

Article

Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications

Pangkaj Chandra Paul ^{*,†} , John Loane [†], Fergal McCaffery [†] and Gilbert Regan [†]

Regulated Software Research Centre, Dundalk Institute of Technology, A91K584 Dundalk, Ireland; john.loane@dkit.ie (J.L.); fergal.mccaffery@dkit.ie (F.M.); gilbert.regan@dkit.ie (G.R.)

* Correspondence: paulp@dkit.ie

† This paper is partially based on the conference paper: Paul, P.C.; Loane, J.; McCaffery, F.; Regan, G. A Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications*. 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2021, 704–710, doi:10.1109/PerComWorkshops51409.2021.9431069.

Abstract: Assuring security and privacy of data is a key challenge for organizations when developing WBAN applications. The reasons for this challenge include (i) developers have limited knowledge of market-specific regulatory requirements and security standards, and (ii) there are a vast number of security controls with insufficient implementation detail. To address these challenges, we have developed a WBAN data security and privacy risk management framework. The goal of this paper is trifold. First, we present the methodology used to develop the framework. The framework was developed by considering recommendations from legislation and standards. Second, we present the findings from an initial validation of the framework's usability and effectiveness of the security and privacy controls. Finally, we present an updated version of the framework and explain how it addresses the aforementioned challenges.

Keywords: wireless body area network; security; privacy; risk management



Citation: Paul, P.C.; Loane, J.; McCaffery, F.; Regan, G. Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications. *Appl. Syst. Innov.* **2021**, *4*, 76. <https://doi.org/10.3390/asi4040076>

Academic Editor:
Subhas Mukhopadhyay

Received: 31 July 2021
Accepted: 24 September 2021
Published: 12 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A Wireless Body Area Network (WBAN) application is composed of intelligent, low-power sensor nodes which monitor body functions and physiological states. These sensor nodes can collect and process data, store it locally and transmit it to an actuator or a local server. WBAN based applications collect personal health record (PHR) data, which can provide real-time healthcare monitoring services. A general architecture for WBAN applications is illustrated in Figure 1. A WBAN based health care application can provide long term health monitoring of a patient's natural physiological states without constraining their everyday activities. It also helps in the provision of a smart, easily accessible and affordable health care system. Additionally, a WBAN based health care application can also assist with diagnostic procedures, supervised recovery from a surgical procedure, and can handle emergency events [1].

The main design requirements for any WBAN application are that the body sensor node needs to be extremely small and thin, capable of wireless communication, and use minimal power for data collection and processing [2]. User requirements such as privacy, safety, ease of use, security and compatibility are also of great importance [3]. WBAN applications operate in an environment where many people have open internet access which leaves them vulnerable and open to many types of attacks and threats [4]. Open connectivity creates a large attack surface. Attacks can affect the performance and availability of the service, sometimes leading to life threatening situations [4]. Therefore, security and privacy safeguards need to be considered during development of this type of healthcare application.

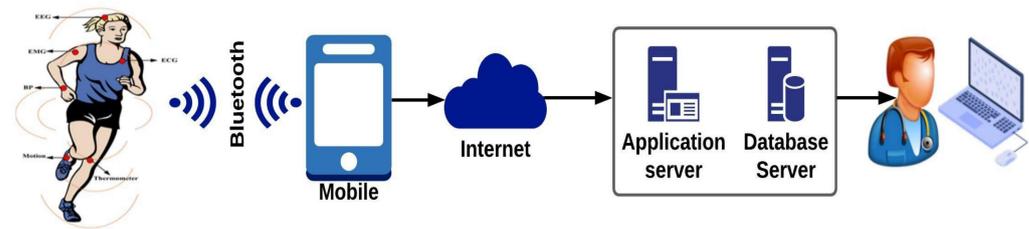


Figure 1. General architecture of WBAN application [5].

The goal of this research paper is to present the development of a WBAN data security and privacy risk management framework, and to demonstrate how the framework addresses the challenges faced by developers in assuring security and privacy of WBAN based healthcare applications. This paper is extended from the previous study which was presented at the PerCom 2021 conference [6]. The paper is organized as follows: Section 2 presents the various regulations and risk management frameworks for healthcare applications. Section 3 presents the methodology used to develop and validate the framework. Section 4 presents the challenges faced by developers in adopting security and privacy standards, while Section 5 presents the alpha version of the WBAN data security and privacy framework followed by implementation within an industrial setting which is outlined in Section 6. Section 7 presents an overview of the beta version of the framework. Section 8 presents the steps to conduct the security risk assessment at both the requirement analysis and system architecture phases. Section 9 outlines the steps to implement security risk controls followed by Section 10, which outlines the steps to evaluate the effectiveness of the controls. Section 11 presents a discussion about how the framework addresses the challenges. Finally, Section 12 concludes this paper.

2. Background and Related Work

Data security means ensuring that data are protected while the data are being collected, processed, stored and transmitted. The data confidentiality, integrity and availability (CIA) triad is a common concept to ensure data security. Confidentiality ensures that data are not made available or disclosed to unauthorized individuals or entities. Integrity provides assurance that data are not modified accidentally or deliberately. Availability ensures the reliable accessibility of the system for authorized entities. Data privacy governs how data are collected, shared and used; it also ensures that only authorized persons can access the data [7]. However, data privacy cannot be achieved by securing only personally identifiable information (PII). As PHR data include both PII and patient health record data, privacy needs to be assured for both PII and health record data.

WBAN applications are vulnerable and open to many types of attacks and threats as sensor nodes operate in an environment where the sensor node uses low powered radio signals for communication. These attacks make the security and privacy of PHR data one of the primary challenges for WBAN systems. We have previously conducted a structured literature review and identified a total of 11 types of attacks on WBAN applications, in addition to identifying 22 security and privacy requirements for WBAN applications [8].

2.1. Regulations and Standards

Nowadays, healthcare applications and medical devices need to be compliant with various regulations. Ensuring security and privacy is a vital requirement for compliance with these regulations. This section presents the various regulations from the US and EU markets with their individual security and privacy requirements.

- FDA: The 800 series under Title 21 of the Code of Federal Regulations (CFR) outlines the regulations which govern medical devices within the United States (US). This regulation is enforced by the Food and Drug Administration (FDA). The FDA recognizes that the security and privacy of medical devices is a shared responsibility among stakeholders, including health care facilities, patients, health care providers, and man-

ufacturers of medical devices [9]. Medical devices should be designed to protect assets and functionality, and to reduce the risk of loss of authenticity, availability, integrity and confidentiality. As part of Title 21 CFR part 820 -Quality System Regulation states that the medical device manufacturer needs to employ a cybersecurity risk management program [10]. The aim of the risk management program is to reduce the likelihood of the device functionality being compromised, intentionally or unintentionally, by inadequate cybersecurity. An effective cybersecurity risk management program should address cybersecurity in both premarket and postmarket medical device development lifecycle phases.

- HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was brought forward by the Secretary of the US Department of Health and Human Services (HHS) as a law to enforce regulations for governing electronically managed patient information in the healthcare industry, and includes privacy and security protection of electronic personal health information(e-PHI) [11]. Title II of HIPAA provides five rules: Privacy Rule, Transactions and Code Sets Rule, Security Rule, Unique Identifiers Rule, and Enforcement Rule. The purpose of these rules is to prevent fraud and abuse within the healthcare system. The Privacy Rule requires implementing different policies and procedures to provide federal protections for personal health information held by covered entities. This rule also ensures patient rights concerning that information. The Security Rule specifies a series of administrative, physical, and technical safeguards to assure the confidentiality, integrity, and availability of electronically protected health information. Below are the key security and privacy requirements outlined in the HIPAA Security and Privacy Rule:
 - Ensure the confidentiality, integrity, and availability of all PHI while they create, receive, store and transmit.
 - Identify and protect against reasonably anticipated threats to the security or integrity of the information.
 - Protect against reasonably anticipated, impermissible uses or disclosures of the information.
 - Perform risk analysis as part of the security management processes
 - Implement technical policies and procedures that allow only authorized persons to access e-PHI.
 - Implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed.
 - Implement security measures to guard against unauthorized access to e-PHI.
- EU Medical Devices Regulations: The European Medical Device Regulation (EU MDR) ensures high standards of safety, security, and quality of medical devices being marketed within the EU for human uses [12]. EU MDR is also known as EU Directive 2017/745 and 2017/746, which was published in 2017. The cybersecurity requirements listed in Annex I of the MDR deal with the medical device's premarket and postmarket aspects. Below is the list of key cybersecurity requirements from the EU MDR:
 - Manufacturers shall establish, implement, document and maintain a risk management system.
 - Medical device software should be developed in accordance with the state-of-the-art principles of the development life cycle, risk management, including information security, verification and validation.
 - Manufacturers shall set out minimum requirements concerning hardware, IT networks security measures, including protection against unauthorized access.
 - Implement proper safeguards to avoid unauthorized access, disclosure, dissemination, alteration or loss of information and personal data processed.
 - Implement adequate safeguards to ensure confidentiality of records and personal data of subjects.
 - Implement proper incident response plan and safeguards in case of a data security breach in order to mitigate the possible adverse effects.

- **GDPR:** The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for citizens in the European Union (EU) and European Economic Area [13]. It was introduced in May 2018. The EU commission designed the GDPR to achieve key goals such as, (1) protect the rights, privacy and freedom of individuals in the EU, (2) reduce the barrier for free movement of data inside the EU, (3) inform individuals how personal data will be processed and who will be given access, (4) individuals will be able to obtain their data and reuse it for their own purposes and (5) individuals have the right to restrict access and erase their data.

Adoption of the following standards can help an organization achieve regulatory compliance from a security and privacy perspective:

- **FDA premarket and postmarket guidelines:** The FDA provides premarket and postmarket guidelines for organizations and developers that need to be considered during the development lifecycle of a medical device or healthcare application. The premarket guidance [14] outlines the following key security and privacy related recommendations for medical device manufacturers:
 - To employ a risk-based approach to the design and development of medical devices with appropriate cybersecurity protections.
 - Take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the product's lifecycle.
 - Identify the assets, threats, and vulnerabilities.
 - Perform an impact assessment of the threats and vulnerabilities on device functionality and end-users.
 - Assess the likelihood of a threat and of a vulnerability being exploited.
 - Determine the risk levels and suitable mitigation strategies.

As cybersecurity risks to medical devices are continuously evolving, it is impossible to mitigate the risk within the premarket controls alone. Therefore, the FDA provides the following key guidance for manufacturers as part of postmarket medical device development [15]:

- Take an approach to monitor the cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk.
- Identify and assess the threats and vulnerabilities being exploited.
- Take a holistic approach to detect and assess the threat sources.
- Establish a communication process for incident response.
- Design a verification and validation process for software updates and patches used to remediate the vulnerabilities.
- **IEC 62304:** IEC 62304 provides guidelines for each stage of the medical device software lifecycle with activities and tasks required for the safe design and maintenance of medical device software [16]. This standard is recognized by the FDA, EU and other regulatory agencies across the world. IEC 62304 recommends that organizations establish and maintain a risk management process to manage risk associated with security. The process should provide a methodology to identify the vulnerabilities, evaluate the associated threats, and implement risk controls to mitigate these threats. Finally, the process should also monitor the effectiveness of the risk control.
- **NIST 800-53:** The NIST 800-53 standard provides security and privacy controls to protect the application, data, assets and organizations from a diverse set of attacks, threats and risks [17]. These controls can be employed as safeguards to assure confidentiality, integrity, and availability of the information while it is processed, stored and transmitted.
- **ISO 27002:** ISO 27002 is an information security standard developed by International Organization for Standardization (ISO) which provides best practice recommendations and information security controls to assure confidentiality, integrity, and availability of data [18]. This standard aims to guide organizations to select, implement, and manage controls to minimize security risk.

2.2. Risk Management Frameworks

This section presents two risk management frameworks the IEC 80001-1:2010 and the AAMI TIR57 which are widely used for developing healthcare applications. This section also outlines why they are not directly applicable to WBAN applications, even though they are specific to healthcare applications.

- IEC 80001-1:2010: IEC 80001-1—Application of risk management for IT-networks incorporating medical devices was introduced in 2010 to address risks associated with medical devices when connecting to IT-networks [19]. The framework aims to help organizations define the risk management roles, responsibilities, and activities to achieve medical device safety and security. IEC/TR 80001-2-2 [20] is a technical report that provides background processes to address security risk related capabilities for connecting medical devices to IT-networks.
- AAMI TIR57: AAMI TIR57 provides guidance for manufacturers to perform information security risk management to address security risks within medical devices [21]. AAMI TIR57 was developed with guidelines provided by ISO 14971 [22] and NIST SP 800-30 Revision 1—security risk management process developed for traditional IT systems [23]. The goal of AAMI TIR57 is to assist manufacturers with the following key outcomes: (1) identification of assets, threats and vulnerabilities, (2) estimation and evaluation of associated security risk, (3) selection of security risk controls and (4) monitoring the effectiveness of the security risk controls.

The risk management frameworks mentioned above are not directly applicable to WBAN applications for the following reasons:

- IEC 80001-1:2010 was primarily developed for applications which operate within a healthcare delivery organization's IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media.
- A WBAN application consists of resource constrained sensor devices which have limited memory and computational power and cannot accommodate complex security solutions like traditional healthcare applications. Neither framework provides any guidance for managing security and privacy risks for resource constrained sensor devices.

3. Methodology

This section presents the methodology used to develop a data security and privacy risk management framework for WBAN. The methodology used to conduct this research comprised of four key stages, as illustrated in Figure 2.

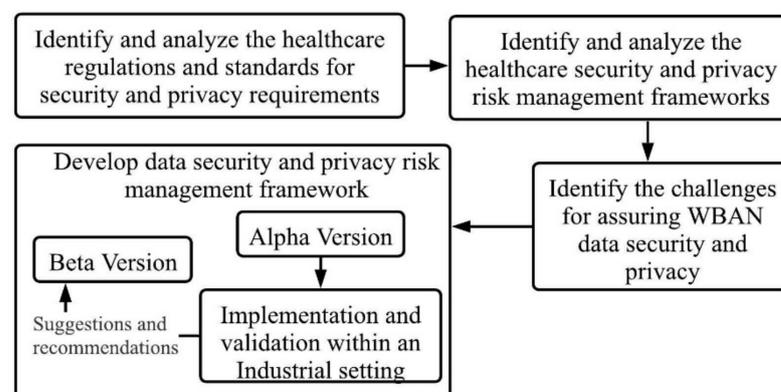


Figure 2. Methodology.

3.1. Identify and Analyse the Healthcare Regulations and Standards for Security and Privacy Requirements

The goal of this step was to identify and analyze the security and privacy recommendations provided by the various healthcare-related regulations and standards. The scope was limited to regulations that apply in the US and Europe. The approach taken for the identification and analysis was as follows:

- The Regulated Software Research Centre, of which the authors are members, is widely recognized for its research in the medical device regulatory world. Its members provided advice on the applicable regulations and standards. The respective regions legislative portal website was also checked to identify the regulations. This resulted in a total of four regulations which were the FDA's Code of Federal regulation for medical devices, HIPAA, EU MDR and GDPR.
- The resultant four regulations were analyzed to extract the security and privacy requirements for developing healthcare applications. The regulations, along with their respective security and privacy requirements are detailed in Section 2.1 above.
- Additionally, a snowballing approach was taken for reviewing each regulation to identify the security and privacy standards. Along with a snowballing approach and guidance from members of the Regulated Software Research, the following standards were identified as applicable: the FDA's premarket and postmarket guidelines, IEC 62304, NIST 800-53 and ISO 27002.
- The resultant five standards were analyzed to extract the security and privacy requirements. These security and privacy requirements are detailed in Section 2.1 above.

3.2. Identify and Analyse the Healthcare Security and Privacy Risk Management Frameworks

The goal of this step was to identify and analyze the risk management process recommended by the regulations and standards identified in the previous section (Section 3.1) to manage security and privacy risks throughout the development lifecycle of medical devices and healthcare applications. The risk management frameworks were analyzed to check whether they were applicable to the development of WBAN based healthcare applications. The approach taken during the identification and analysis process was as follows:

- Review the regulations and standards identified in the previous section (Section 3.1) for references to security and privacy risk management frameworks. The review resulted in a total of four risk management frameworks: ISO/IEC 80001-1:2010, AAMI TIR57, ISO 14971 and NIST 800-30.
- Analyze the risk management frameworks to identify which of them are specific for developing healthcare-based applications. An initial analysis found that only two of these four frameworks were 'healthcare specific' security and privacy risk management frameworks, that is ISO/IEC 80001-1:2010 and AAMI TIR57. Details of the risk management frameworks are outlined in Section 2.2. ISO/IEC 80001-1:2010 and AAMI TIR57 were selected for further analysis to identify whether both are applicable for developing WBAN based healthcare applications. It was found that neither of these frameworks were suitable for developing WBAN applications. The reason for their unsuitability is presented at the end of Section 2.2.

3.3. Identify the Challenges for Assuring WBAN Data Security and Privacy

The goal of this step was to identify the challenges faced by developers for assuring data security and privacy for WBAN based healthcare applications and complying with regulations. A two-step process was utilized to identify the challenges. The first step involved a literature review, while the second step involved an interview with the Chief Technology Officer (CTO) and the tech lead of an organization that develops a WBAN based fitness tracking application. The findings from the literature review and interview have been published here [24], and are summarised in Section 4. The following steps were utilised by the lead author of this paper to conduct the literature review:

- Conduct a search on IEEEExplore, ScienceDirect and Google scholar using the search string; “healthcare AND (security OR privacy) AND (standard OR regulation OR compliance) AND (barrier OR challenges OR difficulties)”.
- Set inclusion criteria as follows: (1) presented the challenges for assuring security and privacy of healthcare applications that comply with regulations; (2) publication year: 2010–2020; (3) language is English and full text available.
- The initial search resulted in a total of 320 research papers.
- In the first screening each paper was analyzed by reviewing the abstract and conclusion. If the paper addressed any challenges, then it was selected for the second screening. A total of 125 papers out of 320 were selected for the second screening.
- In the second screening each paper was analyzed by reading the full text and checking whether the paper presented any challenges for assuring security and privacy of healthcare applications that comply with regulations. The second screening resulted in a total of 19 papers out of 125.
- Finally, a list of challenges was recorded from those papers which is presented in Section 4.

3.4. Develop the Proposed Security and Privacy Framework

The following steps were used to develop the security and privacy risk management framework:

- Identify the possible threats and vulnerabilities of a WBAN based healthcare application by conducting threat modeling.
- Review the report from threat modeling to identify the respective control(s) for each threat and vulnerability.
- Develop the implementation details for these controls (presented in Section 5.2.).
- Validate the effectiveness of the controls by implementation in an industrial setting. This is outlined in Section 6.
- Gather recommendations and suggestions for improvement to the alpha version from the organization who conducted the implementation. This is outlined in Section 6.5.

Each of the suggestions were then reviewed by the authors of this paper. All the suggestions were considered, and appropriate action was taken during development of the beta version. For example, the developer suggested to identify the threats and vulnerabilities at the requirement analysis phase to produce the security and privacy requirements. To address this suggestion a security risk assessment step was designed to be conducted in both the requirement analysis and the system architecture phases (presented in Section 8.3). Sections 7–10 present the detailed steps and implementation process of the beta version of the framework.

4. Challenges

The list of challenges from both the literature review and interview is presented in Table 1. The second column indicates whether the challenges were identified by literature review or by interview, or indeed by both literature review and interview.

Table 1. List of challenges.

Challenges	Sources
Lack of trained staff, responsibilities, budget, and management support	Literature [25–34]
The existing standards are too complex and complicated to implement	Literature [27,30,35–37]
Limited knowledge about market-specific regulatory requirements, security standards, and policies	Literature & Interview [32,36,38–40]

Table 1. *Cont.*

Challenges	Sources
Lack of comprehensive understanding of the architecture for WBAN security and privacy	Interview
Understanding the data flow around the system and what assets need to be protected	Interview
Standards outline each security control at a very high-level with limited amount of implementation details	Literature & Interview [27,33]
Identification of appropriate security controls with respective implementation details to ensure CIA and privacy of data	Literature & Interview [41]
Due to a vast number of controls, the challenge is prioritizing these controls in addition to planning releases without compromising security and privacy	Interview
Lack of security mechanisms for sensor device nodes connected to wireless networks, which are often limited by physical memory, computational power and storage	Literature & Interview [37,38,42,43]

5. Data Security and Privacy Framework (Alpha Version)

The alpha version of the data security and privacy framework consists of the following key stages:

- Identification of possible threats and vulnerabilities.
- Implement controls to protect the application against those threats and vulnerabilities.
- Evaluate the effectiveness of the controls.

The remainder of this section describes each stage (parts 1, 2 and 3), and also outlines how the framework should be used (part 4).

5.1. Identification of Possible Threats and Vulnerabilities

A structured process is required to examine how vulnerable an application is, and which types of attack can be launched to compromise the application. Threat modelling is a widely recognised process for identifying the possible threats to an application and is considered a significant step in assuring security. Threat modelling activities will start with defining the scope and data flow of the application. There are several tools and methods available to conduct threat modelling such as STRIDE, Linddun, The Process for Attack Simulation & Threat Analysis (PASTA), and Trike.

5.2. Implement Controls to Protect the Application against Those Threats and Vulnerabilities

One of the key stages in the development of this framework was to identify appropriate WBAN security and privacy controls with implementation details to mitigate the risks. The controls were identified by considering the potential security and privacy weaknesses of WBAN application ecosystems and mapping them against controls from the standards. Both ISO 62304 and AAMI TIR57 recommend considering the security capabilities outlined by the ISO/IEC 80001-2-2 while developing security and privacy requirements. Therefore, the ISO/IEC 80001-2-2 standard was selected as the primary standard for developing data security and privacy guidelines. To identify appropriate security controls and to develop the implementation detail for each control, the three-step process illustrated in Figure 3 was followed.

5.2.1. Control Collection

The ISO/IEC 80001-2-2 technical report provides 19 security capabilities with high-level details for Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs), but this technical report does not provide any security control implementation details. The ISO/IEC 80001-2-8 [44] technical report guides the establishment of the security

capabilities identified in ISO/IEC 80001-2-2. ISO/IEC 80001-2-8 also provides security controls from other standards such as NIST 800-53, ISO 27002 [18], and ISO 27799 [45]. These controls will help HDOs and MDMs to implement each capability identified in ISO/IEC 80001-2-2. In this step, all the controls for the respective security capabilities were collected for further analysis. Appropriate controls were selected using exclusion criteria and a review process which is described in the next step.

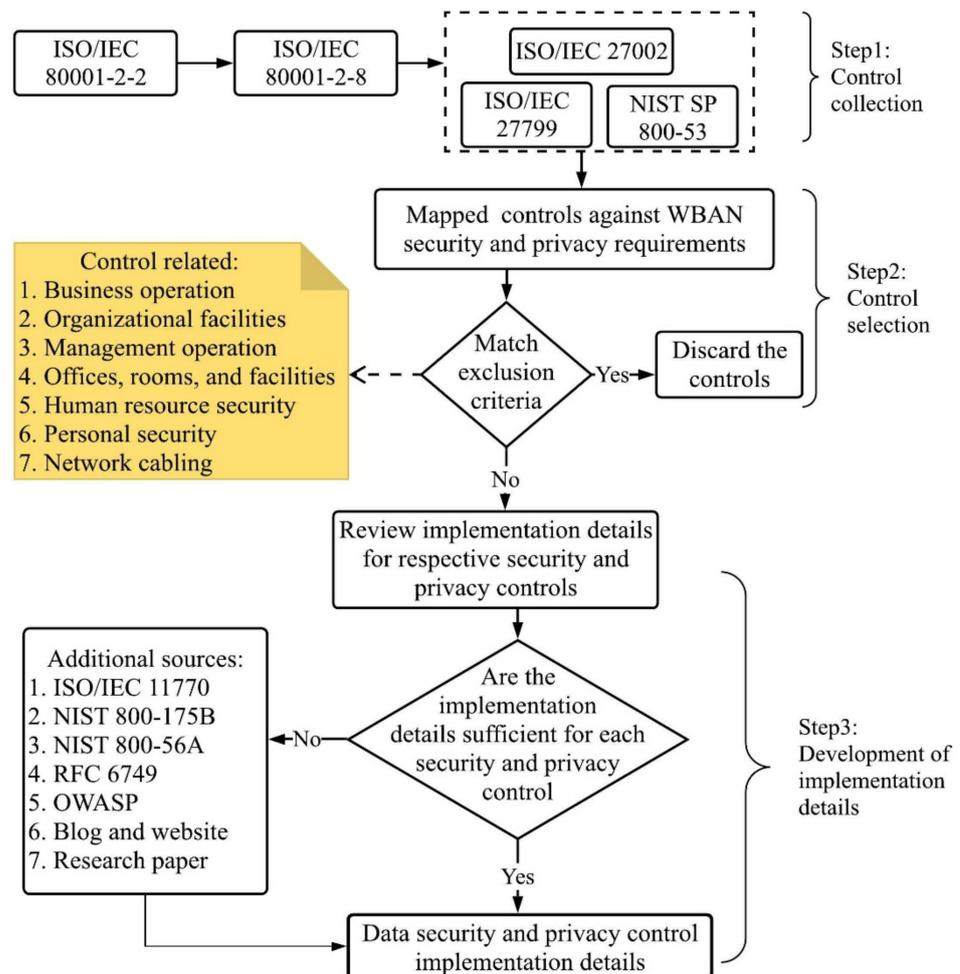


Figure 3. Data security and privacy control guidelines development process.

5.2.2. Control Selection

Each control was mapped to the WBAN security and privacy requirements that the authors had previously identified through a literature review, which is presented in [8]. Controls were then selected by excluding controls that related to: (1) Business operation, (2) Organizational facilities, (3) Management operation, (4) Offices, rooms and facilities, (5) Human resource security, (6) Personal security and (7) Network cabling. The controls related to security and privacy requirements such as access control, authorization, cryptography, key management, non-repudiation and intrusion detection are included.

5.2.3. Development of Security Control Implementation Details

As stated earlier, ISO/IEC 80001-2-8 refers to other standards such as NIST 800-53, ISO 27002 or ISO 27799 for implementation guidelines. Each control’s implementation details were extracted from the respective standards for review. A review team was setup which composed of the lead author of this paper, a tech lead and a senior developer from Company A. During the review process, each control’s implementation details were checked for whether it had enough detail for developers to implement. If the implementation details

were not adequate, then further details were selected from other sources. Other sources included standards or technical reports as detailed in Figure 3, OWASP guidelines, blogs, websites and scientific research papers. For example, the ISO/IEC 80001-2-8 proposes the use of a key management process as a risk control to generate, distribute and revoke a cryptographic key. To achieve this the standard refers to Section 10.1.2 of ISO 27002 for further details. Section 10.1.2 of ISO 27002 provides very high level and generic details about a key management process and does not provide any information about how the key will be generated and how the key will be transferred from the mobile application to the sensor device. ISO 27002 again refers to another standard ISO/IEC 11770 [46] for further details about key management, however ISO/IEC 11770 only outlines the details about the key generation and not about the key transfer. From the above example, the developer needs to review three different standards to find implementation details for key management. A goal of this framework is to provide implementation details for each security and privacy control. As an example, implementation details for key management, which a developer can quickly adopt, are outlined in Appendix B.

5.3. Evaluate the Effectiveness of the Controls

To evaluate the effectiveness of the controls an assessment needs to be conducted on the application. This assessment will help to identify to what degree the application will assure the security and privacy of the PHR data. According to NIST 800-53, vulnerability scanning and/or penetration testing can be used as part of the assessment process. An organization can conduct an assessment by forming a team of people within the organization who have technical expertise in conducting an assessment. Additionally, an organization can also onboard external resources to conduct the assessment, for example security consultants.

5.4. Implementation Process

The implementation of the data security and privacy framework commences by defining the scope and the WBAN application use-cases. The developer then needs to convert the proposed use-cases into a data flow diagram which will be used as input for the threat identification process. As discussed in the threat identification section, a threat modelling technique can be used as part of the threat identification process. The threat modelling will produce a list of threats and vulnerabilities for the application. After that the developer needs to identify the controls provided the framework to mitigate the threats and vulnerabilities. If a control is not available in the framework the developer needs to find the control's implementation details from the standards or external sources and update the existing security and privacy guidelines. Once the control is selected, the developer needs to implement it. Finally, penetration testing needs to be conducted upon completion of the development. If the penetration test fails, then the reason for the failure needs to be reviewed. The penetration test can fail due not to implementing the control as outlined in the framework, or a new threat could be identified. If the penetration test failed due not to implementing a control properly, the developer needs to implement the control as presented in the framework. Suppose any new threats are identified during the penetration testing. In that case, the developer needs to find the respective security and privacy controls from the standards or external sources and implement them. Figure 4 illustrates the implementation process of the data security and privacy framework.

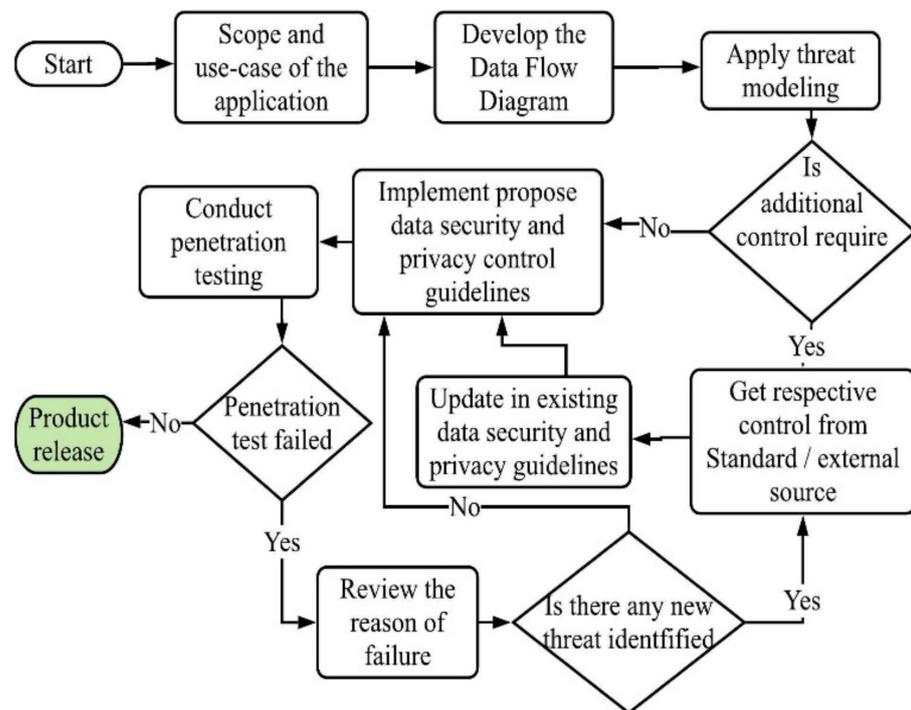


Figure 4. Implementation process of the data security and privacy framework.

6. Validation within an Industrial Setting

The purpose of this section is to demonstrate the validation of the security control implementation details provided in the WBAN risk management framework. This validation was achieved through implementation of the framework within Company A (an Irish WBAN development company). In this section we outline the results of threat modelling, which was conducted on Company A's WBAN application, along with the security controls which were implemented as a result of vulnerabilities identified through the threat modelling. Finally, the results of a penetration test are presented. The penetration test was conducted in order to verify to what degree the controls assure security and privacy of the WBAN fitness tracking application.

6.1. Scope and Application Use-Case

The FitnessX app is the first consumer product for Company A following on from the success of the core product for professional sports teams. The product uses a physical activity monitor, known as a pod, which uses GPS and a series of sensors to track an athlete's activity during training and gameplay, and relay this information to the app running on either iOS or Android over Bluetooth. In the app, users can sign up for an account and pair their device, before tracking sessions and syncing this data to the cloud. Sessions generate statistics and analysis which can be used by the individual to track their performance and they can choose to share some of their data in a global leader-board. They can also create mini private or group leagues to use the same leader-board functionality among a closed group of individuals.

6.2. Develop Data Flow Diagram

A data flow diagram (DFD) is used to provide an overview of the application and graphically represent the flow of the data through an information system or application. A DFD can also provide insight about input and output of data, how data will flow and where it will be stored in an application. There are several levels of DFDs that can be drawn for an application. These are categorised based on the level of complexity. Increasing the

level of a DFD increases the complexity. Level '0' and Level '1' are widely used levels of DFD.

6.3. Apply Threat Modelling

STRIDE is a widely recognized threat modelling technique for web-based applications. It was developed by Microsoft, which also provide an open-source tool named the Microsoft Threat Modelling Tool (TMT). This tool includes a graphical interface to conduct threat modelling. By using the graphical interface, a user can easily design the data flow diagram, configure necessary parameters and track the threat with respective implementation status. Conducting threat modelling using this tool is carried out in three steps:

- Design and configuration.
- Generate threat report.
- Identify the security controls by analyzing the report.

The design and configuration step starts by drawing the Data Flow Diagram (DFD). This DFD diagram is enhanced by adding the proper data flows, data stores, processes, interactors, and trust boundaries. Each of the DFD element properties is configured based on the respective element behaviour. For example, device attribute properties are configured by setting "Yes" to GPS, data, store log data, encrypted, write access, removable storage and backup. After that, each of the DFD elements is connected by defining the proper connectivity attribute. The connectivity attribute is set to "Bluetooth" from device to iOS and Android mobile app, and mobile app to REST API is set to "Wi-Fi". The REST API to Non-Relational database is configured as "wired" as both are deployed in cloud infrastructure. Finally, a trust boundary is configured to enable the trust level between DFD elements for data exchange. Figure 5 illustrates the application's updated DFD.

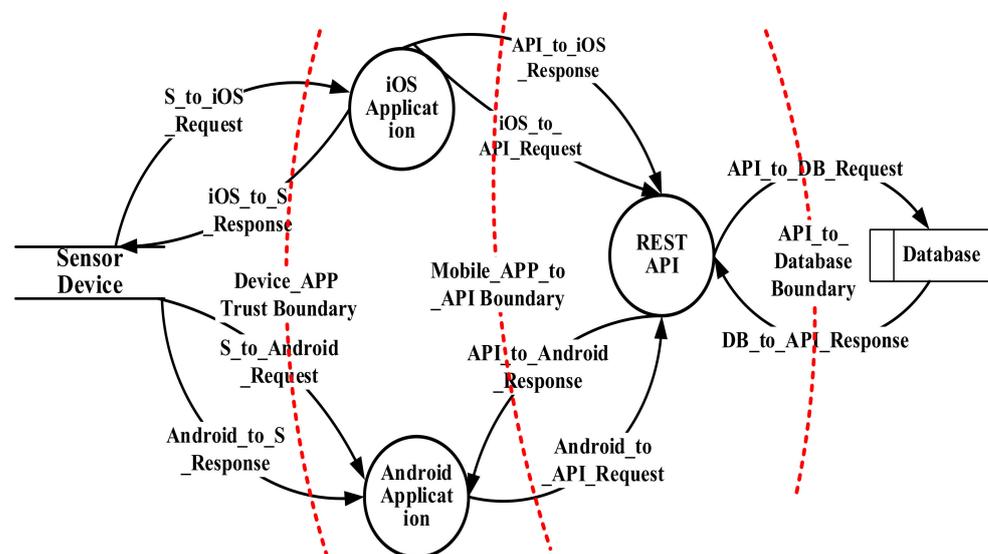


Figure 5. DFD diagram in Microsoft Threat Modeling Tool.

One of the key features of the Microsoft TMT tool is the ability to generate a threat report based on the DFD and element attributes. The threat report consists of a list of threats, threat categories, data flow directions and respective descriptions. Table 2 illustrates some sample threats and vulnerabilities with their respective descriptions.

Table 2. Sample vulnerabilities identified using Microsoft TMT tool.

Vulnerabilities	Description
The device data store could be corrupted	Data flowing across iOS_to_S_Response may be tampered with by an attacker. This may lead to corruption of device. Ensure the integrity of the data flow to the data store.
Potential weak protections for audit data	Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs. Ensure access to the log is through channels which control read and write separately.
Potential data repudiation by REST API	REST API claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Weak authentication scheme	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials and a weak credential change management system.
Potential lack of input validation for REST API	Data flowing across Android_to_API_Request may be tampered with by an attacker. This may lead to a denial of service (DoS) attack against REST API or an elevation of privilege attack against REST API or an information disclosure by REST API.

The description of each threat will help to identify the appropriate security controls. After exporting the threat report from the TMT tool, each threat needs to be reviewed to identify appropriate controls. During the review process, each threat description, threat type and data flow interaction needs to be considered. In some cases, if a threat does not contain enough description of the threat, then the threat category will be used to select a control as a countermeasure. Table 3 outlines a snapshot of the list of controls for mitigating the vulnerabilities.

Table 3. Mapping of the control for respective vulnerabilities.

Vulnerabilities	Control
Weak authentication scheme	Authentication
Weak credential transit	Authentication, Encryption
Potential data repudiation by Android and/or iOS application	Auditing, Non-repudiation
Potential process crash or stop for REST API due to the DOS attack	Access control, Intrusion detection, Auditing
Lack of data input validation	Data integrity, Input validation
Lack of encryption on transmitted data	Encryption, Communication security
Lack of encryption on private/sensitive data at rest	Encryption
Lack of physical tamper detection and response	Physical protection
Weak remote access controls	Access control
Lack of system hardening	Physical protection, Client platform security

6.4. Implementation of the Controls

Upon completion of the security control selection process, the next task was to implement the controls. The developer needed to follow the implementation details outlined in Appendix B for each control. The examples below illustrate the implementation details for one vulnerability from Table 3.

Vulnerability name: Weak authentication scheme

Security control: Authentication

Implementation details:

- Force users to have a strong password.
- Do not display or transmit the password in clear text. Validate the email address and password through an input validation technique. Validate email address by sending an email verification link.
- Lock user accounts after a certain number of failed logins attempts during a time-period.
- Maintain a list of commonly used, expected, or compromised passwords and update the list when passwords are compromised directly or indirectly.

6.5. Evaluate the Effectiveness of the Controls

The goal of this stage is to evaluate the effectiveness of the controls implemented to mitigate the threats and vulnerabilities. To carry out this evaluation, a penetration test was conducted with the help of a third-party penetration service provider. The goal of this stage is to evaluate the effectiveness of the controls implemented to mitigate the threats and vulnerabilities. To carry out this evaluation, a penetration test was conducted with the help of a third-party penetration service provider.

6.5.1. Scope of the Testing

The scope of the testing consists of what networks, applications, databases, accounts, people, physical security controls and assets will be attacked during the testing. So, the sensor device, mobile application, database, and respective communication medium was set as scope for the testing. Furthermore, a combination of manual and automated tools was used to exploit the system.

6.5.2. Testing Tools

As discussed in the previous section penetration testing can be conducted using a combination of manual and automated tools. Table A3 in Appendix C illustrates some of the automated tools used during penetration testing.

6.5.3. Penetration Test Result

The penetration tests identified two different types of vulnerabilities. Along with the test result, the penetration service provider also included recommendations on how to mitigate the vulnerabilities. Below is the list of vulnerabilities, along with mitigation recommendations which were identified during the penetration testing:

- Potential denial of service points: During testing, there were four potential DoS points found. These are requests that timeout within 10 s due to malformed data inside the payload. These can be run multiple times in multiple threads, driving up the usage and putting stress and strain on the service. Recommendation: It was advised that the API endpoints backend code should handle potential malformed data gracefully by input validation. Additionally, a proper HTTP response is needed if an API endpoint failed to process a request, so that the user can retry a request later. Action: Added input validation to validate the input data stream. Additionally, an error response code was also added to notify the user that API endpoints were unable to process the malformed input data.
- Security misconfiguration—Stack traces enabled: During testing, it was discovered that stack traces were enabled for some API endpoints. Recommendation: It was advised to turn off the stack trace for all endpoints and use a code review process to detect this coding error during development. Action: Stack trace was disabled for all the endpoints and the exception was written into a log file for auditing.

After making the necessary changes in the codebase to address the issues found during the penetration testing, the update was shared with the penetration service provider.

A retest of the updated application was conducted, and it was unable to reproduce these vulnerabilities.

6.6. Suggestions

Suggestions for improvement to the framework, received from the developer and the penetration test service provider, are described below.

- Identify threats and vulnerabilities at the requirement analysis phase to produce security and privacy requirements.
- A guideline for system architecture review would be useful to check whether the minimum security and privacy requirements are taken into consideration.
- A risk evaluation process would be helpful to identify the severity level of the identified threats and vulnerabilities.
- A risk treatment process will be useful to identify the risks which require controls to mitigate.
- A code review process during the control's implementation will help to minimize coding errors.
- Conduct unit testing during the implementation phase to identify whether the control is implemented properly.

By considering the above suggestions, the beta version of the framework was developed which is presented in Section 7.

7. Overview of the Data Security and Privacy Risk Management Framework (Beta Version)

ISO 62304 is a widely known standard which provides guidelines for developing healthcare applications [16]. This standard states that organizations need to implement a risk management process while developing healthcare software to assure security and privacy. ISO 62304 refers to AAMI TIR57 for managing security and privacy risks during development. The framework proposed in this paper is based on the guidelines provided by AAMI TIR 57. Furthermore, security and privacy activities in the healthcare application lifecycle guidance provided by IEC 80001-5-1 were also taken into consideration. The framework consists of three different stages: (1) Security and privacy risk assessment, (2) Security and privacy risk controls and (3) Evaluation of overall residual security and privacy risk acceptability. These stages are similar to AAMI TIR57, but is differentiated as follows:

- AAMI TIR57 does not clearly define how to conduct the security and privacy risk assessment at both the requirements analysis and the system architecture phases. This framework provides the steps to conduct security and privacy risk assessment at both phases. Additionally, the framework also provides a list of assets, threats and vulnerabilities which are specific to WBAN applications, which can be used as a starting point for conducting risk analysis.
- AAMI TIR57 does not provide any design review guidelines at the system architecture phase. The proposed framework added the design review guidelines recommended by IEC 80001-5-1.
- TIR57 does not include risk treatment to identify unacceptable risks which require controls to mitigate. This framework provides risk treatment steps as part of the risk assessment.
- This framework also consists of a mapping of possible threats and vulnerabilities with respective controls along with implementation details for the controls.
- This framework provides steps and tools to conduct in-house vulnerability scans and penetration testing.

The framework takes initial product requirements as an input but does not perform any validation or verification of the quality of the product requirements. To develop quality product requirements, guidelines provided by ISO/IEC 62304 can be utilized. To

implement this framework an organization needs to gather a team. Table 4 outlines the respective tasks of each role related to the implementation of the framework. In the case of limited resource in an organization, a single resource can carry out multiple roles and conduct more than one task.

Table 4. Team structure for implementing the proposed framework.

Task No.	Task Definition	Key Roles
1	Defining the scope	* Executives, ** Management, *** Assessor
2	Risk analysis	Management, Assessor, **** Third-party resource (if needed)
4	Security and privacy risk evaluation	Executives, Management, Assessor
5	Security and privacy risk control	Management, Assessor, Third-party resource (if needed)
7	Evaluation of overall residual security and privacy risk acceptability	Assessor, Management, Third-party resource (if needed)

* Executives: C-level executives of the organizations. ** Management: Product manager, Project manager, Team Lead, QA Lead. *** Assessor: Technical Lead, Software Architect, Product Owner, Senior Software Engineer, Senior QA Engineer. **** Third-party resource: Consultant, Penetration tester.

The three different stages of the beta version of the framework are outlined as follows; Section 8 presents the steps to conduct the security and privacy risk assessment at both the requirement analysis and system architecture phases. Section 9 outlines the steps to implement risk controls. Finally, Section 10 outlines the steps to evaluate the effectiveness of the controls.

8. Security and Privacy Risk Assessment

The security and privacy risk assessment helps to identify, analyze and evaluate potential security risks. This assessment helps an organization to make decisions about which risks require controls. Based on the recommendation of ISO 62304 Clause 5.2 and 5.3, this framework conducts risk assessment at the requirements analysis and system architecture phase of the development lifecycle.

The security and privacy risk assessment are divided into two key stages; (1) Risk analysis and (2) Risk evaluation and treatment. The risk analysis stage aims to identify the assets, threats, vulnerabilities and adverse impacts on an application. To assist with the security risk analysis, an organization may use relevant information obtained from a previously risk analysis of a similar type of product as a starting point. The degree of reusability of data from previous analyses depends on the difference between the applications from a security perspective. The risk evaluation and treatment stage will identify the acceptable risks and unacceptable risks which will require controls to mitigate.

8.1. Define Scope and Purpose

Before conducting the security and privacy risk assessment, organizations need to define and document the purpose and scope of the assessment. The scope will include:

- The intended use.
- Initial product requirements.
- Operating environment of the application.
- List of team members presented in Table 4 who will conduct the risk assessment.
- Timeline for the security and privacy risk assessment.

8.2. Risk Assessment Approach

There are three different risk assessment approaches—qualitative, quantitative and semi-quantitative. A qualitative assessment approach uses subjective values with a scale of qualifying attributes (e.g., Very Low, Low, Medium, High, Very High) to describe the

impact and likelihood of potential consequences of threats and vulnerabilities. The value of the impact and likelihood depends on the experience, expertise and competence of the person conducting the risk assessment. The qualitative assessment approach is very easy and less time consuming to perform compared to quantitative and semi-qualitative approaches, as this approach does not require any special tools or methods.

Quantitative risk assessments use a scale with numerical values based on a set of mathematical methods, rules and historical incident data. This approach is usually expressed in a monetary term which reflects the amount of money an organization may lose over a time period if the threat event occurs, or a vulnerability is exploited. The quality of the analysis depends on the accuracy of the numerical values, historical incident data and the validity of the methods used. A semi-quantitative risk assessment provides an intermediate level between the qualitative and quantitative risk assessment. To evaluate a security risk using a semi-quantitative approach, use bins (e.g., 0–4, 5–20, 21–79, 80–95, 96–100) and scales (e.g., 1–10) which will provide the textual evaluation of qualitative risk assessment and the numerical evaluation of quantitative risk assessment. The value of the bins and scales will help to communicate the risk to decision-makers as well as to perform a relative comparison of risk. This approach does not require the same level of skill, tools, mathematical methods and historical incident data as in quantitative risk assessment.

All three approaches have advantages and disadvantages. Quantitative risk assessment requires historical data to determine the likelihood of a threat event occurring or a vulnerability being exploited. Historical data that is not recently updated may add additional error to the risk assessment. Furthermore, it is difficult to calculate the cost of organization reputational damage, loss of competitive advantage and harm to user health if any threat event occurs or a vulnerability is exploited. Due to these facts, the quantitative approach will not be appropriate in information security and privacy risk assessment. This framework will use qualitative and semi-quantitative assessment approaches for evaluating the risk.

8.3. Security and Privacy Risk Assessment at the Requirements Analysis Phase

The objective of conducting a security and privacy risk assessment at the requirement analysis phase is to identify the risks, evaluate the identified risks, apply risk treatment to identify the risks which will require controls to mitigate and develop the security and privacy requirements. The initial product requirements and risk assessment approach will be taken as an input to conduct the security and privacy risk assessment at this phase. Figure 6 illustrates the steps to conduct a risk assessment at the requirements analysis phase.

Below is the list of key tasks to be conducted during the risk assessment at the requirements analysis phase:

- Apply risk analysis to identify the risk.
- Evaluate each risk to identify the acceptable and unacceptable risks.
- Update list of security and privacy requirements for unacceptable risk.

8.3.1. Risk Analysis

As part of the risk analysis, the following four tasks need to be conducted. Of the following four tasks, identify and document threats and identify and document vulnerabilities can be performed in any order.

8.3.1.1. Identify and Document the Assets

Assets of a WBAN application include sensor devices, information collected by the sensor devices, and server instances which are used to process and store the data. If the application interfaces with any external services such as third-party libraries or third-party application services, these also need to be taken into consideration. The assets will be documented in the security and privacy risk assessment report, along with the date that the assets were identified, and the name of the persons with their role as presented in Table

4. Figure 7 illustrates the list of assets for general WBAN applications which can be used as a starting point.

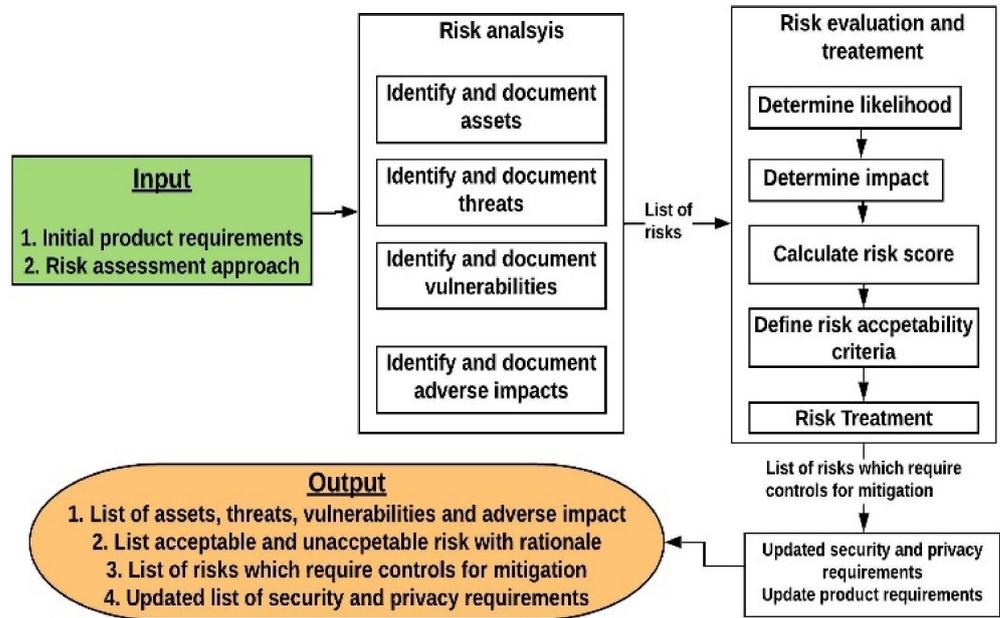


Figure 6. Security and privacy risk assessment steps in the requirement analysis phase.

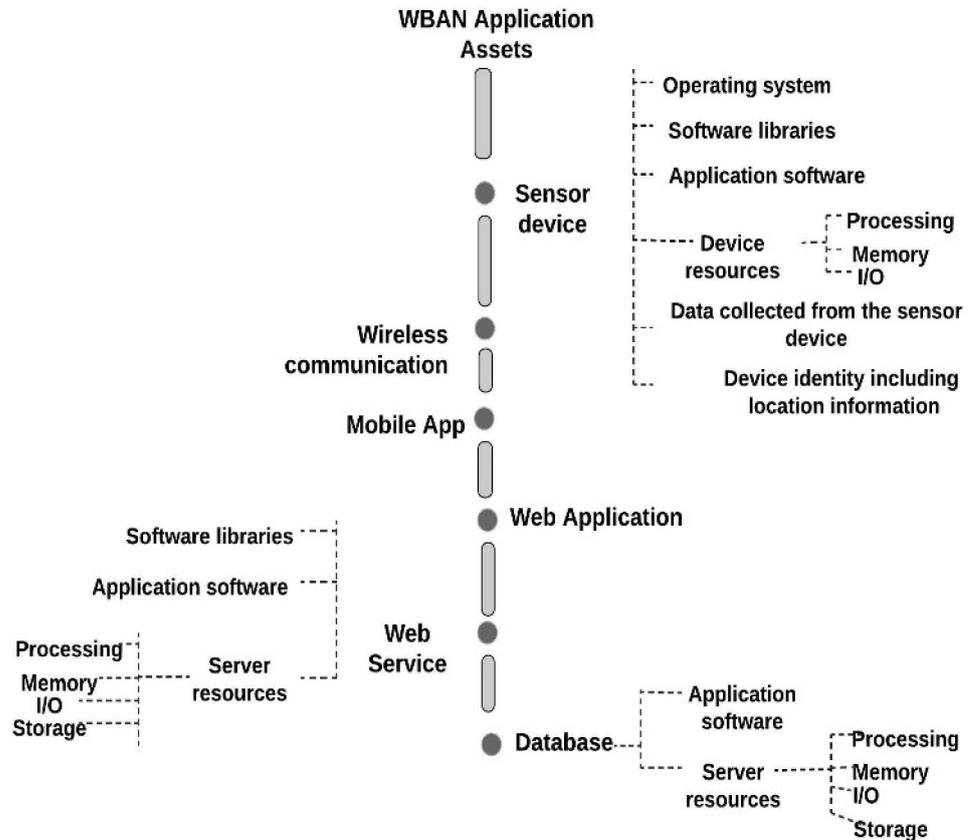


Figure 7. List of assets for WBAN applications.

8.3.1.2. Identify and Document Threats

To identify threats, the assessor team comprised of the technical lead, software architect, product owner, and senior software engineer needs to perform the following steps:

- Using Table A1 in Appendix A, select the threats related to the assets identified in the previous section.
- As the threat landscape is changing rapidly, it is recommended to check for newly discovered threats at the time of threat identification. To gather information about newly discovered threats, the assessor team can use various sources such as research articles, blog posts, OWASP (<https://owasp.org/www-community/attacks/> access on 30 July 2021), governmental agencies such as US-CERT (<https://www.us-cert.gov/resources/cybersecurity-framework> access on 30 July 2021), ENISA (<https://etl.enisa.europa.eu/> access on 30 July 2021), NIST (<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> access on 30 July 2021), BSI (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2 access on 30 July 2021) and private organizations such as HITRUST (<https://hitrustalliance.net/threat-catalogue/> access on 30 July 2021). Each newly discovered threat needs to be analyzed by studying the threat description, threat agents, possible attack scenarios and checking whether the same attack scenario can occur within the WBAN application. If a threat is applicable to WBAN applications, then the assessor team needs to identify the assets which will be affected if the threat occurs.
- Document the following in the security and privacy risk assessment report:
 - List of threats and respective affected assets.
 - Date when the threat identification was conducted.
 - The name and role of the person who conducted the threat identification.

8.3.1.3. Identify and Document the Vulnerabilities

To identify vulnerabilities, the assessor team need to perform the following steps:

- Review the list of vulnerabilities presented in Table A1 in Appendix A and select which are related to the identified assets.
- As the vulnerability landscape is constantly changing, the team need to check in various sources such as OWASP IoT Top 10 (https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project access on 30 July 2021) and OWASP Mobile Top 10 (<https://owasp.org/www-project-mobile-top-10/> access on 30 July 2021). During the review of a newly discovered vulnerability, the team needs to review the common security weaknesses and possible threat scenario section, in order to check whether the vulnerability can be exploited by any threat and affect any assets.
- Finally, the assessor team will document all the vulnerabilities details, name and role of the person, and date when the vulnerability identification process was conducted in a security and privacy risk assessment report.

8.3.1.4. Identify and Document the Adverse Impacts

An adverse impact of a security breach can be described in terms of loss or degradation of confidentiality, integrity, availability and privacy of data. TIR 57 outlines a set of questions to identify the adverse impact. This framework has extended those questions by the addition of point 4 below:

1. What is the impact if that asset's confidentiality is compromised, and the information it contained is made available to an attacker?
2. What is the impact if that asset's integrity is compromised?
3. What is the impact if that asset is made unavailable?
4. What is the impact if that asset's privacy is compromised?
5. Can the immediate impact of a compromised asset lead to another type of attack or vulnerability?

The members of the assessor team will review each threat and vulnerability and ask the above questions to identify the adverse impacts. For example, if the attacker launches a DoS attack on the webserver and makes the service unavailable, it will have an impact on

the service operation and business mission. Finally, document the adverse impact of each threat and vulnerability in the security risk assessment report.

8.3.2. Risk Evaluation and Treatment

The risk evaluation process helps to determine whether the threats and vulnerabilities are acceptable or not by calculating the impact and likelihood level. Furthermore, risk treatment will help to decide how each unacceptable risk will be addressed. Figure 8 illustrates the steps to conduct risk evaluation and risk treatment.

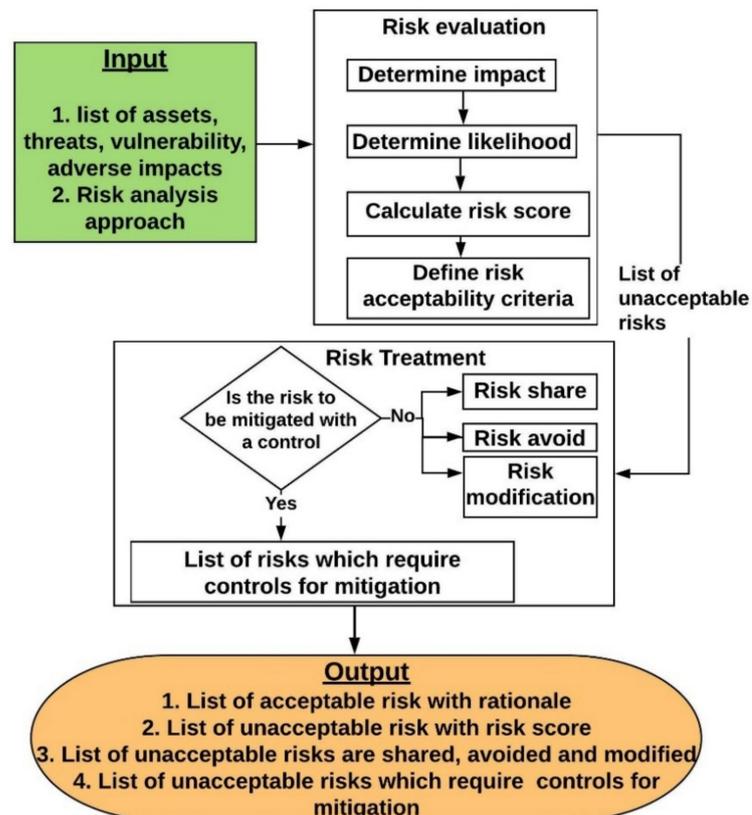


Figure 8. Steps to conduct risk evaluation and risk treatment.

8.3.2.1. Determine Impact

Impact refers to the extent to which a threat event might affect the application. Impact assessment criteria may include:

- Harm to user health and organization reputation.
- Operational impacts.
- Financial loss.
- Reputational harm.
- Loss of assets.

The assessor team also needs to consider the asset's valuation while calculating the impact score of a threat. An asset's valuation will include the importance of that asset to fulfil the business objectives, the replacement value of the asset and the business consequences due to the asset being lost or compromised. For example, a physical attack on a sensor device or a database will have a different impact on business operations. A physical attack on a sensor will only compromise that particular sensor device. If the database is compromised and data are lost, then it will have a much larger impact on financial, reputation, regulatory consequences and the operation of the application. Table 5 outlines the assessment scale for calculating impact scores.

Table 5. Assessment scale for impact.

Qualitative Values	Semi-Quantitative Values		Impact Definition
	Scale	Bins	
–			–
Very Low (1)	0–4	0	Threat event will have negligible adverse effects
Low (2)	5–20	2	Threat event will have limited adverse effects
Medium (3)	21–79	5	Threat event will have serious adverse effects
High (4)	80–95	8	Threat event will have catastrophic adverse effects
Very High (5)	96–100	10	Threat event will have multiple catastrophic effects

Table 6 illustrates an example for identifying the impact level of a physical attack on a sensor node. During the calculation, the impact level value is assigned to each impact factor and then the average is calculated.

Table 6. Impact analysis for physical attack on a sensor node.

Impact Factor	Impact Description	Impact Level		
		Qualitative	Semi-Quantitative Scale	Bins
Harm to user health	Only the person who is using the device will be in risk	Very High	100	10
Operational impacts	Only that device will be out of operation, it will not severely affect the overall application operation	Medium	30	5
Financial loss	Loss of a single device will have limited financial impact	Low	10	2
Reputational harm	Loss of a single sensor device will not create severe reputational harm	Medium	40	5
Loss of assets	Only one sensor device	Medium	30	5
	Average	Medium	70	5.2

8.3.2.2. Determine Likelihood

The likelihood represents the probability that a threat event will occur by exploiting one or more vulnerabilities. To estimate the likelihood, the assessor team needs to consider factors such as:

- Adversary intent and skill level.
- The affected asset.
- Historical evidence about the threat.

The same threat can have a different likelihood score based on the source of the threat and assets affected. For example, a DoS attack can compromise the availability of the web server and sensor devices. Initiating a DoS attack on a web server will be easier than the sensor device, as an attack on a sensor device will require advanced level skills and tools. In this scenario, the likelihood level will be different on both assets. So, during the assessment the assessor team needs to assign the likelihood level based on the available evidence, experience and expert judgement. Table 7 outlines the assessment scale for calculating likelihood level.

Table 7. Assessment scale for likelihood.

Qualitative Values	Semi-Quantitative Values		Likelihood Score Definition
	Scale	Bins	
Very Low (1)	0–4	0	Highly unlikely the threat event occurs or exploits the vulnerabilities
Low (2)	5–20	2	Unlikely the threat event occurs or exploits the vulnerabilities
Medium (3)	21–79	5	Somewhat likely the threat event occurs or exploits the vulnerabilities
High (4)	80–95	8	Highly likely the threat event occurs or exploits the vulnerabilities
Very High (5)	96–100	10	Almost certain the threat event occurs or exploits the vulnerabilities

Table 8 illustrates an example for identifying the likelihood level for a DoS attack on a web server. During the calculation, the likelihood level value is assigned to each likelihood factor and then the average of all the factors is calculated.

Table 8. Likelihood analysis for DoS attack on a web server.

Likelihood Factor	Likelihood Description	Likelihood Level		
		Qualitative	Semi-Quantitative Scale	Bins
Adversary intent	Make the whole application unavailable	Very High	100	10
Adversary skill level	Requires medium level skill to launch the attack	High	90	8
Affected asset	All assets that depend on the web server including the web server itself	Very High	100	10
Historical evidence	Very common attack for web server	Very High	100	10
Average		Very High	97.5	9.5

8.3.2.3. Calculate Risk Score

The aim of this stage is to calculate the risk score based on the impact and likelihood of threats and vulnerabilities. Appendix I of NIST 800-30 details calculating the risk score by multiplying impact times likelihood [23]. Alternatively, the team can use the CVSS risk score calculator to calculate the risk score [47]. A sample risk score matrix using a qualitative assessment approach is presented in Table 9.

Table 9. Risk score matrix for qualitative approach.

Impact	Likelihood				
	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Very High (5)	5	10	15	20	25
High (4)	4	8	12	16	20
Medium (3)	3	6	9	12	15
Low (2)	2	2	6	8	10
Very Low (1)	1	2	3	4	5

8.3.2.4. Risk Acceptability Criteria

Risk acceptability criteria will help to identify whether the threats and vulnerabilities are acceptable or unacceptable based on a set of criteria defined by the security and privacy evaluation team. There are no standard guidelines available to define the set of criteria. However, the team can consider various factors while defining the criteria such as:

- The organization's goals and objectives.
- Business operations.
- Application use case and technology stack used for developing the application.
- Legal and regulatory aspects.
- Budget and time for developing the application.

Table 10 outlines the risk acceptability criteria based on the risk score calculated using the qualitative approach. The proposed criteria treat the risks with a low or very low score as acceptable risks, and rest as unacceptable risks. If required, the evaluation team can make adjustments to the selection criteria. Finally, all unacceptable and acceptable risks with the rationale need to be documented in the security and privacy risk assessment report.

Table 10. Risk acceptability criteria (Qualitative approach).

Risk Score	Semi-Quantitative Values		Description
	Scale	Bins	
–	–	–	–
Very Low	0–4	0	The risks are acceptable. Plans mitigate the risk should be included in future plans.
Low	5–20	2	The risk may be acceptable over the short term. Plans to mitigate risk should be included in future plans and budgets.
Medium	21–79	5	The risk is unacceptable. Measures to reduce and mitigate the risk should be implemented as soon as possible.
High	80–95	8	The risk is unacceptable. Immediate measures to reduce and mitigate the risk should be implemented as soon as possible.
Very High	96–100	10	The risk is totally unacceptable. Immediate measures must be taken to mitigate the risk.

8.3.2.5. Risk Treatment

Risk Treatment is the process of selecting and implementing measures to address the risk. There are three options available for risk treatment which include:

- Risk modification: A risk which requires implementation of controls to reduce the impact and/or likelihood to an acceptable level.
- Risk avoidance: A risk can be avoided by eliminating the source of the risk or the asset exposed to the risk. This is usually applied when the severity of the risk impact and/or likelihood outweighs the benefits gained from implementing the countermeasure. For example, physically moving an on-premises server to an alternative location to mitigate the risk caused by nature might be outweighed with the cost of moving the server.
- Risk sharing: A risk can be fully or partially shared or transferred to another party. If the application is using any third-party libraries or public cloud services, risk related to these can be shared or transferred to the owner of the service.

The risk evaluation team will evaluate each unacceptable risk taking the above possible risk treatment options into account. Finally, the team will also record the list of risks that require controls, shared risks and avoided risks with rationale in the risk assessment report.

8.3.2.6. Update Security and Privacy Requirements

The goal of this stage is to update the security and privacy requirements with the list of security and privacy risks which require controls to mitigate. As risk analysis on the requirement analysis stage uses the initial product requirements, the updated security and privacy requirements will feed into the final product requirements. The following security and privacy requirements can be used as a starting point:

- Assure data confidentiality by protecting sensor nodes, and database server from unauthorized access. Assure data integrity by protecting data from external modification during transmission or while in storage.
- Assure that data will always be available to an authorized entity of the application.
- Assure privacy of the data during collection, processing and transmission. Allow access of the data only to authorized entities.
- Use a lightweight, memory and energy-efficient cryptographic algorithm for encryption.
- Facilitate a key management service for key generation, key refreshing, key agreement, key distribution and key revocation.
- Include a firewall and intrusion detection system to identify and block suspicious activity on a network.
- Include logging for auditing and accountability.
- Include a data backup strategy to assure high availability of the application.

After identifying the security and privacy requirements the following two tasks need to be conducted:

- Update the initial product requirements with security and privacy requirements.
- Document the security and privacy requirements in the security assessment report.

8.4. Security and Privacy Risk Assessment at the System Architecture Phase

To conduct security and privacy risk assessment at the system architecture phase, the updated product requirements and system architecture will be taken as an input to this phase. Figure 9 illustrates the steps to conduct a risk assessment at the system architecture phase.

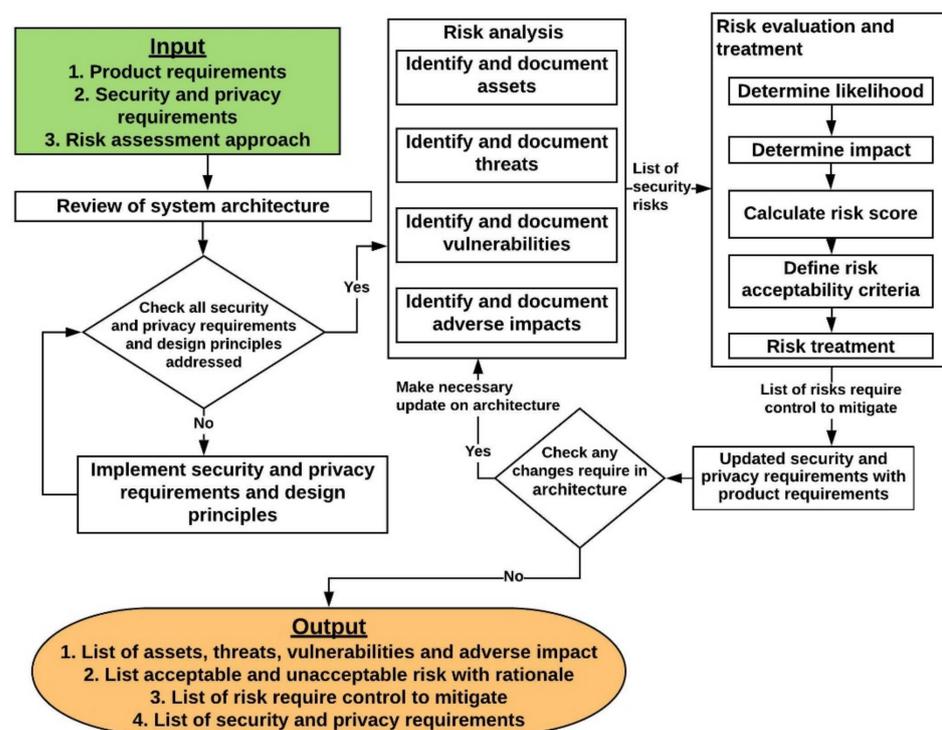


Figure 9. Security and privacy risk assessment steps in the system architecture phase.

Below is the list of key tasks that will be conducted during the security and privacy risk assessment at the system architecture phase:

- Review system architecture according to security and privacy principles and requirements identified in Section 8.3.2.6.
- Apply risk analysis to identify the security and privacy risks.
- Identify acceptable and unacceptable risks.
- Identify the list of unacceptable risks which will require controls to mitigate.
- Update security and privacy requirements and product requirements with unacceptable risks.
- Check whether any update to the current system architecture is required due to newly identified security and privacy requirements. If yes, then make necessary changes to the system architecture and conduct risk analysis followed by risk evaluation and treatment.

8.4.1. Review System Architecture

To review the system architecture an organization needs to consider the following steps:

- Review the system architecture for compliance with security and privacy design principles. To review system architecture, organizations should take the following security and privacy design principles into consideration:
 - Identify whether each component of the application will interface externally or internally or both.
 - Identify how the user will access each component of the application and define the trust boundary.
 - Use least privilege principle while accessing and interfacing with any component.
 - Take the threats and vulnerabilities identified in the requirement analysis phase into consideration while designing the security and privacy requirements.
 - Identify the use of any third-party components and their security and privacy capabilities.
 - Keep the system architecture as simple as possible.
- Ensure that all security and privacy requirements identified in Section 8.3.2.6 are implemented.
- If any security and privacy requirements or design principles are not implemented, then implement the missing one and iterate the review process.

8.4.2. Risk Analysis

To conduct risk analysis at the system architecture phase, the following four steps need to be performed. Among these four tasks, identifying the threats and vulnerabilities can be performed in any order.

8.4.2.1. Identify and Document the Assets

To identify and document the assets in the system architecture conduct the following steps:

- Check whether any new asset is discovered compared to the list of assets identified during the requirement analysis phase in Section 8.3.1.1.
- Document the complete list of assets in the risk assessment report.

8.4.2.2. Identify and Document Threats

To identify and document the threats at the system architecture phase, the assessor team should conduct the following steps:

- Follow the steps outlined in Section 8.3.1.2.
- Document the complete list of threats in the risk assessment report.

8.4.2.3. Identify and Document the Vulnerabilities

To identify vulnerabilities at the system architecture phase, the assessor team should conduct the following steps:

- Apply threat modelling to identify vulnerabilities in a WBAN application. Section 6.3 outlines guidance on how to conduct threat modelling.
- Check if there are any additional vulnerabilities to those in the list of vulnerabilities identified during the requirements analysis phase in Section 8.3.1.3.
- If yes, then record the newly discovered vulnerabilities with possible countermeasures (if available) in the security assessment report.

8.4.2.4. Identify and Document the Adverse Impacts

To identify the adverse impact of newly discovered threats and vulnerabilities, the assessor team can reuse the questionnaire and process outlined in Section 8.3.1.4.

8.4.3. Risk Evaluation and Treatment

To evaluate and treat the risks identified at the system architecture phase, conduct the following steps:

- Follow the steps outlined in Sections 8.3.2.1 to 8.3.2.5.
- Identify the list of acceptable risks followed by unacceptable risks which require control to mitigate.
- Finally, document the updated product requirements, list the acceptable and unacceptable risks in the security and privacy risk assessment report.

8.4.4. Update Security and Privacy Requirements

Follow the steps outlined in Section 8.3.2.6 to develop the security and privacy requirements for the unacceptable risks which require security controls to mitigate. Update the product requirements with the updated security and privacy requirements. If the updated requirements require modifications to the system architecture, then conduct the following steps:

- Make necessary modifications to the system architecture.
- Iterate the security risk analysis and security evaluation with treatment process until the security requirements are addressed in the system architecture.

8.5. Security and Privacy Risk Assessment Report

The result of the security and privacy risk assessment needs to be documented in a report which will include the following:

- Scope of the security and privacy risk assessment.
- Team members who conducted the risk analysis, the risk evaluation and treatment with date.
- Initial product requirements.
- Selected risk assessment approach with rationale.
- List of assets identified in both phases.
- List of threats and vulnerabilities, along with impact and likelihood score that were identified in both phases.
- Risk acceptability criteria with rationale for both the requirements and system architecture phases.
- List of acceptable and unacceptable risks with rationale.
- List of unacceptable risks to be shared, avoided and which require controls to mitigate.
- List of security and privacy requirements identified at both the requirement analysis and the system architecture phases.

9. Security and Privacy Risk Controls

Security and privacy risk controls are safeguards or countermeasures whose purpose is to mitigate the threats and vulnerabilities. This stage will take a list of unacceptable risks which require controls to mitigate as the input and produce an application that has all the necessary risk controls implemented and verified. Figure 10 presents the steps for the selection and implementation of security and privacy risk controls.

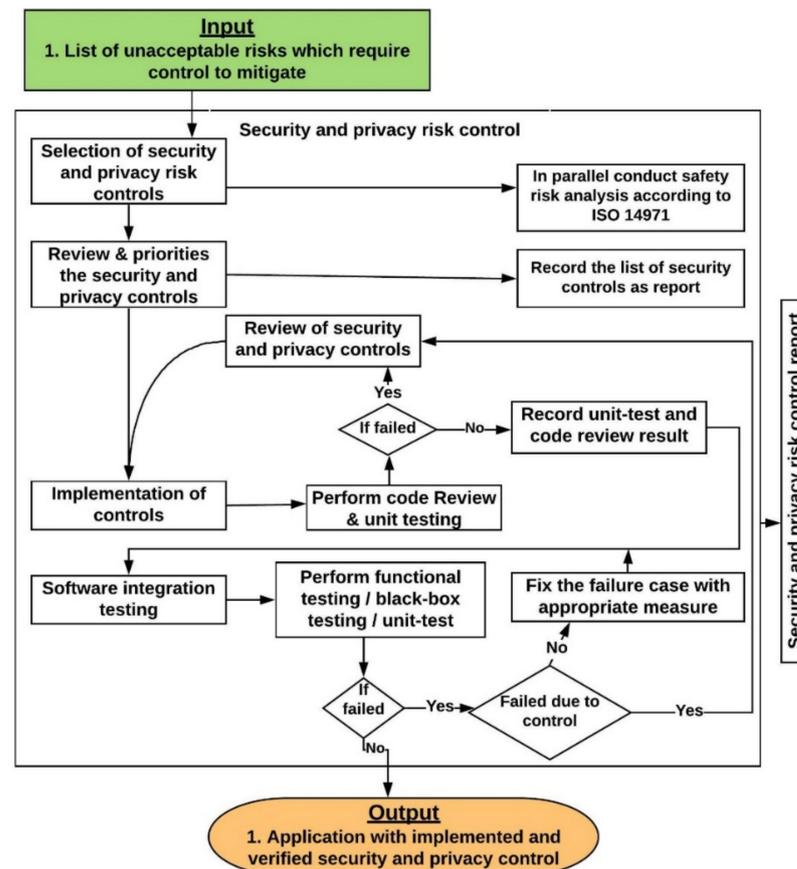


Figure 10. Selection and implementation process of security and privacy risk controls.

9.1. Review and Prioritise the Security and Privacy Risk Controls

After completing the security and privacy risk control selection process, the next task is to review the implementation details and prioritize the controls. The review and prioritization of the security and privacy risk controls should be conducted as follows:

- A team, comprised of a technical lead, a developer, and a QA person will review the implementation details presented in Appendix B for each control
- Prioritize the controls based on the following:
 - Risk score.
 - Product delivery plan and timeline of the project.
 - The priority of each use case.
 - Complexity, time required to implement the control.
- Document the list of controls, along with their implementation details and prioritization in the security and privacy risk control report.

9.2. Implementation and Verification of Security and Privacy Risk Controls

In the development phase, the developer will implement and verify each of the selected controls. During the implementation, developers should consider secure coding practices. The developer will use organization defined secure coding practices if available;

otherwise the developer can follow the secure coding guidelines provided below. Finally, to verify whether controls have been implemented properly, code review and unit testing should be conducted.

Secure coding guidelines:

- Validate input from all data sources.
- Compile code using the highest warning level and take necessary action to resolve the warnings.
- Use version control to track code changes.
- Sanitize the input to SQL statements. Use parameterized SQL statements. Do not use string concatenation or string replacement to build SQL statements.
- Use the latest version of compilers, which often include defences against coding errors; for example, GCC protects code from buffer overflows.
- Include proper error/exception handling. Check the return values of every function, especially security and privacy related functions.
- Encode HTML input field data. Do not store sensitive data in cookies.
- Use code review tools to find security and privacy issues early.

Code Review: Code review is an effective technique to examine the source code to minimize coding errors and reduce the risk of introducing vulnerabilities during the implementation phase. Secure coding guidelines also need to be considered during the code review process. Code review can be performed manually and/or by using an automated tool. To conduct a manual code review, organizations need to assign an experienced person from the development team. To conduct a code review using an automated tool, an organization needs to select the tool based on the technology stack. There are various automated code review tools available such as: SonarQube, IBM Security AppScan, Code Dx or Veracode which support a wider range of technology stacks.

Unit Testing: Unit testing is a testing method which helps to test an individual unit or component of an application. The goal of unit testing, from a security and privacy perspective, is to verify that each implemented control effectively mitigates its respective risk. Sample acceptance criteria for unit-tests are present in Table 11. The example below details the test to verify that the countermeasure for “*Weak Authentication Scheme*” is properly implemented.

Table 11. Sample acceptance criteria for unit testing.

Id	Test Case	Expected Result
Test01	Testing for valid user with right password	Successful authentication response
Test02	Testing for valid user with wrong password	Authentication failed due to the wrong password
Test03	Testing for a nonexistent username	Authentication failed due to invalid username
Test04	Testing authentication with blank passwords	Authentication failed due to empty password supplied
Test05	Attempt to log in with an incorrect password four times	Account locked out due to maximum try with the wrong password.

Sample use case: User login with username and password

Test objectives: Verify that the user authentication is aligned with business and security requirements

If the code review or unit test identifies any control failures, then the developer needs to conduct the following steps in order:

- Review the reason for the failure and take necessary action based on the scenario presented in Section 9.3.

- Conduct code review and/or unit test again to check whether the failure case is addressed.
- Finally, the result of the code review and the unit testing needs to be documented in the security risk control report with the updated list of controls (if any new control were added).

9.3. Review of Security and Privacy Controls

The aim at this stage is to present a list of reasons which can cause a control to fail. During the review, the following considerations need to be taken into account in order to identify the cause of the failure:

- The control was not properly implemented according to the implementation guidelines outlined in Appendix B. In that case the developer needs to implement the control again according to the implementation guidelines.
- Appropriate control was not selected for addressing the threats and/or vulnerabilities. If the appropriate control is not available in Appendix B, then analyze external sources such as NIST 800-53, ISO 27005, OWASP and blogs for appropriate control and implementation details.
- The developer did not follow appropriate secure coding practices during implementation.

9.4. Software Integration Testing

Software integration testing is a level of software testing where individual units are combined and tested as a group. Integration tests help to identify whether independently developed units of software work correctly when they are connected together. Integration testing can adopt different approaches, such as: Black Box Testing, White Box Testing and Gray Box Testing methods. During software integration testing, the developer needs to conduct two key tests:

- Security and privacy requirements testing—to validate the security and privacy requirements identified during the risk assessment are implemented properly by conducting functional, performance and scalability testing.
- Threat and vulnerabilities mitigating testing—to validate the effectiveness of the implemented controls against the identified threats and vulnerabilities. The following steps should be conducted at the software integration testing stage:
- Perform integration testing by conducting functional, unit-test, black-box, white box and gray box testing. Organizations can use one or a combination of multiple testing approaches to conduct the integration testing based on the QA resource expertise and availability.
- If an integration test fails, then check whether it failed due to a security risk control
 - If no, then take appropriate measures to fix the failure case and conduct the software integration test again.
 - If yes, then review based on considerations presented in Section 9.3 in order to identify the reason for failure and take appropriate measures to address the failure case and conduct the software integration test again.

10. Evaluation of Overall Residual Security and Privacy Risk Acceptability

Evaluating an application's overall residual security and privacy risk is a complex process as determining how an attacker will exploit the application and the severity level of the exploit, is difficult to assess. According to the TIR 57 standard, an organization can employ security testing techniques such as vulnerability scans and/or penetration testing to assess the overall residual security and privacy risk of an application. This stage will take the application with controls implemented and verified as input. Figure 11 presents the steps for evaluating the overall residual security and privacy risk of the application.

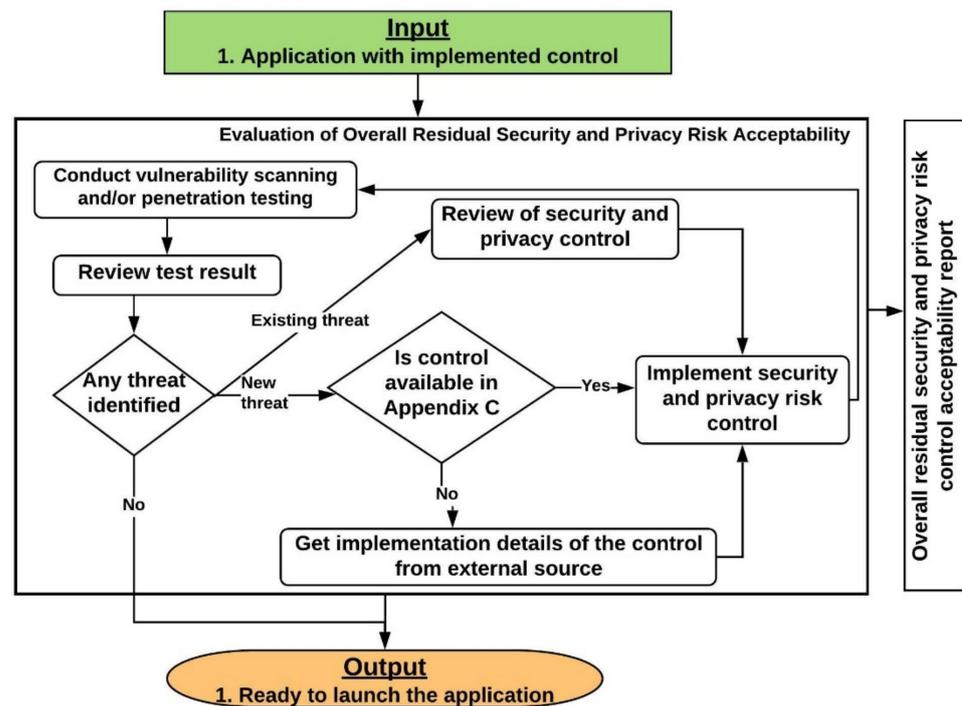


Figure 11. Steps for evaluating the overall residual security and privacy risk acceptability.

10.1. Conduct Vulnerability Scanning/Penetration Testing

Vulnerability scans and penetration testing are very different from each other, but both serve important functions for evaluating the implemented controls. A vulnerability scan only discovers known vulnerabilities; it does not attempt to exploit a vulnerability but instead only confirms the possible existence of a vulnerability. An organization can conduct vulnerability scanning using an automated tool with some manual support. Table A2 in Appendix C lists popular tools for vulnerability scanning. Penetration testing is a security testing approach which identifies exploitable vulnerabilities of a system, or of individual components of a system. Penetration testing requires specialized skills, higher budgets and more time than vulnerability scanning. An organization can conduct penetration testing by forming a team of people within the organization who have the technical expertise to and/or on-board external resources with the required expertise to conduct penetration testing. Table A3 in Appendix C lists some penetration testing tools. To conduct vulnerability scanning and/or penetration testing, an organization should conduct the following steps:

- Define the scope of the vulnerability scanning and/or penetration testing. The scope will include:
 - List of application use-cases.
 - List of assets.
 - List of threats and vulnerabilities for which countermeasures are implemented.
- Select the tools to be used to conduct the testing.
- Include external expertise (if required).
- Collect the results for review.
- Document the overall residual security and privacy risk acceptability in a report including:
 - Date of the testing.
 - Name of people/organization who performed the scanning and/or testing.
 - Scope of the testing.
 - List of tools used for conducting the testing.

10.2. Review Test Result

Passing a penetration test/vulnerability scan does not guarantee that the application is invulnerable, however it does mean that the application is at least invulnerable within the scope of the testing. If the testing is successful (i.e., did not record a fail), then the organization can mark the product for launch. If it fails, then the reason of the failure needs to be analyzed using the following steps:

- Check whether the threat is a new threat or existing threat which was identified during the security and privacy risk assessment steps.
- If the threat is an existing threat, then perform a review of the control based on the considerations presented in Section 9.3. to identify the reason for failure and take appropriate measures to address the failure case and mitigate the threat.
- If the threat is a new threat, then check whether the suggested control from scanning and/or testing report is available in Appendix B
 - If yes, then implement according to implementation details to mitigate the threat and add the selected control to the existing list.
 - If no, then collect implementation details from external sources such as: NIST 800-53, ISO 27005, OWASP, blogs, etc. Update the existing implementation details in Appendix B with the newly identified threat and respective control with implementation guidelines.
- Upon completion of the implementation of the controls, testing needs to be conducted again to verify that the control successfully mitigates the threat.
- Document the action taken to address each threat in the overall residual security and privacy risk acceptability report.

11. Discussion

The goal of this section is to present how the beta version of the framework addresses the challenges presented in Section 4, followed by a discussion on the threats to the validity of this study.

11.1. How the Proposed Framework Addresses the Challenges

Section 4 outlines the challenges faced by developers and organizations in adopting a risk management framework and standards for assuring security and privacy of WBAN applications.

- Lack of trained staff, responsibilities, budget, and management support—this framework consists of a list of assets, threats, vulnerabilities, and controls with implementation details which are specific to WBAN applications. The implementation of this framework requires minimal security expertise and will help to reduce development time, and thereby development cost.
- The existing standards are too complex and complicated to implement—this framework provides detailed guidance on how to conduct each step of the risk management process. This guidance should greatly assist developers with limited experience in implementing a risk management process.
- Limited knowledge about healthcare regulatory requirements and standards—the framework is based on recommendations and best practice guidelines provided by regulations such as HIPPA and GDPR, and by standards such ISO/IEC 80001-2-2, TIR 57, NIST 800-53 and ISO 27002.
- Understanding the data flow around the system and what assets need to be protected—the framework provide guidance on conducting security risk assessment at both the requirements analysis and the system architecture phases. This guidance will help the organization understand how data flows around the system and to identify the assets that need protection.
- Comprehensive understanding of the architecture for WBAN security and privacy—the framework outlines the possible assets, threats and vulnerabilities, and provides

guidelines on how to conduct the architecture review. Additionally, the framework identifies the security requirements that need to be considered during the development of the architecture of a WBAN application. This will help organizations to obtain a comprehensive understanding of WBAN architecture.

- Identifying appropriate security controls with respective implementation details—the framework provides appropriate security controls, along with their implementation details, for a WBAN application. The implementation details will assist a developer to implement the security controls.
- Due to a vast number of security controls, the challenge is prioritizing these controls in addition to planning releases without compromising security and privacy—the security risk score which is identified during the security risk evaluation and treatment stage can be used to prioritize the risk and respective security risk control.
- Security mechanisms for sensor device nodes—the framework suggests using very lightweight encryption and decryption processes. This framework recommends use of the AES symmetric cryptographic algorithm and the Diffie-Hellman process for key exchanges between mobile applications and sensor devices.

11.2. Threat to Validity

A threat to validity arises due to the fact that the alpha version of the framework has only been validated through implementation within one industrial setting. This also raises concerns around the generalisability of the framework to all WBAN development organizations. To address these concerns, we intend to have the framework undergo expert review, and to further trial the framework within other WBAN development organizations.

12. Conclusions and Future Work

Assuring security and privacy of PHR data are a key concern and challenging task faced by developers of WBAN applications. Developers have difficulties in assuring security and privacy of WBAN based healthcare applications for a number of reasons which include: lack of knowledge and complexity of the security and privacy standards; lack of understanding of what assets need to be protected in WBAN ecosystems; and difficulty with the identification of appropriate controls and lack of implementation details.

In this paper, we identified a number of healthcare-related risk management frameworks. However, these risk management frameworks were not directly applicable to WBAN applications because the primary objective of these frameworks is to manage the risk of applications which operate within a HDO's IT-network, whereas WBAN applications may operate in a public, open network using short-range communication media. Furthermore, these frameworks lack a process for selecting controls, lack implementation details for controls, and do not provide any guidance to assure security and privacy for resource constrained sensor devices.

This paper presents a risk management framework specifically for WBAN applications which addresses the challenges detailed above. The framework was developed in two stages, the alpha version and beta version. The beta version of the framework was developed by considering the suggestions and recommendations received after implementing the alpha version in an industrial setting. We have detailed how the framework addresses the difficulties developers face in assuring security and privacy of WBAN applications, and through implementing the framework within a WBAN development organization we have demonstrated the effectiveness of the security control implementation details provided within the framework.

Future work is to validate this framework through expert review.

Author Contributions: Conceptualization, P.C.P.; Methodology, P.C.P., J.L. and G.R.; Supervision, J.L., F.M. and G.R.; Writing—original draft, P.C.P.; Writing—review & editing, J.L. and G.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported with the financial support of the Science Foundation Ireland Grant No. 13/RC/2094_2 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero—the Science Foundation Ireland Research Centre for Software (www.lero.ie access on 30 July 2021).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

A non-exhaustive list of assets, possible threats, vulnerabilities and respective security controls for WBAN applications is presented in in Table A1.

Table A1. List of assets, threats, vulnerability and security controls for wban application.

Asset Name	Asset Sub-Category	Threat Name	Vulnerabilities	Security Controls
Operating system		Malware	Over-privileged users Over-privileged code Use of the same operating system	Malware protection
		Code injection	Input validation vulnerability	Input validation Output validation
Software libraries	Third-parties failures	Insecure ecosystem interfaces	Third-Party data distribution policy Monitoring and review of third-party services	
Application software	Command injection	Input validation vulnerability	Input validation	
	Repudiation attack	Access control vulnerability Logging and auditing vulnerability	Logging Access control Non-repudiation	
Device identity including location information	Attacks on privacy	Insecure data storage Insufficient privacy protection	Encryption Authorization Data anonymization	
	Data/Sensitive information leakage	Insecure data storage	Encryption Authorization Data anonymization	
Sensor Device	Data collected from the sensor device	Modification of information	Insecure communication Insecure data storage	Encryption Data integrity
		Replay attack	Lack of session management Insufficient cryptography	Session management Encryption
Device resources	Processing	Buffer overflow attack	Buffer overflow	Code review
		Denial of Service	Input validation vulnerability	Blocking brute force attacks Access control Session management
	Memory	Buffer overflow attack	Buffer overflow	Code review
	I/O	communication protocol hijacking	Insecure communication	Encryption Authentication
-	Masquerading attack	Lack of access control Insecure authorization Insufficient cryptography	Access control Authorization Encryption	
-	Physical attacks	Lack of physical hardening	Physical protection Client platform security	

Table A1. Cont.

Asset Name	Asset Sub-Category	Threat Name	Vulnerabilities	Security Controls	
Mobile App	-	Cryptanalysis	Insufficient cryptography	Encryption Cryptography Key management	
		Man-in-the-middle attack	Session management vulnerability Insecure communication	Authentication Input validation Session management Encryption	
		Web parameter tampering	Input validation vulnerability	Input validation	
		Session hijacking attack	Input validation vulnerability	Session management	
Web Application	-	Code injection	Input validation vulnerability	Input validation Output validation	
		Cross Site Scripting (XSS)	Improper data validation	Data validation	
		Cryptanalysis	Insufficient cryptography	Encryption Cryptography Key management	
		Man-in-the-middle attack	Session management vulnerability Insecure communication	Authentication Input validation Session management Encryption	
		Session hijacking attack	Input validation vulnerability	Session management	
Web Service	Application software	Modification of information	Insecure communication Insecure data storage	Encryption Data integrity	
		Brute force attack	Insufficient session-ID length	Authentication	
		SQL injection	Input validation vulnerability	Input validation	
		Replay attack	Lack of session management Insufficient cryptography	Session management Encryption	
	Processing	Denial of Service	Input validation vulnerability API abuse Lack of intrusion detection	Access control Session management Firewall	
		Command injection	Input validation vulnerability	Input validation	
	Memory	Buffer overflow attack	Buffer overflow	Code review	
	Server resources	I/O	Denial of Service	Input validation vulnerability API abuse Lack of intrusion detection	Access control Session management Firewall
			Replay attack	Lack of session management Insufficient cryptography	Session management Encryption
		Storage	Attacks on privacy	Insecure data storage Insufficient privacy protection	Encryption Authorization Data anonymization
Modification of information			Insecure communication Insecure data storage	Encryption Data integrity	
	Data/Sensitive information leakage	Insecure data storage	Encryption Authorization Data anonymization		
	Physical attacks	Lack of physical hardening	Physical protection Client platform security		

Table A1. Cont.

Asset Name	Asset Sub-Category	Threat Name	Vulnerabilities	Security Controls	
Database	Application software	Blind SQL injection	Input validation vulnerability	Input validation	
		SQL Injection	Input validation vulnerability	Query parameterization Input validation	
	Processing	Information or products from an unreliable source	Lack of access control Insecure authorization	Access control Authorization	
	Server resources	Memory	Denial of Service	Input validation vulnerability Lack of intrusion detection Database access abuse	Access control Session management Firewall
		I/O	Denial of Service	Input validation vulnerability Lack of intrusion detection Database access abuse	Access control Session management Firewall
		Storage	Data/Sensitive information leakage	Insecure data Storage Insecure communication	Encryption Authorization Data anonymization
	–	Physical attacks	Lack of physical hardening	Physical protection Client platform security	
	Wireless communication	–	Communication protocol hijacking	Insecure communication	Encryption Authentication
			Interception of information	Insecure communication	Encryption
			Eavesdropping	Insecure communication	Encryption
Man-in-the-middle attack		Session management vulnerability Insecure communication	Authentication Input validation Session management Encryption		
Masquerading attack		Lack of access control Insecure authorization Insufficient cryptography	Access control Authorization Encryption		
Sniffing attack		Insecure communication	Encryption		

Appendix B

Sample implementation guideline for security controls.

Appendix B.1. Auditing and Accountability

In WBAN applications, it is necessary to keep track of each activity performed by an authorized and/or unauthorized user. Auditing is the process which will keep track of different types of event including password changes; failed log-on, key management, query parameters and file access. This audit record can be used make a user accountable.

Source:

NIST 800-53 r5: AU-2, AU-3, AU-5, AU-6, AU-7, AU-8, AU-9, AU-5

ISO IEC 27002/ISO 27799: 12.4.1, 12.4.2

Guidelines:

- Define the list of parameters that will be captured as part of audit records and use a centralized platform to configure and manage these list of parameters (AU-3, 12.4.1)
 - user IDs.
 - system activities.
 - dates, times and details of key events, e.g., log-on and log-off.
 - device identity or location if possible and system identifier.
 - records of successful and rejected system and other resource access attempts.
 - changes to system configuration.
 - use of privileges.
 - use of system utilities and applications.

- files accessed and the kind of access.
- network addresses and protocols.
- alarms raised by the access control system.
- activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.
- records of transactions executed by users in applications.
- Limit the capturing of PHI and/or PHR data in audit records to minimize the privacy risk. If required anonymize the PHI and/or PHR data records before capturing in the audit log (AU-3, 12.4.1).
- Provide a warning to respective roles or owner within an organization when allocated audit record storage volume reaches the maximum audit record storage capacity (AU-5, 12.4.2).
- Provide a real-time alert if the system failed to capture audit record in a time-period (AU-5).
- Implement an automated process to review and analysis the audit log which followed by generating report. Use this report to investigation and response to suspicious activities (AU-6).
- Implement the capability to sort and search audit records for an event based on the content fields of audit records (AU-7).
- Use internal system clocks to generate the timestamp for audit records (AU-8).
- Implement cryptographic mechanisms to protect the integrity of audit records and ensure only authorized users obtain access to these audit records. If required, create an authorized user with read-only permission to audit record (AU-9).
- Initiate session audits including automatically file transfer, user request/response at the system start-up (AU-14).

Appendix B.2. Key Management

Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms. NIST 800-53 propose to use NIST FIPS-compliant or NSA-approved key management technology to produce, control and distribute symmetric cryptographic keys. In this study ISO/IEC 1170 and NIST 800-56A key management guidelines are used for key generation, control and distribution.

Source:

NIST 800-53 r5: AU-2, AU-3, AU-5, AU-6, AU-7, AU-8, AU-9, AU-5

ISO IEC 27002/ISO 27799: 12.4.1, 12.4.2

Guidelines:

- A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle (NIST 800-53 SC-12, ISO 27002 10.1.2).
- Create keys with appropriate key size and block size. Do not use a laptop or random application to generate the key. Only generate the key using any application or service provider which supports hardware security modules (HSMs) (ISO/IEC 11770).
- Do not use any random cryptographic algorithms. Select only which are recognized by different standards. For example, AES is currently recognized by the Federal Government standard body for symmetric techniques (NIST 800-175B).
- Consider the proper key size during cryptographic algorithms. For AES 128, 168 or 256-bits key size can be used (NIST 800-175B).
- Generated keys need to be distributed securely by keeping confidentiality and integrity (ISO/IEC 11770).
- Use key wrapping techniques to exchange the key between mobile applications and devices. Diffie-Hellman provides the capability for two parties to agree upon a shared secret for exchanging keys over a public channel (NIST 800-56A).
- If any user and/or device is identified as compromised, the respective key of the user or device needs to be removed from the application and key management server. After

the revocation of a compromised key, a new key needs to be generated and distributed using the above steps (ISO/IEC 11770).

- Log each activity related to key management and use this data to perform auditing (ISO 27002 10.1.2).

Appendix C

List of tools for vulnerability scanning and penetration testing.

Table A2. List of tools for vulnerability scanning.

Name	Description	License	Source
OpenVAS	OpenVAS Scanner is a vulnerability assessment tool that is used to spot issues related to security in the servers and other devices of the network.	GNU General Public License	https://www.openvas.org/ (access on 30 July 2021)
Nikto	Nikto is an open-source web scanner employed for assessing the probable issues and vulnerabilities on web servers.	GNU General Public License	https://cirt.net/Nikto2 (access on 30 July 2021)
Tripwire IP360	Tripwire IP360 is a vulnerability assessment solution to run wide-ranging of testing on the networks to spot all the vulnerabilities, configurations, applications, network hosts.	Commercial	https://www.tripwire.com/products/tripwire-ip360 (access on 30 July 2021)
Wireshark	Wireshark is an extensively used as network protocol analyzer tool.	GNU General Public License	https://www.wireshark.org/ (access on 30 July 2021)
Aircrack	Aircrack is a tool to assess the WiFi network security.	GNU General Public License	https://www.aircrack-ng.org/ (access on 30 July 2021)

Table A3. List of tools for penetration testing.

Name	Description	License	Source
Apache ab test	Apache ab load test tool uses to generate the number of request per second. This tool very useful to perform load testing and DDOS attack scenario.	GNU General Public License	https://httpd.apache.org/docs/2.4/programs/ab.html (access on 30 July 2021)
OWASP ZAP	The Open Web Application Security Project—Zed Attack Proxy (ZAP) is a penetration testing tool for finding vulnerabilities in applications.	GNU General Public License	https://owasp.org/www-project-zap/ (access on 30 July 2021)
BURP SUITE	Burp Suite is a platform for performing security testing of applications.	Commercial	https://portswigger.net/burp (access on 30 July 2021)
NMAP	Nmap (Network Mapper) is a free and open-source utility for network exploration or security auditing.	GNU General Public License	https://nmap.org/ (access on 30 July 2021)
SSLSCAN	SSLScan tests for different SSL exploits, such as heartbleed and the POODLE vulnerability, it also tests the cipher suites and key exchanges.	GNU General Public License	https://github.com/rbsec/sslscan (access on 30 July 2021)
HYDRA brute force	Hydra is a rapid dictionary attacker which can be configured against over 50 different protocols. It is most commonly used for brute-forcing user accounts to test for weak passwords.	GNU General Public License	https://github.com/vanhauser-thc/thc-hydra (access on 30 July 2021)
KALI LINUX	Kali is a Debian-derived Linux distribution designed for digital forensics and penetration testing installed with hundreds of different tools.	GNU General Public License	https://www.kali.org/ (access on 30 July 2021)

References

1. Ullah, S.; Higgins, H.; Braem, B.; Latre, B.; Blondia, C.; Moerman, I.; Saleem, S.; Rahman, Z.; Kwak, K.S. A comprehensive survey of wireless body area networks on PHY, MAC, and network layers solutions. *J. Med. Syst.* **2012**, *36*, 1065–1094. [CrossRef] [PubMed]
2. Antonescu, B.; Basagni, S. Wireless body area networks: Challenges, trends and emerging technologies. In Proceedings of the 8th International Conference on Body Area Networks, Boston, MA, USA, 30 September–2 October 2013; pp. 1–7.
3. Salayma, M.; Al-dubai, A.; Romdhani, I. Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence. *ACM Comput. Surv.* **2017**, *50*, 1–38. [CrossRef]
4. Kotz, D. A threat taxonomy for mHealth privacy. In Proceedings of the 3rd International Conference on Communication Systems and Networks, COMSNETS, Bangalore, India, 4–8 January 2011; pp. 1–6.
5. Li, M.; Lou, W.; Ren, K. Data security and privacy in wireless body area networks. *IEEE Wirel. Commun.* **2010**, *17*, 51–58. [CrossRef]
6. Paul, P.C.; Loane, J.; McCaffery, F.; Regan, G. A data security and privacy risk management framework for wban based healthcare applications*. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Kassel, Germany, 22–26 March 2021; pp. 704–710.
7. Ramli, S.N.; Ahmad, R. Surveying the wireless body area network in the realm of wireless communication. In Proceedings of the 7th International Conference on Information Assurance and Security (IAS), Melacca, Malaysia, 5–8 December 2011; pp. 58–61.
8. Paul, P.C.; Loane, J.; Regan, G.; McCaffery, F. Analysis of Attacks and Security Requirements for Wireless Body Area Networks-A Systematic Literature Review. In Proceedings of the European Conference on Software Process Improvement, Edinburgh, UK, 18–20 September 2019; pp. 439–452.
9. FDA Overview of Device Regulation. Available online: <https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation> (accessed on 9 November 2020).
10. CFR Electronic Code of Federal Regulations. Available online: https://www.ecfr.gov/cgi-bin/text-idx?SID=ba90ee4a08a5ba017a34366276d68234&mc=true&tpl=/ecfrbrowse/Title21/21cfrv8_02.tpl#0 (accessed on 13 October 2020).
11. HIPAA Security Rule. Available online: <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (accessed on 10 October 2020).
12. EU Commission Medical Device Regulation. Available online: <https://eur-lex.europa.eu/eli/reg/2017/745/2017-05-05> (accessed on 13 October 2020).
13. EU Commission General Data Protection Regulation. Available online: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (accessed on 13 October 2020).
14. FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Available online: <https://www.fda.gov/media/119933/download> (accessed on 13 October 2020).
15. FDA Postmarket Management of Cybersecurity in Medical Devices. Available online: <https://www.fda.gov/media/95862/download> (accessed on 13 October 2020).
16. IEC 62304. *Health Software—Software Life Cycle Processes*; ISO: Geneva, Switzerland, 2019.
17. NIST SP800-53. *Security and Privacy Controls for Federal Information Systems and Organizations*; NIST: Gaithersburg, MD, USA, 2020.
18. ISO/IEC 27002. *Information Technology—Security Techniques—Code of Practice for Information Security Controls*; ISO: Geneva, Switzerland, 2017.
19. IEC 80001-1. *Application of Risk Management for IT-Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities and Activities*; ISO: Geneva, Switzerland, 2015.
20. IEC 80001-2-2. *Application of Risk Management for IT-Networks Incorporating Medical Devices—Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Control*; ISO: Geneva, Switzerland, 2011.
21. AAMI TIR57. *Principles for Medical Device Security—Risk Management*; AAMI: Bronson, VA, USA, 2016.
22. ISO 14971. *Medical Devices—Application of Risk Management to Medical Devices*; ISO: Geneva, Switzerland, 2018.
23. NIST:800-30. *Guide for Conducting Risk Assessments*; NIST: Gaithersburg, MD, USA, 2012.
24. Duc, A.N.; Jabangwe, R.; Paul, P.; Abrahamsson, P. Security challenges in IoT development: A software engineering perspective. In Proceedings of the XP2017 Scientific Workshops, Cologne, Germany, 22–26 May 2017; pp. 1–5.
25. Townsend, K. Organizations Challenged with Cybersecurity Framework Implementation. Available online: <https://www.securityweek.com/organizations-challenged-cybersecurity-framework-implementation> (accessed on 10 October 2020).
26. Holden, W.L. Bridging the culture gap between healthcare IT and medical device development. *Biomed. Instrum. Technol.* **2014**, *48*, 22–28. [CrossRef] [PubMed]
27. MacMahon, S.T.; Cooper, T.; McCaffery, F. Revising IEC 80001-1: Risk management of health information technology systems. *Comput. Stand. Interfaces* **2018**, *60*, 67–72. [CrossRef]
28. Chen, Q.; Lambright, J.; Abdelwahed, S. Towards Autonomic Security Management of Healthcare Information Systems. In Proceedings of the 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Washington, DC, USA, 27–29 June 2016; pp. 113–118.
29. Shah, S.M.; Khan, R.A. Secondary use of electronic health record: Opportunities and challenges. *IEEE Access* **2020**, *8*, 136947–136965. [CrossRef]

30. Eom, D.; Lee, H. A holistic approach to exploring the divided standards landscape in E-Health research. In Proceedings of the 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), Nanjing, China, 27–29 November 2017; pp. 1–7.
31. Benz, M.; Chatterjee, D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus. Horiz.* **2020**, *63*, 531–540. [[CrossRef](#)]
32. Chen, J.Q.; Benusa, A. HIPAA security compliance challenges: The case for small healthcare providers. *Int. J. Healthc. Manag.* **2017**, *10*, 135–146. [[CrossRef](#)]
33. Mariani, D.M.R.; Mohammed, S. Cybersecurity challenges and compliance issues within the US healthcare sector. *Int. J. Bus. Soc. Res.* **2015**, *5*, 55–66.
34. Ključnikov, A.; Mura, L.; Sklenár, D. Information security management in SMEs: Factors of success. *Entrep. Sustain. Issues* **2019**, *6*, 2081. [[CrossRef](#)]
35. Aljohani, M.; Blustein, J. A study using the in-depth interview approach to understand current practices in the management of personal health information and privacy compliance. In Proceedings of the 2018 IEEE International Conference on Healthcare Informatics (ICHI), New York, NY, USA, 4–7 June 2018; pp. 75–86.
36. Skierka, I.M. The governance of safety and security risks in connected healthcare. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018; pp. 1–12.
37. Thapa, C.; Camtepe, S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Comput. Biol. Med.* **2021**, *129*, 104130. [[CrossRef](#)] [[PubMed](#)]
38. Supriya, S.; Padaki, S. Data Security and Privacy Challenges in Adopting Solutions for IOT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 410–415.
39. Stevovic, J.; Casati, F.; Farraj, B.; Li, J.; Motahari-Nezhad, H.R.; Armellin, G. Compliance aware cross-organization medical record sharing. In Proceedings of the 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), Ghent, Belgium, 27–31 May 2013; pp. 772–775.
40. Abraham, C.; Chatterjee, D.; Sims, R.R. Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Bus. Horiz.* **2019**, *62*, 539–548. [[CrossRef](#)]
41. Aceto, G.; Persico, V.; Pescapé, A. The role of Information and Communication Technologies in healthcare: Taxonomies, perspectives, and challenges. *J. Netw. Comput. Appl.* **2018**, *107*, 125–154. [[CrossRef](#)]
42. Iyengar, A.; Kundu, A.; Pallis, G. Healthcare informatics and privacy. *IEEE Internet Comput.* **2018**, *22*, 29–31. [[CrossRef](#)]
43. Paquette, A.; Painter, F.; Jackson, J.L. Management and risk assessment of wireless medical devices in the hospital. *Biomed. Instrum. Technol.* **2011**, *45*, 243–248. [[CrossRef](#)] [[PubMed](#)]
44. ISO/IEC 80001-2-8. *Application of Risk Management for IT-Networks Incorporating Medical Devices Part 2-8: Application Guidance—Guidance on Standards for Establishing the Security Capabilities Identified in IEC TR 80001-2-2*; ISO: Geneva, Switzerland, 2016.
45. ISO 27799:2008. *Health Informatics—Information Security Management in Health Using ISO/IEC 27002*; ISO: Geneva, Switzerland, 2016.
46. ISO 11770. *BS ISO/IEC 11770-2:2018 IT Security Techniques. Key Management. Mechanisms Using Symmetric Techniques*; ISO: Geneva, Switzerland, 2018.
47. NIST NVD—CVSS v3 Calculator. Available online: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator> (accessed on 19 August 2020).