple geographical regions. Besides that, to ensure an effective border control, a cooperation with customs authorities will be established to prevent non-compliant devices from reaching the market of the EU.

4.1.2 Technical implementation

Technologically, the certification will leverage state-of-the-art technology for making compliance and security verification process easier. The creation of a compliance checking system driven by AI, using machine learning algorithms trained on datasets containing compliant or non-compliant devices. This technology will make it possible to automatically test how well the scheme complies with cybersecurity requirements, and in case of non-compliance, we can quickly identify potential shortcomings without having to conduct lengthy control checks manually. This is really what most people are referring to when they say a blockchain-based supply chain will be put in place. Work in this space will enable an end-to-end transparent life cycle of a medical device from raw materials all the way to consumption. The system will verify that components are legitimate and have not been tampered with between the point of manufacture and distribution. This way, the chances of tampered and counterfeited devices making their way into the market will be avoided. For suppliers outside the EU, remote audits will be allowed. This would allow appropriate auditors to conduct thorough and safe appraisements, without the need for any physical visit. Envisioned as a new market service for customers looking to accelerate migration of therapeutics development plans, the system combines encrypted video streaming infrastructure with Internet of Things sensors and AI analysis tools,

allowing audit administration services to follow stringent observation protocols necessary in these rapidly evolving times. So, even an online audit can perform inspection similar to onsite review. These are technical implementations that improve the efficiency as well as scalability of the certification scheme to make sure medical devices around the globe will have a secure and transparent regulatory environment.

4.2 Implementation details of the certification scheme

4.2.1 Scope, definition and compliance requirements

The implementation of the certification scheme begins with a clear definition of scope, where all medical devices are profiled using a custom taxonomy system that aligns to NIST Cybersecurity Framework [52]. This ensures that devices are systematically classified by their use and the risks they represent to the healthcare environment. A more powerful a Natural Language Processing (NLP) algorithm is used to analyze all the detailed specifications in order to make this process even easier. By automating the classification of certification scheme products, in this example devices within scope, using a natural language processing (NLP) model, it is possible to eliminate manual workload and as such ensure classification accuracy.

4.2.2 Risk assessment, security control implementation and continuous monitoring

The certification scheme comes with a Bayesian network model for risk assessment and management [53]. This model is applied to assess the probability of occurrence and impact encoding security threats considering interdependences among system constituents. Quantifying risk levels is done through Monte Carlo Simulations, which lets us take a probabilistic view on how to address risks and what mitigation strategies we should prioritize. The integration of Structural Threat Information eXpression) (STIX) threat intelligence feeds in the risk assessment workflow ensures that the process is dynamic and able to adapt to any changes in threat landscapes, hence always showcasing an 'at-the-moment' picture of possible vulnerabilities. To implement security controls, the Preconfigured Security Control Templates library could be leveraged on the NIST SP 800–53 Controls. These templates help to decouple the essential security requirements from specific medical device platforms. Automation and validation of these security controls was implemented by way of an automated configuration management tool into the service. This is to ensure that controls are uniformly implemented and also operational on every single device, thereby minimizing the risk of configuration drift or even human error. In addition, the certification scheme supports continuous monitoring and threat detection by way of deploying a Security Information and Event Management (SIEM) system that collects security events from medical devices.

4.2.3 Vulnerability management, secure deployment and documentation

In order to keep vulnerability management up-to-date, the certification scheme interacts with a variety of vulnerability databases like National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE), enabling a personalised list of vulnerabilities regarding medical devices. This provides a constantly updated perspective of risk. In addition to this, an automated vulnerability scanning tool was stablished with a firmware and software combability for medical devises. Scans are used to rapidly identify any known vulnerabilities that could be exploited by an attacker, so you can patch those quickly. As for secure software development, the certification scheme could consist of running SAST tools in the pipeline. This leads to the timely discovery and remediation of code-level vulnerabilities, therefore decreasing the likelihood that security weaknesses are built into medical devices. Secure code review process is a combination between automated tools and manual expert reviews, trying to inspect the code as much as possible for risks. Further, compliance results are reported in more than one format (e.g., pdf, xml) by a custom reporting engine to facilitate broad exposure to the data/information being generated. To ensure that these reports are not tampered with and provide non-repudiation over the certification lifecycle and blockchain-based system is employed.

4.2.4 Collaboration, regulatory engagement and training

Working with regulators is an important part of the certification programme. Trusted Automated Exchange of Indicator Information protocol could be used by the scheme to enable secure and efficient data sharing, enabling certification results to be shared with regulatory authorities. A version control system to record and manage regulatory changes could be leveraged, meaning: the certification scheme will always keep pace with new standards. The certification body or the manufacturers are automatically migrated to the new requirements ensuring both entities are compliant with the updated standard. And finally, to achieve strong deployment of best practices for cybersecurity in the healthcare field, an e-learning center could be used and an established training module focused on medical device cybersecurity. This includes training in different parts related to the certification, such as risk management, regulatory compliance and security control implementation.

5 An agile and extended information security management system (ISMS)

An agile and extended ISMS is proposed for the systematic approach to managing cybersecurity risks, generating protection profiles, auditing controls, and handling security incidents in connected medical devices.

The ISMS consists of several features: Risk Forecasting and Identification, which involves continuous monitoring of the cybersecurity landscape, gathering threat intelligence, and identifying potential risks; Risk Analysis and Estimation focuses on conducting detailed risk assessments, analyzing the impact and likelihood of identified risks, and estimating their potential consequences; Risk Mitigation encompasses the development and implementation of security controls and measures to mitigate the identified risks; and lastly, Protection Profile Generation involves creating comprehensive protection profiles that outline the necessary security requirements, countermeasures, and assurance measures specifically tailored for connected medical devices.

Two key responsible entities in this architecture are the Manufacturers and Auditors. Manufacturers of connected medical devices have specific responsibilities within the system. They are responsible for conducting risk forecasting, risk analysis, risk mitigation, and generating protection profiles. The manufacturers implement security controls, adhere to recognized standards, and establish incident management processes to ensure the security of their devices. On the other hand, Auditors play a crucial role in assessing the effectiveness of the implemented controls. They conduct audits to evaluate compliance with protection profiles, security standards, and regulatory requirements, providing assurance and oversight to ensure proper security practices are in place.

There are important connections and collaborations between Manufacturers and Auditors throughout the process. Manufacturers and Auditors work closely together, with Manufacturers providing insights into device architecture, risk assessment findings, and mitigation strategies. Auditors review and assess the effectiveness of the implemented controls, ensuring alignment with protection profiles and security standards. The outputs of Risk Analysis and Estimation influence the development of protection profiles, as Manufacturers consider the identified risks and their potential impact when creating these profiles. Additionally, Audit Effectiveness findings provide valuable feedback to Manufacturers for continuous improvement of their security controls, risk management practices, and compliance with protection profiles.

Integration of Incident Management processes is another vital aspect of the architecture. Manufacturers establish incident response plans, procedures, and mechanisms to detect, respond to, and recover from security incidents. Incident management is an integral part of the overall system, ensuring that security incidents are promptly addressed. Auditors may review the effectiveness of these incident management processes during audits, verifying their alignment with best practices and regulatory requirements. By incorporating incident management, the architecture aims to enhance the overall security posture and resilience of connected medical devices, minimizing the impact of security incidents and ensuring swift response and recovery.

5.1 Generic ISMS high-level architecture

A detailed description of each component in the proposed ISMS high-level architecture that integrates the principles of the certification scheme and incorporates AI capabilities is presented below. Figure 5 shows the high-level architecture through three distinct layers of abstraction including application services and components, core systems and apps for the overall ISMS implementation.

Application services & components layer:

1. *Cyber-environment management* This component is responsible for managing the inventory of assets, their interrelations, and interdependencies within the ISMS. It includes intelligent activities for vendor and auditor management, such as tracking vendor security practices and managing auditor engagements.
2. *Code auditing* This component inspects the medical code used in the ISMS for defects, violations, and vulnerabilities. It implements static application security testing (SAST) techniques and scans the code against known security concerns to identify potential weaknesses and security flaws.
3. *Vulnerability management* The vulnerability management component conducts regular vulnerability assessments and analyses to identify and mitigate risks associated with connected medical devices and their components. It scans for known vulnerabilities and assesses their potential impact, enabling proactive risk mitigation measures.
4. *Threat intelligence* This component collects and analyzes threat information from various sources to identify and classify relevant threats to the ISMS. It utilizes machine learning (ML) and deep learning techniques to detect and predict emerging threats, enhancing the system's ability to respond effectively to evolving cybersecurity risks.
5. *Risk & conformity assessment* This component implements a cybersecurity risk management strategy and model within the ISMS. It manages cybersecurity risks through activities such as risk identification, assessment, response planning, and monitoring. By incorporating the principles of the cybersecurity certification scheme, it ensures conformity with relevant security standards and regulatory requirements.

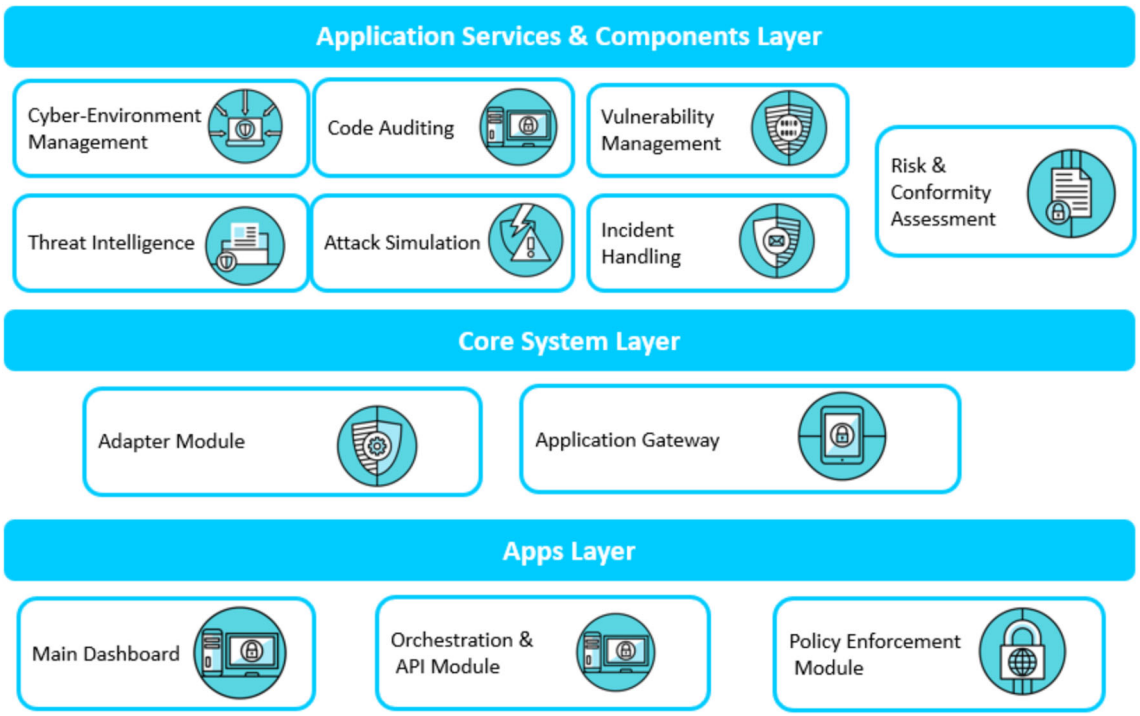

Fig. 5 ISMS high-level architecture

6. *Incident handling* The incident handling component facilitates the identification, analysis, response, prevention, and detection of security incidents and threats within the ISMS. It collects event data for security information and event management, enabling timely incident response and mitigating potential damage.
7. *Attack simulation* This component enables the design, execution, and analysis of risk and attack simulation experiments within the ISMS. It uses information derived from the Threat Intelligence component to calculate cascading effects and attack paths, providing valuable insights into the system's vulnerabilities and areas for improvement.

Core system layer:

1. *Adapter module* The adapter module allows for loose coupling between the core platform and integrated systems within the ISMS. It handles integration configuration in a central repository, facilitating seamless communication and interoperability between different components and external systems.
2. *Application gateway* Acting as a proxy, the application gateway manages communication between the external architecture layers and the core system services of the ISMS. It ensures secure and efficient data transmission between clients and the core system, enabling the smooth operation of the ISMS.

Apps layer:

1. *Main dashboard* This component provides distinct experiences for different user types accessing the ISMS. Implemented as a Single Page Application (SPA), it enhances performance and user experience by providing a responsive and intuitive interface for monitoring and managing cybersecurity activities within the ISMS.
2. *Orchestration & API module* The orchestration and API module enables seamless communication and integration between the internal components and various ISMS applications. It exposes services' APIs for integration purposes, allowing the exchange of data and functionality between different parts of the ISMS ecosystem.
3. *Policy enforcement module* The policy enforcement module administers, specifies, interprets, and enforces policies based on predefined rules, terms, and conditions. It ensures compliance with security policies and regulations within the ISMS, providing granular control over access privileges and enforcing security best practices.

5.2 ISMS adapted for medical devices

The proposed ISMS high-level architecture adapted for medical devices:

Application services & components layer:

1. *Medical device inventory management* Formulate an inventory of medical devices and their components,

including protocols, technologies, systems, processes, functions, and applications. This component should capture detailed information about each device, such as device type, firmware version, manufacturer details, and connectivity features.

2. *Medical device interrelation and interdependency management* Analyze the interconnection and interdependence at the component and device level. This includes understanding how various components of medical devices are interconnected and how medical devices are connected within the healthcare infrastructure. This information helps in mapping the overall infrastructure and identifying potential security risks.
3. *Vendor and auditors management* Implement intelligent activities for managing vendors, manufacturers, integrators, and auditors involved in the lifecycle of medical devices. This component should provide functionalities for registering vendors and auditors, maintaining a predefined list of trusted entities, and enabling the selection of appropriate vendors during the asset registration process.
4. *Code auditing for medical devices* Perform code audits of medical device software to identify defects, programming practice violations, and risky elements. This includes static application security testing (SAST) to identify potential vulnerabilities based on known security concerns. The code auditing component should also assess open-source libraries used in medical device software and evaluate their associated licenses and permissions.
5. *Vulnerability management for medical devices* Conduct vulnerability assessments for medical devices to proactively detect and analyze potential threats. This component should analyze information gathered from various sources, including automatic scanning tools, online repositories, and websites, to identify vulnerabilities in medical devices and associated components. It should generate detailed reports, assign vulnerability scores based on industry-standard metrics, and propagate the findings to the main dashboard.
6. *Threat intelligence for medical devices* Identify threats relevant to medical devices by collecting and analyzing threat information from online repositories and trusted sources. This component should leverage machine learning and deep learning techniques to classify and predict possible threats. It should integrate threat intelligence feeds specific to healthcare, using industry-standard formats such as Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII).
7. *Risk & conformity assessment for medical devices* Establish a comprehensive risk management strategy and model for medical devices. This component should implement the RCA methodology to systematically evaluate cybersecurity risks associated with medical devices. It should include activities for identifying, assessing, responding to, and monitoring risks. The RCA component should document all risk management activities specific to medical devices.
8. *Incident handling for medical devices* Enable incident identification, analysis, response, prevention, and detection of threats specific to medical devices. This component should collect and organize event data from medical devices, network infrastructure, and other relevant systems. It should serve as the interface between the healthcare infrastructure and the ISMS platform, combining security information and event management functions. Incident response procedures should be defined, including preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.
9. *Attack simulation for medical devices* Facilitate the design, execution, and analysis of risk and attack simulation experiments for medical devices. This component should incorporate simulation processes and algorithmic methods to assess attack paths and calculate the cascading effects of threats. It should provide visualizations of attack graphs, showing potential attack paths and affect assets. The attack simulation service should assist in formulating evidence-based mitigation plans.

Core system layer:

1. *Adapter module* Enable loose coupling between the core platform and integrated medical device systems. This module should allow for centralized integration configuration and reduce repetitive configuration efforts.
2. *Application gateway* Act as a proxy between the external architecture layers and the core system. It should manage communication between medical devices, clients, and core system services while ensuring secure and reliable data transmission.

Apps layer:

1. *Main dashboard for medical devices* Provide a comprehensive and intuitive user interface to manage and monitor medical devices' cybersecurity. This dashboard should display real-time information, visualizations, and alerts related to medical device inventory, vulnerabilities, threats, risks, incidents, and compliance status. It should enable authorized users to configure security policies, view reports, and perform necessary actions to ensure the security of medical devices.
2. *Orchestration & API module* Enable seamless communication between internal components and ISMS applications specific to medical devices. This module should

expose services' APIs for integration purposes and facilitate the orchestration of various functionalities within the ISMS platform.

3. *Policy enforcement module for medical devices* Administer, specify, interpret, and enforce policies based on rules, terms, and conditions specific to medical devices. This module should ensure that medical devices comply with the defined security policies and standards. It should integrate with the main dashboard to provide real-time policy violation alerts and facilitate remediation actions.

The proposed ISMS architecture incorporates a range of AI capabilities, offering significant improvements in the effectiveness and efficiency of the system as shown in Fig. 6 These AI integrations encompass various areas. Firstly, AI-based Security Assessments enable the ISMS to conduct more precise and efficient evaluations of ICT products and medical devices. By leveraging AI algorithms, the system can analyze extensive datasets to identify potential vulnerabilities and security weaknesses, allowing organizations to proactively address them. Secondly, through AI-driven Risk Analysis, the ISMS can utilize machine learning and data analytics to perform advanced risk analysis. This enables the system to analyze historical data, detect patterns, and identify potential risks associated with systems and devices, empowering organizations to better understand and manage cybersecurity risks. Thirdly, Continuous AI-based Monitoring implements AI-powered systems for real-time threat detection and incident response. By continuously monitoring network traffic, system logs, and user behavior, the ISMS can swiftly identify anomalies and potential security threats, enabling organizations to promptly detect and respond to incidents, thereby minimizing potential damage. Additionally, AI-assisted Compliance Monitoring utilizes AI tools to automate the monitoring of security standards and regulations. This automation streamlines compliance monitoring processes, allowing organizations to proactively identify any deviations from required security practices or regulatory requirements.

Moreover, AI-enhanced Security Control Implementation employs AI automation to streamline the implementation of security controls. AI algorithms can automate the configuration of security features, encryption mechanisms, access controls, and secure software development practices, ensuring consistent and effective implementation across diverse systems and devices. Furthermore, Intelligent Reporting and Documentation utilize AI technologies to generate intelligent reports and documentation for certification purposes. By automatically extracting relevant information from the ISMS, such as risk assessments, security controls, and compliance monitoring results, AI algorithms simplify the documentation process for auditors and regulators, reducing manual effort while enhancing accuracy. In addition, Adaptive Security Controls employ AI techniques to develop adaptive security controls capable of adjusting to evolving threats and changing environments. By continuously analyzing and learning from new threat intelligence, the ISMS can dynamically adapt security measures and effectively respond to emerging risks. Finally, Collaboration with Certification Authorities is crucial for aligning the ISMS architecture with industry best practices and certification requirements. By cooperating with certification authorities, organizations can ensure their ISMS meets the necessary standards and regulations, facilitating the certification process and demonstrating a strong commitment to cybersecurity.

5.3 Incident handling in the ISMS

The Incident Handling component of the ISMS plays a crucial role in identifying, analyzing, responding to, and mitigating security incidents related to medical devices and healthcare systems. This subsection details the advanced capabilities and processes implemented within this component.

5.3.1 Automated triage and incident classification

The Incident Handler component automatically identifies and classifies security incidents through AI-guided algorithms. *Key aspects include*:

Machine learning models: Activate learnings analyze medical device logs, network traffic and SIEM systems to identify incidents and combine real-time event correlation. Pattern recognition in these models is used to help predict relationships within the data, making it easier and faster for security teams to identify threats. Real-time detection helps in identifying threats quickly from many vectors, which ultimately refers to a more secured healthcare systems.

Risk scoring engine: An AI-based engine that evaluates incoming incidents against a set of patient safety, data confidentiality and system integrity criteria. The system combines rule-based logic with machine learning, trained on the historic incident data to decide how severe each threat is. Through knowledge of the severity level, the system guarantees prompt responses to critical incidents, and appropriate management of manageable events.

Automated incident categorization: Natural language processing (NLP) algorithms categorize incidents, for example, by malware, unauthorized access or data breaches. The incident management process is subsequently sped up due to this categorization automation, which allows responses that are more precise and efficient based on the type of threat.

Dynamic Prioritization: The severity of incidents is constantly adapted according to real-time threat conditions. The

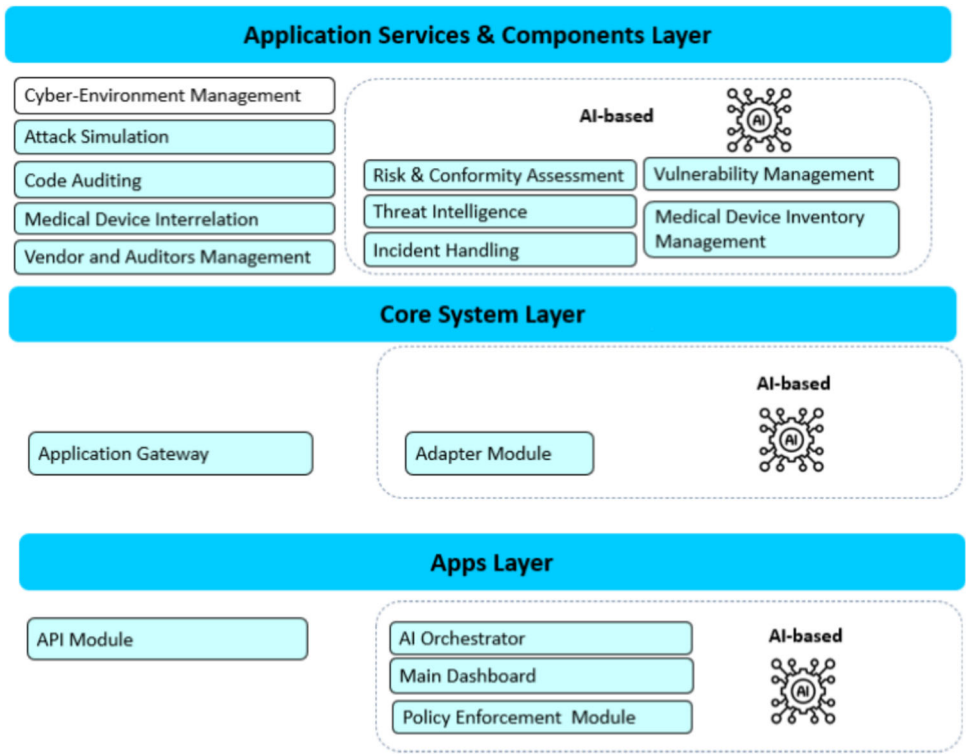

Fig. 6 ISMS for medical devices

adaptive algorithms consider the context, overall security maturity of the organization and historical incident patterns to make sure that most important threats are respond immediately. This dynamic risk prioritization allows for the most at-risk devices to have resources allocated toward protecting them reducing the threat against those devices as much as possible.

5.3.2 Intelligent response workflows

Intelligent Response Workflows with AI for Decision-Making and Automation incident management process streamline:

Automated playbook selection: Select dynamic playbooks based on incident type and severity. These are predefined actions and are specific to the specific incident types. From the perspective of an incident, AI models evaluate real-time incidents allowing to launch a very fast pre-selection thus making sure, that this is the most effective reaction.

Adaptation of workflow based on feedback: Machine learning algorithms analyze feedback for real time effectiveness of response actions. If an action is less effective, or if the incident changes over time, the system learns and updates in order to improve how response happens. The ongoing adaption assures that it is owner of incidents that spin or flutter during resolution.

Automated containment actions—For certain incident types, the system has the ability to autonomously take containment actions (such as isolation of an affected devices or blocking of malicious IPs). It performs these actions via integrations with network management tools and access control systems, which minimizes the impact on other network operations.

Support for AI-assisted decision making: AI models provide recommended actions to the incident responders utilizing historical data and threat intelligence. These recommendations are targeted to the context of the event, so that responders can choose what is likely to be most appropriate. This lowers the cognitive burden on human operators and allows for faster remediation.

5.3.3 Collaboration and information sharing

Secure collaboration is the key, where Information sharing can mitigate the incident faster.

Dedicated secure collaboration platform: With a self-created platform, response teams can interact with and share information securely. MFA and RBAC use control which incident data janitorial staff touch. Secure access to the platform ensured that all sensitive details were transmitted correctly without leaking any key information during the response.

Automated stakeholder notification: System defines a list of stakeholders whose details vary on the type and severity of incident. All of the involved parties are alerted, through email, SMS or push notifications. This solution enforces that decisions are made quickly and the proper resources get allocated to them.

Connection with external threat intelligence platforms: The connection of ISMS to external intelligence platforms helps in incorporating the new updated data related to threats. The integration gives access to the newest vulnerabilities, indicators of compromise, and mitigation strategies making their threat intelligence more rich.

Secure information sharing with regulatory bodies: Regulatory compliance is ensured by allowing organizations to share information with regulatory bodies (e.g. the FDA or ENISA) securely. As part of this, we follow all necessary rules around secure transfer of sensitive incident data (as the tool that collects the information) to help you remain compliant with whatever specific reporting requirements you have within your organization in a way that does not open up additional security risks.

5.3.4 Continuous improvement through lessons learned

Incident Management process also has a Feedback loop to improve continually:

Automatic incident analysis: Machine learning algorithms analyze the timeline, actions taken and their outcome in order to self-learn. Looking into these factors, the system pinpoints any inefficiency or bottlenecks so that an organization can better its response strategies. Since each iteration takes less than a few hours and minimal manpower, the live environment experiences faster response times during an incident and resolves more effectively in future events.

Knowledge base generation: This is performed with assistance of an AI-Powered knowledge base, which extracts insights from the post-incident analysis. This knowledge base serves as a central repository of lessons learned, helps incident responders and operators to access information using data driven insights within our system to make the system more resilient overall.

Forecast modelling for incidence prevention—The predictive models use past data and present states to pinpoint potential risks before they escalate to an incidence. The system flags these situations as well, so that companies are able to put in place security controls in anticipation of a future event.

Automated playbook optimization: Machine learning analyzes response playbooks based on incident outcomes and updates them. This keeps response strategies well orientated with the changing threat environment, which in turn serves to create a proactive defence mechanism.

Simulation-based training: Training for response teams using incident simulations generated by AI from historical incidents. It helps the team in understanding what to do if they face such a scenario in real life, which eventually increases preparedness and decreases response time for any incident.

5.4 Interrelation of RCA framework, certification scheme and ISMS

5.4.1 RCA framework as the foundation

At the heart of this integrated ecosystem is the Risk and Conformity Assessment (RCA) Framework, which serves as a key mechanism for identifying, assessing and controlling the risks associated with cybersecurity in healthcare systems and medical devices. It applies different AI-based methods to detect threats, evaluate possible attack targets and develop adequate countermeasures adapted to the specific security tag of medical devices & healthcare IT systems. The RCA Framework records risk-related data continuously and processes these to provide concrete Risk profiles and mitigation plan. These simulations are the basis of both the Cybersecurity Certification Scheme and the Information Security Management System (ISMS). All other procedures are drawn from a set of robust, well documented risk assessments. It is the combination of both that form the backbone of maintaining security in Healthcare environments and you have importance either to utilize RCA Framework.

5.4.2 Certification scheme as the validation mechanism

The Cybersecurity Certification Scheme is the validation process that ensures compliance to high-level security standards for medical devices before they go live in healthcare. This framework makes use of the RCA Framework outputs making the risks discovered, vulnerabilities identified and mitigation strategies as translated to specific certification criteria. The fact that medical devices must pass this certification process is how hospitals maintain the security standards to keep these devices secure for real-world use within a healthcare environment. AI technologies are central to the automation of this certification i.e. it is used for auto compliance checking which ensures that devices comply with established security benchmarks. This way, the certification scheme not only validates how a device stands in its security posture but changes dynamically with growing threats by leveraging learnings from RCA Framework to evolve the certification requirements.

5.4.3 ISMS as the operational framework

The ISMS serves as the operational framework that implements and manages the processes defined by the RCA

Framework and enforces the standards set by the Certification Scheme. It provides the necessary tools, workflows, and infrastructure to operationalize risk management and certification processes in real-world healthcare settings.

5.4.4 Data flow and integration

An integrated ecosystem is only as efficient as the degree to which data seamlessly passes from the RCA Framework to Certification Scheme, and ISMS—automation plays a key role in enforcing that seamlessness. The RCA Framework is built on cutting-edge machine learning techniques for the real-time generation of full risk profile and mitigation strategy sets for healthcare systems and medical devices. The Certification Scheme uses these outputs to set parameters around what a certification should look like by referencing known threat models and utilizing compliance checking AI systems. Once certified the ISMS as operationally takes your security controls live and it acts upon those to identify, validate their health (including effectiveness of controls) all done via real-time analytics on systems with AI-powered automation tools. Relying on a closed-loop architecture, the ISMS is complemented by continuous feedback mechanisms where near real-time IoT telemetry data from performance of devices and security incidents detection to changes in environmental dynamics are captured. This data is then fed back into the RCA Framework AI models for continued risk reassessment using strategies such as anomaly detection algorithms and predictive analytics. This AI-powered ecosystem automatically adapts and reacts to threats, proactively better-protecting healthcare systems against the range of incoming cyber challenges.

5.4.5 AI-driven synergy

AI technologies play a critical role in enhancing the synergy between the RCA Framework, Certification Scheme, and ISMS. In the RCA Framework, AI models provide advanced capabilities for risk prediction and threat analysis, enabling the framework to identify and assess risks with high accuracy. In the Certification Scheme, AI supports automated compliance checking and adaptive certification processes, enabling a dynamic and efficient validation of medical device security. Meanwhile, in the ISMS, AI is employed for real-time threat detection, automated incident response, and continuous monitoring of security controls. This AI-driven synergy ensures that the integrated ecosystem is capable of identifying, assessing, and mitigating threats in real-time, resulting in a highly adaptive cybersecurity framework that can proactively respond to the evolving threat landscape in healthcare environments.

5.4.6 Regulatory compliance and holistic security

Together, the RCA Framework, Certification Scheme and ISMS form an integrated ecosystem aimed at facilitating adherence to extensive regulations throughout all facets of the medical device lifecycle. The RCA framework ensures that the identification of risks and their mitigation strategies meets standard in the industry, harmonizing risk management processes with regulatory requirements. Through use of the Certification Scheme, risk assessments are translated into specific criteria that all IoT devices must demonstrate in order to show compliance before going live. Finally, the ISMS enable perpetual compliance performance in constantly monitoring and reporting any variances in regulatory standards. This holistic strategy results in a resilient, agile, and compliant cybersecurity infrastructure which allows healthcare providers to combat the multifaceted issues involved with medical device security – spanning from device manufacturing through to clinical deployment and ongoing maintenance.

6 Conclusion and future work

The work discusses the emergence of connected medical devices and the IoMT, highlighting the challenges associated with tacking the security threats and risks. The main contribution of this work is the development of a novel RCA Framework for manufacturers and healthcare organizations, along with a certification scheme and an agile ISMS to address cybersecurity risks in the medical devices and ensure the resilience of the healthcare service delivery. The proposed framework integrates AI to enhance the security assessment process, risk prediction, security control implementation, continuous monitoring, security evaluation, and reporting/documentation. The proposed RCA Framework incorporates AI algorithms to collect and analyze relevant data from various sources, such as system logs, network traffic, and security incident reports. This allows for efficient processing of large volumes of data, enabling the identification of patterns, anomalies, and potential security risks that might be missed through manual analysis methods, and advanced risk assessments, improving the accuracy of risk predictions and enabling proactive security measures. The framework also emphasizes the automated implementation of security controls using AI-driven automation tools, ensuring consistent deployment and configuration across the organization's IT infrastructure. Continuous monitoring powered by AI systems is a key component of the framework, allowing for real-time analysis of network traffic, system logs, and user behavior to swiftly detect abnormal activities or signs of compromise. While this work presents a conceptual framework, it acknowledges that implementation and potential modifications of the framework remain areas for

future research. Further studies will be needed to validate its effectiveness, refine its components, and explore its practical application in real-world healthcare environments.

This work contributes novel advancements by integrating AI into the RCA framework, distinguishing it from existing approaches through its automated, AI-driven processes for risk assessment, control implementation, and continuous monitoring. Unlike traditional manual methods, the proposed framework's AI component enhances scalability, efficiency, and real-time analysis, providing deeper insights into emerging risks and improving the accuracy of predictions. The introduction of an AI-powered certification scheme also sets a new precedent by streamlining compliance efforts, making it a pioneering solution in medical device cybersecurity. The proposal for a Cybersecurity Certification Scheme for medical devices suggests integrating AI-based security assessments into the certification process. This would optimize efficiency and effectiveness by leveraging AI algorithms to analyze large amounts of data, identify patterns, and detect vulnerabilities or risks. The proposed certification scheme for medical devices aims to enhance patient safety, regulatory compliance, and the overall security posture of medical devices. It suggests defining the scope of the scheme, establishing comprehensive cybersecurity requirements tailored to medical devices, employing AI-driven risk assessment techniques, streamlining security control implementation, implementing AI-powered monitoring systems, establishing vulnerability management processes, integrating secure software development practices, and simplifying documentation through AI-generated reports. Collaboration with regulatory bodies, such as the European Cybersecurity Certification Group (ECCG) and the FDA, is recommended to ensure alignment with existing regulations and standards. The proposed framework, certification scheme, and ISMS aim to promote regulatory compliance, improve security practices, and establish trust and confidence in the healthcare ecosystem, contributing to a competitive and trustworthy Digital Single Market (DSM).

While the proposed framework enhances cybersecurity through AI integration, it also presents some notable limitations. One significant concern is the dependence on large datasets, which may raise privacy and data protection issues, particularly in the healthcare sector where sensitive patient information is involved. Additionally, the effectiveness of AI models relies on continuous learning and updating to remain resilient against evolving cyber threats, which can be computationally expensive and resource-intensive. Future work could focus on adopting privacy-preserving technologies, such as homomorphic encryption and differential privacy, to ensure data anonymity while maintaining robust security. Furthermore, the integration of federated learning can reduce the need for centralized data storage, mitigating privacy risks. Establishing industry-wide standards for secure AI deployment in healthcare is also essential for enhancing trust, ensuring regulatory compliance, and fostering collaboration across stakeholders. As next step of the proposed RCA framework, it is crucial to extend the framework's scope to encompass emerging technologies like edge computing, 5G networks, and the IoT, ensuring comprehensive security coverage in the ever-evolving healthcare landscape. In addition, collaborative efforts must be made to establish industry standards and best practices specifically tailored to medical device cybersecurity, fostering information sharing and cultivating a cooperative culture among manufacturers, healthcare organizations, and regulatory bodies. Lastly, continuous monitoring and assessment of the evolving threat landscape are imperative for adapting and updating the framework and certification scheme, accordingly, addressing new and sophisticated attack vectors that may emerge. By prioritizing these areas for future work, stakeholders can collectively strive towards a resilient and trustworthy healthcare ecosystem that places utmost importance on patient safety and data protection.

Acknowledgements The authors would like to acknowledge the financial support provided for the following projects: The 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; The 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; The 'A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processes' (CUSTODES) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; The 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CYberSynchrony) project, which has received funding from the European Union's Digital Europe Programme under grant agreement No. 101158555, supported by the European Cybersecurity Competence Centre (ECCC); The 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932. The views expressed in this paper represent only those of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

Author contributions KK and EG have made significant contributions throughout the research process, encompassing the conception, design, acquisition, and meticulous analysis of the study. Their involvement extended to not only the initial drafting but also the critical and insightful revisions of the primary manuscript, enriching it with essential intellectual content. AY and LC played integral roles in the preparation of Figs. 1–6, which visually communicate key findings and enhance the comprehensibility of the research. The collaborative nature of this endeavor is underscored by the invaluable contributions of SI, AY, LC, and HM, who collectively provided constructive feedback and diligently corrected various aspects of the paper. All authors have consistently demonstrated their unwavering dedication to the study,

assuming responsibility for every facet of its execution. This commitment extends to the rigorous handling of concerns pertaining to the accuracy and integrity of the research. Any potential issues have been meticulously investigated and appropriately resolved, reflecting the authors' dedication to upholding the highest standards of scholarly rigor. As a testament to their collective effort, all authors have conscientiously reviewed and granted their approval for the final version of the manuscript, affirming its readiness for publication in its present form.

Data availability The Research Data Policy and Data Availability Statements are not applicable for this study.

Declarations

Conflict of interest The authors declare no competing interests.

Ethical approval This study constitutes a desk review, and as such, no ethical standards were applicable to its execution.

References

1. Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., Moussa, S.: Internet of medical things privacy and security: challenges, solutions, and future trends from a new perspective. Sustainability **15**(4), 3317 (2023). https://doi.org/10.3390/su15043317
2. Medical Device Network.: Medical device cybersecurity: assessing risks and mitigating threats, 2021. Retrieved from https://www.medicaldevice-network.com/comment/medical-device-cybersecurity/
3. Khaled, A.E.: Internet of medical things (IoMT): overview, taxonomies, and classifications. J. Comput. Commun. **10**(8), 64–89 (2022). https://doi.org/10.4236/jcc.2022.108006
4. Spieske, A., et al.: Improving resilience of the healthcare supply chain in a pandemic: evidence from Europe during the COVID-19 crisis. J. Purch. Supply Manag. **28**(5), 100748 (2022). https://doi.org/10.1016/j.pursup.2022.100748
5. Medical Futurist.: How to improve cybersecurity in healthcare? 7 steps to start, 2021. Retrieved from https://medicalfuturist.com/improve-cybersecurity-in-healthcare/
6. Torky, M., Hassanien, A.E.: COVID-19 contact tracing and detection based on blockchain technology and IoMT. Informatics **8**(4), 72 (2021). https://doi.org/10.3390/informatics8040072
7. National Institute of Standards and Technology (NIST).: Cybersecurity for the internet of things (IoT) and beyond, 2021. Retrieved from https://www.nist.gov/programs-projects/cybersecurity-internet-things-iot-and-beyond
8. The Journal of Medical Device Regulation.: Cybersecurity of medical devices: a regulatory perspective, 2019. Retrieved from https://www.emergobyul.com/resources/white-paper/cybersecurity-medical-devices-regulatory-perspective
9. US Food and Drug Administration (FDA).: Medical device cybersecurity, 2021. Retrieved from https://www.fda.gov/medical-devices/digital-health-center-excellence/medical-device-cybersecurity
10. Medical Devices Coordination Group. MDCG 2019-16 guidance on cybersecurity for medical devices. European Commission, 2019
11. European Union Agency for Cybersecurity. Cybersecurity of connected medical devices—addressing the regulatory challenges (No. EUCS-01/2019). EU Agency for Cybersecurity, 2019
12. The EU cybersecurity act. Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act#:~:text=The%20Cybersecurity%20Act%20strengthens%20the,framework%20for%20products%20and%20services. (Accessed: 12 Jun 2023)
13. Yaqoob, T., Abbas, H., Atiquzzaman, M.: Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. IEEE Commun. Surv. Tutor. **21**(4), 3723–3768 (2019). https://doi.org/10.1109/comst.2019.2914094
14. Pradhan, B., Bhattacharyya, S., Pal, K.: IOT-based applications in healthcare devices. J. Healthcare Eng. **2021**, 1–18 (2021). https://doi.org/10.1155/2021/6632599
15. Connolly, R., Tuunanen, T., Cheah, W.N.: Medical device security in the European Union: challenges and potential solutions. In: Medical device cybersecurity for engineers and manufacturers, pp. 15–32. Springer, Berlin (2021)
16. Islam, I., Islam, M.N.: Digital intervention to reduce counterfeit and falsified medicines: a systematic review and future research agenda. J. King Saud Univ. Comput. Inform. Sci. **34**(9), 6699–6718 (2022). https://doi.org/10.1016/j.jksuci.2022.02.022
17. Sharma, A., et al.: Supply chain management using blockchain security enhancement. Adv. Inform. Commun. Technol. Comput. (2023). https://doi.org/10.1007/978-981-19-9888-1_15
18. Seh, A.H., et al.: Healthcare data breaches: insights and implications. Healthcare **8**(2), 133 (2020). https://doi.org/10.3390/healthcare8020133
19. Dwaraka Srihith, I., et al.: Firmware attacks: the silent threat to your IOT connected devices. Int. J. Adv. Res. Sci. Commun. Technol. (2023). https://doi.org/10.48175/ijarsct-9104
20. Khan, S., et al.: Exploring the impact of covid-19 pandemic on medical supply chain disruption. J. Ind. Integrat. Manage. **06**(02), 235–255 (2021). https://doi.org/10.1142/s2424862221500147
21. Bartock, M., et al.: Hardware-enabled security : [Preprint], 2022. https://doi.org/10.6028/nist.ir.8320.
22. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) http://data.europa.eu/eli/reg/2019/881/oj
23. The EU Cybersecurity Certification Framework.: Available at: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework (Accessed: 23 Jun 2023).
24. Chiara, P.G.: The cyber resilience act: the EU commission's proposal for a horizontal regulation on cybersecurity for products with Digital Elements. Int. Cybersecur. Law Rev. **3**(2), 255–272 (2022). https://doi.org/10.1365/s43439-022-00067-6
25. The NIS2 directive: A high common level of cybersecurity in the EU: Think tank: European parliament (no date) Think Tank | European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333 (Accessed: 23 Jun 2023).
26. Bhushan, B., Kumar, A., Bhattacharya, P., Kumar, A.: Towards a secure and sustainable internet of medical things (IoMT): requirements, design challenges, security techniques, and future trends.

Sustainability **15**(7), 6177 (2023). https://doi.org/10.3390/su15076177
27. Lie, M.F., Sánchez-Gordón, M. and Colomo-Palacios, R.: DevOps in an ISO 13485 regulated environment, In Proceedings of the 14th ACM/IEEE International symposium on empirical software engineering and measurement (ESEM) [Preprint], 2020. https://doi.org/10.1145/3382494.3410679.
28. Flood, D., et al.: A roadmap to ISO 14971 implementation. J. Soft.: Evol. Process **27**(5), 319–336 (2015). https://doi.org/10.1002/smr.1711
29. Jordan, P.: Standard IEC 62304—medical device software—software lifecycle processes, In IET seminar on software for medical devices [Preprint], 2006. https://doi.org/10.1049/ic:20060141
30. Medical devices—part 1: application of usability engineering to medical devices: ANSI/AAMI/IEC 62366–1:2015/(R)2021+AMD1:2020; medical devices—Part 1: application of usability engineering to medical devices + Amendment 1 [Preprint], 2020. https://doi.org/10.2345/9781570207631.ch1.
31. MacMahon, S.T., Cooper, T., McCaffery, F.: Revising IEC 80001–1: risk management of health information technology systems. Comput. Stand. Interfaces **60**, 67–72 (2018). https://doi.org/10.1016/j.csi.2018.04.013
32. ISO 13482:2014: ISO, 2021. Available at: https://www.iso.org/standard/53820.html (Accessed: 23 Jun 2023)
33. More Efficient Supply Chain—GS1. Available at: https://www.gs1.org/industries/healthcare/saving-money/more-efficient-supply-chain (Accessed: 23 Jun 2023).
34. Boyens, J. et al.: Cybersecurity supply chain risk management for systems and organizations [Preprint], 2022a. https://doi.org/10.6028/nist.sp.800-161r1
35. Das, P., Gupta, I., Mishra, S.: Artificial intelligence driven cybersecurity in digital healthcare frameworks. In: Securing next-generation connected healthcare systems, pp. 213–228. Academic Press, California (2024)
36. Kott, A., Theron, P.: Doers, not watchers: intelligent autonomous agents are a path to cyber resilience. IEEE Secur. Priv. **18**(3), 62–66 (2020)
37. Bécue, A., Praça, I., Gama, J.: Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artif. Intell. Rev. **54**(5), 3849–3886 (2021)
38. Carmody, S., Coravos, A., Fahs, G., Hatch, A., Medina, J., Woods, B., Corman, J.: Building resilient medical technology supply chains with a software bill of materials. NPJ Digit. Med. **4**(1), 1–6 (2021)
39. Konstantinov, A.V., Utkin, L.V.: Interpretable machine learning with an ensemble of gradient boosting machines. Knowl.-Based Syst. **222**, 106993 (2021)
40. Zhuang, F., Qi, Z., Duan, K., Xi, D., Zhu, Y., Zhu, H., He, Q.: A comprehensive survey on transfer learning. Proceed. IEEE **109**(1), 43–76 (2020)
41. Nguyen, T.T., Reddi, V.J.: Deep reinforcement learning for cyber security. IEEE Trans. Neural Netw. Learn. Syst. **34**(8), 3779–3795 (2021)
42. Agarwal, A., Kakade, S.M., Lee, J.D., Mahajan, G.: On the theory of policy gradient methods: optimality, approximation, and distribution shift. J. Mach. Learn. Res. **22**(98), 1–76 (2021)
43. Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., Pospelova, V.: The emerging threat of ai-driven cyber attacks: a review. Appl. Artif. Intell. **36**(1), 2037254 (2022)
44. Laghrissi, F., Douzi, S., Douzi, K., Hssina, B.: Intrusion detection systems using long short-term memory (LSTM). J. Big Data **8**(1), 65 (2021)
45. Rasmy, L., Xiang, Y., Xie, Z., Tao, C., Zhi, D.: Med-BERT: pretrained contextualized embeddings on large-scale structured electronic health records for disease prediction. NPJ Digit. Med. **4**(1), 86 (2021)
46. Aziz, N., Akhir, E.A.P., Aziz, I.A., Jaafar, J., Hasan, M. H., Abas, A.N.C.: A study on gradient boosting algorithms for development of AI monitoring and prediction systems. In 2020 International conference on computational intelligence (ICCI) (pp. 11–16). IEEE, 2020
47. Hussain, F., Hassan, S.A., Hussain, R., Hossain, E.: Machine learning for resource management in cellular and IoT networks: potentials, current solutions, and open challenges. IEEE Commun. Surv. Tutor. **22**(2), 1251–1275 (2020)
48. Whig, P., Kouser, S., Bhatia, A.B., Nadikattu, R.R., Alkali, Y.J.: Leveraging meta-heuristics in improving health care delivery: a comprehensive overview. Nature-Inspir. Methods Smart Healthcare Syst. Med. Data (2023). https://doi.org/10.1007/978-3-031-45952-8_8
49. Wang, Z., Cha, Y.J.: Unsupervised deep learning approach using a deep auto-encoder with a one-class support vector machine to detect damage. Struct. Health Monit. **20**(1), 406–425 (2021)
50. Pinheiro Cinelli, L., Araújo Marins, M., Barros da Silva, E.A., Lima Netto, S.: Variational autoencoder. In: Variational methods for machine learning with applications to deep networks, pp. 111–149. Springer International Publishing, Cham (2021)
51. Regulation—2017/745—EN—Medical Device Regulation—EUR-Lex (europa.eu)
52. Alshar'e, M.: Cyber security framework selection: comparision of NIST and ISO27001. Appl. Comput J. (2023). https://doi.org/10.52098/acj.202364
53. Kaikkonen, L., Parviainen, T., Rahikainen, M., Uusitalo, L., Lehikoinen, A.: Bayesian networks in environmental risk assessment: a review. Integr. Environ. Assess. Manag. **17**(1), 62–78 (2021)