
UNIVERSITA' POLITECNICA DELLE MARCHE

Faculty of Engineering

Department of Information Engineering
Master of Science in Biomedical Engineering

# CYBER RISK ASSESSMENT TOOLS FOR MEDICAL NETWORKS AND DEVICES

**Supervisor**:

*Prof. Marco Baldi*

**Candidate**:

*Marco Brandozzi*

**Co-supervisor**:

*Prof. Franco Chiaraluce*

*Academic Year 2019/2020*

# Abstract

The interoperability of medical devices and their incorporation onto IT networks are becoming even more pervasive. This coupled with the increase in cyber-attacks on the IT-Networks incorporating medical devices of the Health Delivery Organizations, make the risks to patient safety and data and system security an issue to be considered within the responsible organization risk management process along the whole life cycle of a medical device. In this context, IEC 80001-1, ISO/TR 80001-2-2 and European Regulation n. 745/2017 represent the main cybersecurity normative framework which manufacturers of medical devices have to comply with. The aim of this work is to provide a tool that can be used by manufacturers to evaluate if their medical devices, intended to be incorporated into a medical IT network, conform to the cybersecurity European regulation and most relevant technical standards requirements focused, in particular, on the patient safety. The tool consists of an excel check list that enables the user to verify if the basic risk controls processes and measures have been applied and if the overall risk management approach have been correctly implemented.

The tool has been tested in a company developing medical device software for healthcare organizations, BiMind srl. The analysis of results showed that the medical device software concerned is secure as expected, but the tool also highlighted that some process and product security aspects have to be improved in order to further reduce the cybersecurity risks.

Nowadays, the patient safety and data and system security results to be critical. However, despite its relevance the topic is not homogeneously regulated today. For this reason a tool concerning the compliance assessment it would be helpful to manufacturers for ensuring an acceptable level of cybersecurity for a medical device integrated in IT-network.

# *List of Contents*

# *List of Figures*

# *List of Tables*

# 1 Introduction

## 1.1 Background

At the beginning, medical devices (MDs) were designed as stand-alone devices and placed in a IT network provided and maintained by the Medical Device Manufacturers (MDMs) when required to be networked (e.g. Physiological Monitors in an Intensive Care Unit) [1].

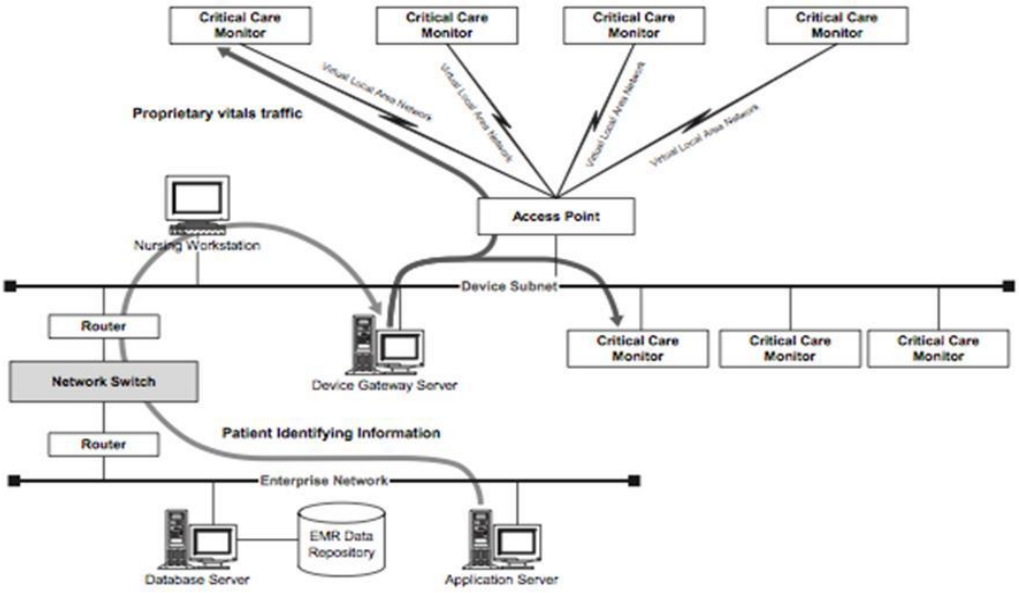


**Figure 1. Physiological Monitoring Proprietary Network [1]**

Over the last couple of decades, we have assisted to a transformation of the IT architecture in Health Delivery Organizations (HDOs) which makes all their IT

systems, applications and medical devices grouped on one single infrastructure utilizing a common network.

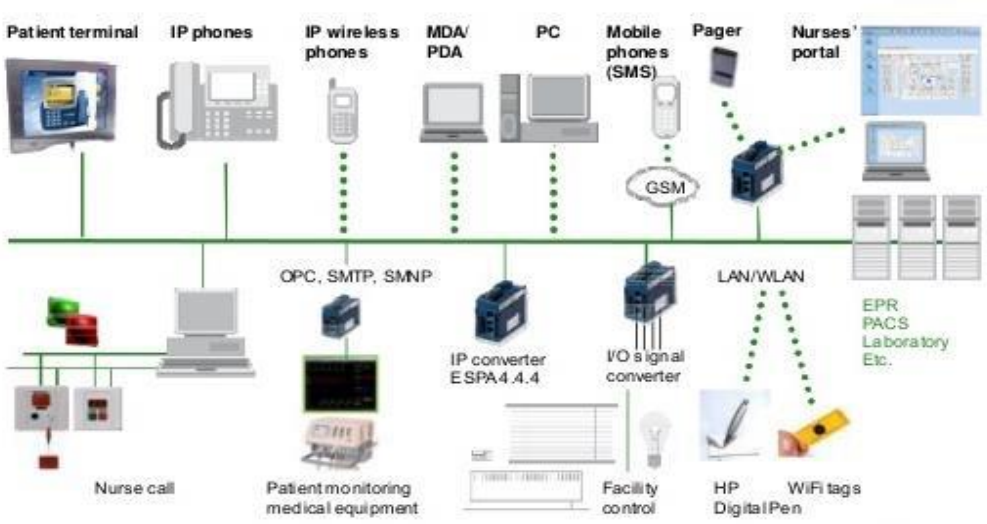


**Figure 2. HDO Single Heterogeneous Network [2]**

This IT-network concept can be very efficient as it ensures that the right information is available to the right person, where and when they need it [3]. Furthermore, results in a reduction of adverse events, leading to improved patient safety.

However, the complexity of the integration of interoperable medical devices and systems onto heterogeneous network combined with their crucial role in the delivery of care to the patient, introduces new unintended consequences which are outside of the control of the MDMs and introduce risks that need to be identified and managed [4].

## 1.2 Medical Devices

The International Electrotechnical Commission (IEC) defines medical device as any instrument, apparatus, implement, machine, appliance, implant, *in vitro* reagent or calibrator, software, material or other similar or related article:

a) intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of:
   - diagnosis, prevention, monitoring, treatment or alleviation of disease,
   - diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
   - investigation, replacement, modification, or support of the anatomy or of a physiological process,
   - supporting or sustaining life,
   - control of conception,
   - disinfection of medical devices,
   - providing information for medical or diagnostic purposes by means of in vitro
   - examination of specimens derived from the human body; and
b) which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means [5].

MDs have evolved from standalone analogue-computer technology to digitalized medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. This evolution requires manufacturers to develop and manufacture their products in accordance with the state of the art taking into account the principles of risk management, including information

security, as well as to set out minimum requirements concerning IT security measures [6].

## 1.3 Medical IT-Network

Patient monitoring systems were initially installed on stand-alone networks with dedicated infrastructure isolating the monitors on their own network. Many of these monitoring applications have been installed over time in different departments within the HDO, each with its own dedicated infrastructure. Gateways have been introduced which allow data exchange between the monitoring systems and hospital administration systems. A 2010 report stated that the simplification of the IT architecture is necessary if HDO want to integrate information from medical devices and computerized physician order entry systems into an electronic health record (EHR) [7].

An IT-network is defined by IEC as a system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes**.** When a medical device is connected onto a IT-network that network then becomes a medical IT-network**.**

Increasingly, electronic medical devices are being connected to each other and to other technologies and information is exchanged and shared between these devices. The effective interconnectivity of various medical devices and systems is dependent on the secure transfer and use of information. This interconnectivity of medical devices and systems is called “interoperability” and has the potential to

promote innovation and facilitate new methods and models of healthcare delivery, resulting in increased efficiency and outcomes in patient care. These shared networks facilitate the transfer of information between interoperable medical devices and their related systems while also allowing the transfer of video, telephone and data communication. The purpose of these heterogeneous networks is to ensure that the right information is available to the right person, where and when they need it. The interoperability of medical devices sharing a common network improves medical device capabilities and ease of use however it also adds complexity and therefore increases risk**.**

## 1.4 Patient Safety and Risk

The World Health Organization (WHO) defines patient safety as the "prevention of errors and adverse effects to patients associated with health care"**,** and statistics from the WHO indicate that approx. 43 million patient safety incidences occur every year equating to 1 in every 10 patients being affected.
Communication failures between physicians, resulting in poor information relating to the clinical condition of a patient being communicated, is one of the most common factors contributing to adverse events. The authors also suggests that the correct use of information technology can improve patient safety by improved communications and the availability of clinical decision support based on real time patient data from connected medical devices.

In relation to medical networks risk is defined as a combination of the probability of occurrence of harm and the severity of that harm.

As a result of this technological advancement and interconnectivity, medical devices have become vulnerable to international cyber threats allowing unauthorized access enabling change of settings and loss of data. Some statistics of Italian Cybersecurity Italian organizations show that in 2019, compared to 2018, the number of the most significant attacks in Italy in the healthcare sector increased by 17%, accounting for the third place in the rank with a remarkable increasing trend over the past six years [8] (Figures 3 and 4).

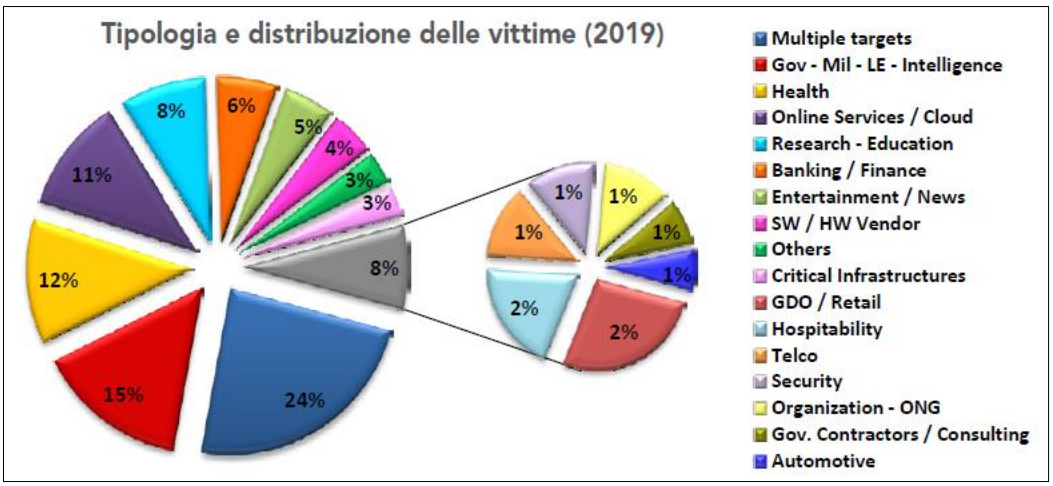


**Figure 3. Type and distribution of attacked sectors [8]**

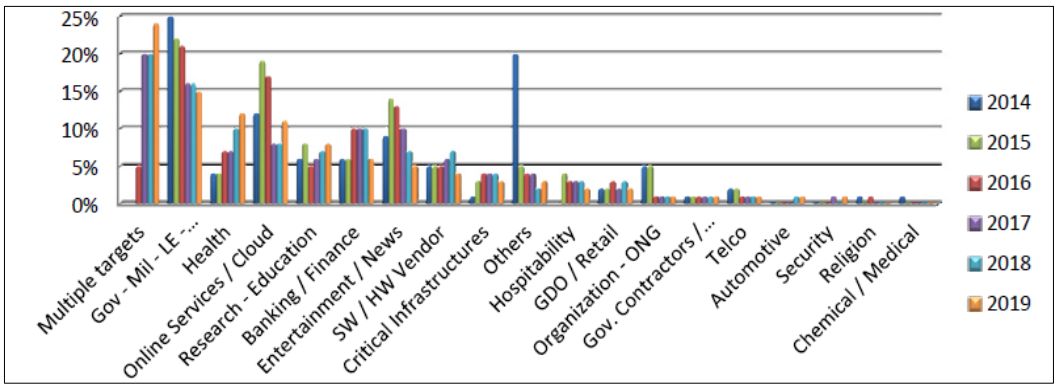


**Figure 4. % distribution of attacked sectors [8]**

The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet, and network-connected devices. Cybersecurity incidents have rendered medical devices and healthcare companies networks inoperable, disrupting the delivery of patient care across healthcare facilities. Such incidents may lead to patient harm through delays and/or errors in diagnoses and/or treatment interventions, etc. Thus, stakeholders within the healthcare sector have a shared responsibility to mitigate those risks compromising the Safety, Effectiveness and the data and system Security of the IT-network.

# 2 Medical devices cybersecurity regulation

Convergence of global healthcare cybersecurity efforts is necessary to ensure that patient safety is maintained while encouraging innovation and allowing timely patient access to safe and effective medical devices. All stakeholders are encouraged to harmonize their approaches to cybersecurity across the entire life cycle of the medical device [9]. To date, however, disparate regulations across many governments lack the global alignment needed to ensure medical device cybersecurity.

## 2.1 European Regulation

Within the European Union medical devices are governed by the Medical Device Directive MDD 93/42/EEC including Directive 2007/47/EC which outlines essential requirements on safety, performance and labelling that all medical devices must adhere to. Furthermore, the recent Regulation n. 2017/745/EC (MDR) makes mandatory the adoption of cybersecurity risk control measures included in the Annex I [10]. They require manufacturers to develop and manufacture their products in accordance with the state of the art taking into account the principles of risk management, including information security, as well as to set out minimum requirements concerning IT security measures, including protection against unauthorized access. These requirements, and their interconnection, are illustrated in Figure 5:

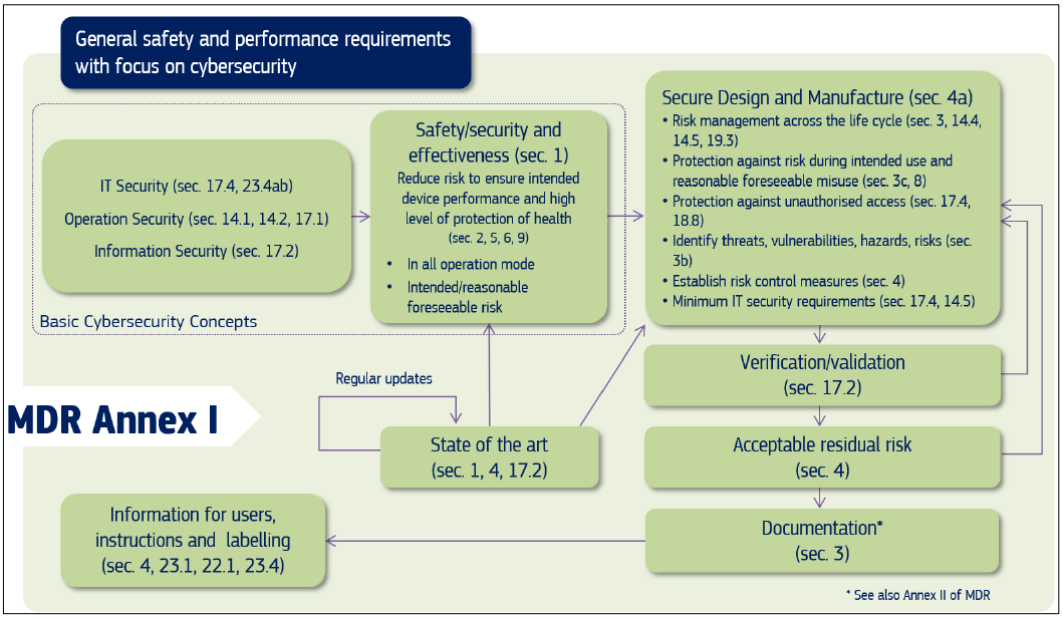


**Figure 5. Cybersecurity requirements contained in MDR Annex I [6]**

With regards to cybersecurity, the aim of the MDR requirements is that the characteristics of **Confidentiality, Integrity** and **Availability** (CIA) of information assets (data and system) are duly protected against the risk of theft, deletion and alteration. However, medical devices must be also developed and manufactured in such a way they are **safe and effective** and not compromise the clinical condition or the safety of patients. To this end, the relationship between "safety and security" must be considered as they relate to risk, as illustrated below in Figure 6.


**Figure 6. Cybersecurity measures may cause safety impacts [6]**

It is crucial to balance safety and security and when the manufacturer fits the medical device with cybersecurity controls and mitigations, the device safety must be maintained.

To effectively manage the development of the cybersecurity risks MDR requires the medical device manufacturer to apply a risk management process throughout all product phases including but not limited to design, manufacturing, testing and post-market monitoring activities (Total Product Life Cycle – TPLC). In fact, addressing cybersecurity risks at the design stage can help mitigate cybersecurity risks that could contribute to a breach in the confidentiality, a compromise in the integrity and availability of the medical device and its data. However, emerging security vulnerabilities or new attack methods may lead to the situation that a medical device became lately unsecure and possibly unsafe. Thus, during the medical device lifetime, manufacturers should take into account adverse events such as security incidents and vulnerabilities directly related to medical device and changes in the threat landscape, including interoperability aspects.

Consequently, they have to apply appropriate measures to control the new risks including, but not limited to, information to operators of medical devices on the

identified risk, network configuration changes, software updates and 3rd party software updates or patches. The following table gives an overview of the risk management processes requested by the MDR [6]:

**Table 1. Cybersecurity activities across the life cycle of medical devices according to the MDR [6]**

| Pre-market activities | Post-market activities |
|---|---|
| Secure Design (Annex I) | |
| Risk management (Annex I) | Risk management (Annex I) |
| Establish Risk Control Measures (Annex I) | Modify Risk Control Measures /Corrective Actions/Patches (Annex I) |
| Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I) | Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I) |
| Technical Documentation (Annex II and III) | Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84) |
| Conformity Assessment (Article 52) | Trend Reporting (Article 88) |
| Establish a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84) | Analysis of Serious Incidents (Article 89) |
| Clinical evaluation process (Chapter VI) | Post-Market Surveillance Report (Article 85) |
| | Periodic Safety Update Report (Article 86) |
| | Update Technical Documentation (Annex II and III) |
| | Inform the Electronic System On Vigilance (Article 92) |

## 2.2 ISO/IEC 80001 Series

With the development of medical devices and the introduction of medical devices integrated in an IT-network, there were numerous unwanted events related to this

new type of medical devices, as reported by Food and Drug Administration (FDA) in 2009. For this reason, in 2010, the International Standard Organization (ISO) published the standard 80001-1 to help HDO in adopting an effective Risk Management to prevent and limit adverse phenomena. Since the publication of IEC 80001-1, a number of technical reports have been published to address specific aspects and assist the individuals responsible for the different aspects of medical device integration into IT networks in the implementation of the standard. These are as shown in Table 2 below.

**Table 2. IEC 80001-1 Technical Reports**

| Name | Description | Published |
|---|---|---|
| IEC/TR 80001-2-1 | Application of risk management for IT-networks incorporating medical devices -- Part 2-1: Step by Step Risk Management (ISO/IEC, 2012a). | 2012 |
| IEC/TR 80001-2-2 | Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls (ISO/IEC, 2012b). | 2012 |
| IEC/TR 80001-2-3 | Application of risk management for IT-networks incorporating medical devices -- Part 2-3: Guidance for wireless networks(ISO/IEC, 2012c). | 2012 |
| IEC/TR 80001-2-4 | Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations (ISO/IEC, 2013b). | 2013 |
| IEC/TR 80001-2-5 | Application of risk management for IT-networks incorporating medical devices -- Part 2-5: Application guidance -Guidance for distributed alarm systems (ISO/IEC, 2014a). | 2014 |
| IEC/TR 80001-2-6 | Application of risk management for IT-networks incorporating medical devices Part 2-6: Application guidance — Guidance for responsibility agreements (ISO/IEC, 2014b). | 2014 |
| ISO/TR 80001-2-7 | Application of risk management for IT-networks incorporating medical devices Part 2-7: Application guidance -- Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1 (ISO/IEC, 2015a). | 2015 |
| IEC/TR 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 80001-2-2 (ISO/IEC, 2016). | 2016 |

This study mainly focuses on the following standards which contain requirements of interest to medical device manufacturer:

1. IEC 80001-1:2010 “Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities”;
2. IEC/TR 80001-2-2:2012 “Application of risk management for IT-networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls”;
3. IEC/TR 80001-2-5:2014 “Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance - Guidance for distributed alarm system”;
4. IEC/TR 80001-2-8:2016 “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”.

The above mentioned standard are supposed to represent, with together others, the current state of-the-art requested by the MDR.

### 2.2.1 IEC 80001-1:2010

In 2010 the IEC released the standard 80001-1 that address the risks associated with medical devices sharing a common IT network with other devices and applications**.**

The goal of IEC 80001-1 is to prevent patient harm and three key properties are identified:

- **Safety**: freedom from unacceptable risk of physical injury or damage to the health of patient or user.

- **Effectiveness**: ability to produce the intended result for the patient and the responsible organization.
- **Security**: operational state of a medical IT-network in which information assets (data and systems) are reasonably protected from degradation of confidentiality, integrity, and availability.

The standard defines roles, responsibilities and activities in relation to the management of risk associated with placing a medical device onto an IT network for healthcare organizations, medical device manufacturer and other providers of IT equipment on the network.

Concerning medical device manufacturer, the standard establishes that, for medical devices connected to an IT-Network, shall be made available instructions for implementing such connection, which include, among other:

- The purposes of the medical device's connection to an IT-Network;
- The required characteristics and configuration of the IT-Network incorporating the medical device;
- The security specification of the network connection of the medical device;
- The intended information flow between the medical devices and the medical IT-Network and, if relevant for the key properties, the intended routing through the medical IT-network;
- A list of the hazardous situation resulting from a failure of the IT-network to provide the characteristics required to meet the purpose of the medical device connection to the IT-network [5].

ISO 80001-1 requires risk management to be performed on medical IT-networks. The risk management activities required by this standard are based largely on those of ISO 14971, but go beyond Safety as defined in ISO 14971 to include

managing risk to Effectiveness and to data and system Security. The Table 4 shows the interconnections between the two risk management systems:

**Table 3. Relationship between IEC 80001-1 and ISO 14971:2007 [5]**

| ISO 14971:2007 section | | IEC 80001-1 section | |
|---|---|---|---|
| 4 | **RISK ANALYSIS** | | |
| 4.1 | RISK ANALYSIS PROCESS | n/a | |
| 4.2 | INTENDED USE and identification of characteristics related to SAFETY | | |
| 4.3 | Identification of HAZARDS | 4.4.2 | **RISK ANALYSIS** |
| 4.4 | Estimation of the RISK(S) for each hazardous situation<br>– "Reasonably foreseeable sequences or combinations of events that can result in a hazardous situation shall be considered and the resulting hazardous situation(s) shall be recorded"<br>– "For each identified hazardous situation, the associated RISK(S) shall be estimated" | 4.4.2 | "For each identified HAZARD, the RESPONSIBLE ORGANIZATION shall estimate the associated RISKS..." |
| 5 | **RISK EVALUATION** | 4.4.3 | **RISK EVALUATION** |
| 6 | **RISK CONTROL** | 4.4.4 | **RISK CONTROL** |
| 6.1 | RISK reduction | n/a | |
| 6.2 | RISK CONTROL option analysis | 4.4.4.1 | RISK CONTROL option analysis |
| | | 4.4.4.2 | RISK CONTROL measures |
| 6.3 | Implementation of RISK CONTROL measures | 4.4.4.3 | Implementation of RISK CONTROL measures |
| | | 4.4.4.4 | VERIFICATION of RISK CONTROL measures |
| 6.4 | RESIDUAL RISK evaluation | | (addressed in 4.4.4.1) |
| 6.5 | RISK/benefit analysis | | (addressed in both 4.4.4.1 and 4.4.5) |
| 6.6 | RISKS arising from RISK CONTROL measures | 4.4.4.5 | New RISKS arising from RISK CONTROL |
| 7 | **Evaluation of overall RESIDUAL RISK acceptability** | 4.4.5 | **RESIDUAL RISK evaluation and reporting** |

Thus, for the purpose of an effective cyber risk mitigation it's crucial a close cooperation between the medical device manufacturer and the healthcare organization in exchanging technical information of medical device and IT

network, identifying risks of interoperability and implementing effective control measures. The details of the persons, roles, activities and documentation being part of this co-operation should be agreed and documented by means a specific Responsibility Agreement.

### 2.2.2 IEC/TR 80001-2-2

Since the publication of IEC 80001-1, a number of technical reports have been published to address specific aspects and assist the individuals responsible for the different aspects of medical device integration into IT networks in the implementation of the standard.

One of these is the IEC/TR 80001-2-2 “Application of risk management for IT-networks incorporating medical devices -- Application guidance -- Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls”, published in 2012.

This technical report creates a framework for the disclosure of security-related capabilities and risks necessary for managing the risk in connecting medical devices to IT-networks. Security capabilities are defined as a broad category of technical, administrative or organizational controls to manage risk to confidentiality, integrity, availability and accountability of data and systems when connecting medical devices to IT-networks. The intended use and local factors determine which exact capabilities will be useful in the dialog about risk.

The security capabilities are potential security risk control options. Their selection follows after identifying the need for mitigation of a security risk which is related, in its turn, to the intended use of the medical device when incorporated into the medical IT-network. This may lead to the situation that a specific security solution developed for a particular device in one use scenario might be inappropriate in

another. The risk controls options that can be applied and the potential security risks that can be addressed using that risk are showed in the Table 4:

**Table 4. Security capabilities and related requirement goals**

| IEC/TR 80001-2-2 | | | |
|---|---|---|---|
| **Section** | **Name** | **Description** | **Requirement goal** |
| 5.1 | ALOF | Automatic log-off | Reduce the risk of unauthorized access to health data from an unattended work spot. Prevent misuse by other users if a system or work spot is left idle for a period. |
| 5.2 | AUDT | Audit controls | Define harmonized approach towards reliably auditing who is doing what with health data, allowing HDO IT to monitor this using public frameworks, standards and technology. To allow security officer to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). |
| 5.3 | AUTH | Authorization | Following the principle of data minimization, provide control of access to health data and functions only as necessary to perform the tasks required by the HDO consistent with the intended use. |
| 5.4 | CNFS | Configuration of security features | To allow the HDO to determine how to utilize the product security capabilities to meet their needs for policy and/or workflow. |
| 5.5 | CSUP | Cyber security product upgrade | Create a unified way of working. Installation / Upgrade of product security patches by on-site service staff, remote service staff, and possibly authorized HDO staff (downloadable patches). |
| 5.6 | DIDT | Health data de-identification | Ability of equipment (application software or additional tooling) to directly remove information that allows identification of patient. Data scrubbing prior to shipping back to factory; designing to allow remote service without health data access/exposure; in-factory quarantine, labelling, and training. |
| 5.7 | DTBK | Data backup and disaster recovery | Assure that the healthcare provider can continue business after damage or destruction of data, hardware, or software |
| 5.8 | EMRG | Emergency access | Ensure that access to protected health data is possible in case of an emergency requiring immediate access to stored health data. |

| IEC/TR 80001-2-2 | | | |
|---|---|---|---|
| **Section** | **Name** | **Description** | **Requirement goal** |
| 5.9 | IGAU | Health data integrity and authenticity | Assure that health data has not been altered or destroyed in not authorized manner and is from the originator. Assure integrity of health data. |
| 5.10 | MLDP | Malware detection and protection | Product supports regulatory, HDO and user needs in ensuring an effective and uniform support for the prevention, detection and removal of malware. This is an essential step in a proper defence in depth approach to security. Malware application software is updated, malware pattern data files kept current and operating systems and applications are patched in a timely fashion. Post-updating verification testing of device operation for both continued intended use and safety is often necessary to meet regulatory quality requirements. |
| 5.11 | NAUT | Node authentication | Authentication policies need to be flexible to adapt to local HDO IT policy. As necessary, use node authentication when communicating health data. |
| 5.12 | PAUT | Person authentication | Authentication policies need to be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when providing access to health data. To control access to devices, network resources and health data and to generate non-repudiatable audit trails. This feature should be able to identify unambiguously and with certainty the individual who is accessing the network, device or resource. |
| 5.13 | PLOK | Physical locks on device | Assure that unauthorized access does not compromise the system or data confidentiality, integrity and availability. |
| 5.14 | RDMP | Third-party components in product lifecycle roadmaps | HDOs want an understanding of security throughout the full life cycle of a medical device. MDM plans such that products are sustainable throughout their life cycle according internal quality systems and external regulations. Products provided with clear statement of expected life span. Goal is to manage proactively impact of life cycle of components throughout a product's full life cycle. This commercial off-the-shelf or 3rd party software includes operating systems, database systems, report generators, MIP components etc. (assumption is that existing PCP already manages hardware component obsolescence). |

| IEC/TR 80001-2-2 | | | |
|---|---|---|---|
| **Section** | **Name** | **Description** | **Requirement goal** |
| 5.15 | SAHD | System and application hardening | Adjust security controls on the medical device and/or software applications such that security is maximized ("hardened") while maintaining intended use. Minimize attack vectors and overall attack surface area via port closing; service removal, etc. |
| 5.16 | SGUD | Security guides | Ensure that security guidance for operators and administrators of the system is available. Separate manuals for operators and administrators (including MDM sales and service) are desirable as they allow understanding of full administrative functions to be kept only by administrators. |
| 5.17 | STCF | Health data storage confidentiality | MDM establishes technical controls to mitigate the potential for compromise to the integrity and confidentiality of health data stored on products or removable media. |
| 5.18 | TXCF | Transmission confidentiality | Medical device meets local laws, regulations and standards according to HDO needs to ensure the confidentiality of transmitted health data. |
| 5.19 | TXIG | Transmission integrity | Device protects the integrity of transmitted health data. |

Often, the listed security capabilities are used to supply health delivery organizations and medical device manufacturers with a basis for discussing security risk and their respective roles and responsibilities toward its management. This discussion among the risk partners serves as the basis for the Responsibility Agreement as specified in IEC 80001-1 [5].

One of the resources that MDMs can use to inform the healthcare organizations is expressed with the acronym MDS2 that stands for Medical Disclosure Statement for Medical Device Security, developed by HIMMS (Healthcare Information and Management Systems Society).

The MDS2 is provided by manufacturers in the spirit of transparency, recognizing that safe and secure delivery of patient care is a responsibility shared between MDMs and HDOs. The former ensure the devices they place on the market

include industry-standard security controls to enable safe and secure operation, the latter are responsible for operational security within their environment.

### 2.2.3 IEC/TR 80001-2-5

In 2014 IEC published the technical report 80001-2-5 ”Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance - Guidance for distributed alarm system”.

This technical report gives guidance and practical techniques for medical device manufacturers, responsible organization and providers of other information technology in the application of IEC 80001-1-2010 for the risk management of distributed alarm system. It applies to the transmission of alarm conditions between sources, integrator and communicators where at least one source is a medical device and at least one communication path utilizes a medical IT-network. This technical report provides recommendations for the integration, communication of responses and redirection (to another operator) of alarm conditions from one or more sources to ensure safety, effectiveness and data and system security [11].

The Figure 7 below shows an example of which are the functions of a medical IT-network to distribute alarm condition:

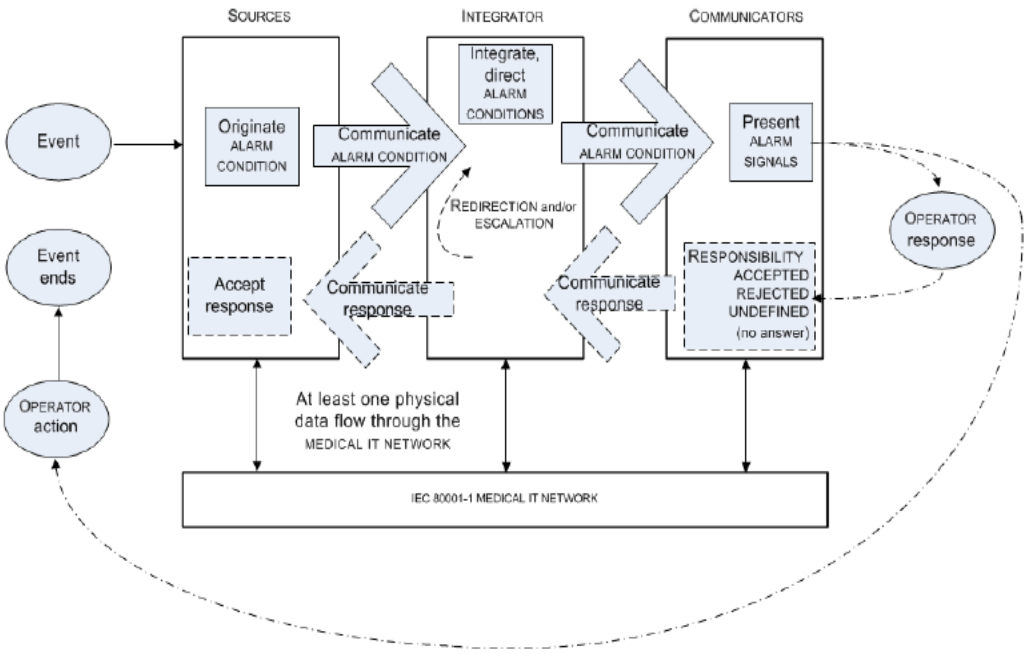


**Figure 7. Functions of a medical IT-network to distribute alarm conditions [10]**

## 2.2.4 IEC/TR 80001-2-8

Lately, in 2016, the IEC published the technical report ISO/TR 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".

This technical report provides guidance to healthcare organizations and medical device manufacturer for the application of the framework outlined in IEC/TR 80001-2-2.

As established by the IEC/TR 80001-2-2 managing the risk in connecting medical devices into IT-network requires the disclosure of security-related capabilities and risks. This report addresses each of them and identifies security controls during risk management activities, device selection, implementation and operation.

The 19 security capabilities are not required in every case and should not be considered exhaustive. Their selection should be based on the risk evaluation and the risk acceptance policy with consideration of for the protection of patient safety, life and health. The intended use of the medical device, operational environment, network structure and other local factors determine which security capabilities are necessary and which security controls are required to make that security capabilities effective [12].

# 3 Tool design and implementation

## 3.1 Introduction

This chapter focuses on the iterative development of the tool. Alike the HDOs to date does not exist any tool which helps MDMs to assess their compliance with the requirements set by norms mentioned in the previous chapter.

The aim of this work is to build a toolkit that can be used to assess the maturity of a software used in the healthcare environment in terms of cybersecurity. In particular, this work aims to provide medical device manufacturer with instructions and a specific checklist in order to encourage the step-by-step implementation of IT security for medical devices, especially for networkable ones, and compensate for the absence of harmonized standard as well as possible. Moreover, it can also be suitable for assessing the technical measures required for data protection. Nevertheless, the focus is on the patient safety and not on the confidentiality of data.

The toolkit developed has like starting point the ISO/IEC 80001 series, that is an international standard but not largely used in Europe. For this purpose, the attention is focused on this standard to diffuse it in the context of medical device incorporated in an IT-network. Furthermore, the attention is also focused on the MDR 2017/745, that will enter in force from May 2021, but only on cybersecurity aspects.

## 3.2 Structure of the toolkit

The structure of the checklist is based on the idea that IT security relays on three fundamental topics:

1. process requirements
2. product requirements
3. documented evidence that these process and product requirements have been met.

The checklist is composed by more than 100 requirements which show an appropriate maturity level according to the following criteria:

**Table 5. Criteria of requirement prioritization**

| PRIORITIZATION LEVEL | LEVEL DEFINITION |
|---|---|
| **0** | Basic level |
| **1** | Advanced level |
| **2** | State of the art |
| **3** | Expert level |

The logic of the requirement prioritization is the following:

- **Basic level**: Anyone who does not even meet the requirements of this level should not develop medical devices. An auditor must expect these requirements to be met in the very first audit;
- **Advanced level**: The manufacturer has already addressed the issue of IT security. This level can be accepted for less critical products and at the initial audits. However, an improvement is expected in each subsequent year until level 2 is reached;
- **State of the art**: This is the level that manufactures generally have to reach in the long run. However, it does not yet reflect the state of scientific knowledge;
- **Expert level**: This level is reached by professional IT security experts. It goes beyond what an auditor can normally expect from medical devices. Energy suppliers, intelligence services and military would have to operate at this level [13]

As it can be seen from the table 5, for each level definition corresponds a specific number describing the level of prioritization. Since the achievement of basic level requirements is fundamental for a medical device manufacturer, the tool carries out a special control thanks to which if all of the basic level requirements are fully achieved then the final assessment result can be calculated, otherwise even if only one of the basic requirements is not fully achieved, the final result cannot be assessed. Consequently, MDM is forced to full implement the risk controls or processes of basic level attributes.

About the choice of the prioritization, are taken into account the following dimensions:

- Risk for an individual patient
- Scope
- Feasibility

All of these requirements are divided in two categories: *process* and *product* requirements. The first category includes all the requirements for the development process and for the post-development phase; while the second category includes all the requirements including preliminary remarks, general information, system requirements, system and software architecture, and finally support materials.

The *process* and *product* requirements in turn are subdivided in several subcategories.

**Table 6. Subcategories of process and product requirements**

| | TOPIC |
|---|---|
| PROCESS REQUIREMENTS | 2 - Expertise |
| | **3.1 - Intended purposes** |
| | **3.2.1 - SysSoft - authentication** |
| | 3.2.2 - SysSoft - data, communication |
| | 3.2.3 - SysSoft - patches and vulnerability |
| | 3.2.4 - SysSoft - other |
| | 3.3 - SysSoft - architecture |
| | **3.4 - Software - implementation** |
| | 3.5 - Software - evaluation |
| | 3.6 - SysSoft - tests |
| | 3.7 - Product release |
| | 4.1 - Production, distribution, installation |
| | **4.2 - Market surveillance** |
| | 4.3 - Incident response plan |
| PRODUCT REQUIREMENTS | **5.1 - SysSoft - authentication** |
| | 5.2 - SysSoft - communication and storage |
| | 5.3 - SysSoft - patches |
| | 5.4 - SysSoft - other |
| | 6 - SysSoft - architecture |
| | 7 - Accompanying materials |

In the Table 6, the subcategories that are highlighted for both the *process* and *product* requirements contain basic level attributes.

Requirements of each subcategory are referred to the related standard above described: MDR 2017/745 and ISO/IEC 80001 series, and for each of them the MDM has to show a specific compliance with a correlated score. By analyzing the ISO/TR 80001-2-7, scores for compliance are assigned by means of the ordinal rating scale to express the levels of achievement, like described in the Table 7 [14]:

**Table 7. Scoring of compliance status**

| SCORES | ACHIEVEMENT LEVELS |
|---|---|
| **0** | **N**= Not achieved |
| **1** | **P=** Partially achieved |
| **2** | **L=** Largely achieved |
| **3** | **F=** Fully achieved |

The logic of the achievement levels is the following:

- **Not achieved**: little or no evidence of achievement of the defined attribute in the assessed process;
- **Partially achieved**: some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of the achievement of the attribute may be unpredictable;
- **Largely achieved**: evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed approach. Some weaknesses related to this attribute exist in the assessed process;
- **Fully achieved**: evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process [14].

## 3.3 Implementation of the tool

Behind the construction of the tool, there is an hard work about the knowledge of right regulations for the cybersecurity topic. In fact, it started from a complex study of several standards concerning the cybersecurity risks. The problem was that the regulations considered in this thesis treated a very wide variety of

subjects. So, the difficulty was to find in these regulations topics which were right for this type of work. Thanks to a long period of research and detailed study, it was possible to extract the most interesting parts and by making an accurate work of synthesis were created a list of requirements specific for cybersecurity aspects. All of these requirements were inserted in Microsoft Excel generating a wide and detailed checklist, composed of attributes referred to ISO/IEC 80001 series and MDR 2017/745 and helpful for manufacturers of medical devices incorporated in a medical IT-network.

Since most of companies use Microsoft Excel for their assessments, the tool was developed by means this program in order to favor its implementation. The toolkit consists of lots of sheets, which are is well defined and they have an appropriate logic. Excel sheets start from those regarding the *assessment criteria*, basic and logic concepts such as the prioritization of requirements, scoring of compliance status (described in the previous paragraph); *overall assessment result* and the *level assessment*.

| Table | Criteria of requirement prioritization |
|---|---|
| Level | |
| 0 | **Basic level**<br>Anyone who does not even meet the requirements of this level should not develop medical devices. An auditor must expect these requirements to be met in the very first audit. |
| 1 | **Advanced level**<br>The manufacturer has already addressed the issue of IT security. This level can be accepted for less critical products and at the initial audits. However, an improvement is expected in each subsequent year until level 2 is reached. |
| 2 | **State of the art**<br>This is the level that manufactures generally have to reach in the long run. However, it does not yet reflect the state of scientific knowledge. |
| 3 | **Expert level**<br>This level is reached by professional IT security experts. It goes beyond what an auditor can normally expect from medical devices. Energy suppliers, intelligence services and military would have to operate at this level. |

| Table | Scoring of compliance status |
|---|---|
| Point | |
| 0 | **N = Not achieved**<br>There is little or no evidence of achievement of the defined attribute in the assessed requirement |
| 1 | **P = Partially achieved**<br>There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed requirement. Some aspects of the achievement may be unpredictable. |
| 2 | **L = Largely achieved**<br>There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed requirement. Some weaknesses related to this attribute may exist in the assessed requirement. |
| 3 | **F = Fully achieved**<br>There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed requirement. No significant weaknesses related to this attribute exist in the assessed requirement. |

| % | Assessment result |
|---|---|
| ≤ 15 | Not compliant |
| 16 - 50 | Partially compliant |
| 51 - 85 | Largely compliant |
| > 85 | Fully compliant |

**Figure 8. Assessment criteria**

| | TOPIC | 0<br>N<br>Not Achieved | 1<br>P<br>Partially | 2<br>L<br>Largely Achieved | 3<br>F<br>Fully Achieved | n° of requirements | n° of basic requirements | n° of Fully Compliant basic requirements | total score<br>achievable | <br>achieved | <br>% | Applicable |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PROCESS REQUIREMENTS | 2 - Expertise | 0 | 1 | 0 | 3 | 4 | 0 | 0 | 12 | 10 | 83 | yes |
| | **3.1 - Intended purposes** | 0 | 0 | 1 | 8 | 9 | 3 | 3 | 27 | 26 | 96 | yes |
| | **3.2.1 - SysSoft - authentication** | 0 | 0 | 2 | 7 | 10 | 4 | 4 | 30 | 25 | 83 | yes |
| | 3.2.2 - SysSoft - data, communication | 0 | 0 | 3 | 4 | 7 | 0 | 0 | 21 | 18 | 86 | yes |
| | 3.2.3 - SysSoft - patches and vulnerability | 0 | 0 | 0 | 3 | 3 | 0 | 0 | 9 | 9 | 100 | yes |
| | 3.2.4 - SysSoft - other | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 6 | 4 | 67 | yes |
| | 3.3 - SysSoft - architecture | 0 | 2 | 3 | 8 | 14 | 0 | 0 | 42 | 32 | 76 | yes |
| | **3.4 - Software - implementation** | 0 | 0 | 1 | 3 | 4 | 1 | 1 | 12 | 11 | 92 | yes |
| | 3.5 - Software - evaluation | 0 | 0 | 0 | 6 | 6 | 0 | 0 | 18 | 18 | 100 | yes |
| | 3.6 - SysSoft - tests | 0 | 1 | 5 | 3 | 9 | 0 | 0 | 27 | 20 | 74 | yes |
| | 3.7 - Product release | 0 | 1 | 0 | 4 | 7 | 0 | 0 | 21 | 13 | 62 | yes |
| | 4.1 - Production, distribution, installation | 0 | 0 | 1 | 3 | 4 | 0 | 0 | 12 | 11 | 92 | yes |
| | **4.2 - Market surveillance** | 0 | 0 | 3 | 4 | 7 | 1 | 1 | 21 | 18 | 86 | yes |
| | 4.3 - Incident response plan | 0 | 0 | 5 | 3 | 8 | 0 | 0 | 24 | 19 | 79 | yes |
| PRODUCT REQUIREMENTS | **5.1 - SysSoft - authentication** | 0 | 5 | 5 | 6 | 16 | 3 | 3 | 48 | 33 | 69 | yes |
| | 5.2 - SysSoft - communication and storage | 0 | 2 | 7 | 5 | 14 | 0 | 0 | 42 | 31 | 74 | yes |
| | 5.3 - SysSoft - patches | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 12 | 10 | 83 | yes |
| | 5.4 - SysSoft - other | 0 | 2 | 1 | 2 | 5 | 0 | 0 | 15 | 10 | 67 | yes |
| | 6 - SysSoft - architecture | 0 | 0 | 1 | 3 | 4 | 0 | 0 | 12 | 11 | 92 | yes |
| | 7 - Accompanying materials | 0 | 0 | 4 | 3 | 8 | 0 | 0 | 24 | 17 | 71 | yes |
| | Sum: | 0 | 14 | 46 | 80 | 145 | 12 | 12 | 435 | 346 | | |

**Figure 9. Example of an *overall assessment result***

| LEVEL | 0<br>N<br>Not Achieved | 1<br>P<br>Partially Achieved | 2<br>L<br>Largely Achieved | 3<br>F<br>Fully Achieved | n° of requirement | total score<br>achievable | <br>achieved | <br>% |
|---|---|---|---|---|---|---|---|---|
| LEVEL 0 | 0 | 0 | 0 | 12 | 12 | 36 | **36** | 100 |
| LEVEL 1 | 0 | 2 | 6 | 46 | 58 | 174 | **152** | 87 |
| LEVEL 2 | 0 | 9 | 37 | 22 | 69 | 207 | **149** | 72 |
| LEVEL 3 | 0 | 3 | 3 | 0 | 6 | 18 | **9** | 50 |
| Sum: | 0 | 14 | 46 | 80 | 145 | 435 | 346 | |

| | |
|---|---|
| Assessment score | ***80%*** |
| Compliance result | ***Largely compliant*** |

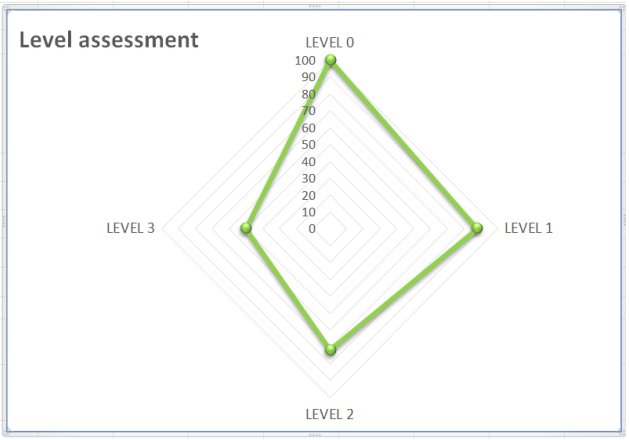


**Figure 10. Example of a *level assessment***

After those begin the subcategories sheets and each of them are characterized by cybersecurity requirements with a specific level of prioritization, referred to specific standards (ISO/IEC 80001 series and/or MDR 2017/745), and distinguished by the corresponding score of compliance status. The general composition of a subcategory worksheet is reported in the next figure:

| Q# | REQUIREMENT | NORM/STANDARD | LEVEL | COMPLIANCE | |
|---|---|---|---|---|---|
| | **PROCESS REQUIREMENTS**<br>**3.Development process**<br>**3.1.Intended purposes and stakeholder** | | | | |
| 3.1.1 | The manufacturer has identified all neighboring systems (e.g. medical devices, IT systems) that may be connected to the product. | (EU) 2017/745, Annex I, section 14.1<br>IEC 80001-1:2010 | 0 | F | |
| 3.1.2 | The manufacturer has created a list of roles (people, neighboring systems) that may interact with the product. | (EU) 2017/745, Annex I, section 14.1<br>IEC 80001-1:2010 | 0 | F | |
| 3.1.3 | The manufacturer has identified all markets and all the regulatory requirements that are relevant in these markets. | IEC 80001-1:2010 | 0 | F | |
| 3.1.4 | The manufacturer has identified the intended primary and secondary users with their IT expertise. | (EU) 2017/745, Annex I, section 1<br>IEC 80001-1:2010 | 1 | F | |
| 3.1.5 | The manufacturer has defined the intended use environment. | (EU) 2017/745, Annex I, section 14.2d<br>IEC 80001-1:2010 | 1 | F | |
| 3.1.6 | The manufacturer has analyzed the risks (hazards) that result if the system is not used by specified users or in the specified use environment. | (EU) 2017/745, Annex I, section 14.1<br>IEC 80001-1:2010 | 1 | F | |
| 3.1.7 | The manufacturer has described in the risk management documentation what the IT security threats are and what the consequences would be for patients, users and third parties. | (EU) 2017/745, Annex I, section 3b<br>IEC 80001-1:2010 | 1 | F | |
| 3.1.8 | The manufacturer has traceably generated the risk acceptance criteria based on the product's use and the state-of-the-art. | (EU) 2017/745, Annex I, section 4-8<br>IEC 80001-1:2010 | 1 | F | |
| 3.1.9 | The manufacturer has developed a system it can use to evaluate IT security-related risks. | (EU) 2017/745, Annex I, section 3c<br>IEC 80001-1:2010 | 2 | L | |
| | | | | ← | result |

**Figure 11. Example of subcategory worksheet**

As to be noted by the Figure 11, at the bottom on the right there is a blue arrow which allows thanks to special control to return at the final result.

Once scores are assigned for each requirement, thanks to a special control it is possible to assess the compliance of medical device for both process and product requirements separately. This allows medical device manufacturers to understand

the difference of the compliance level between the two macro-categories by using a spider diagram, as reported below in the Figure 12.

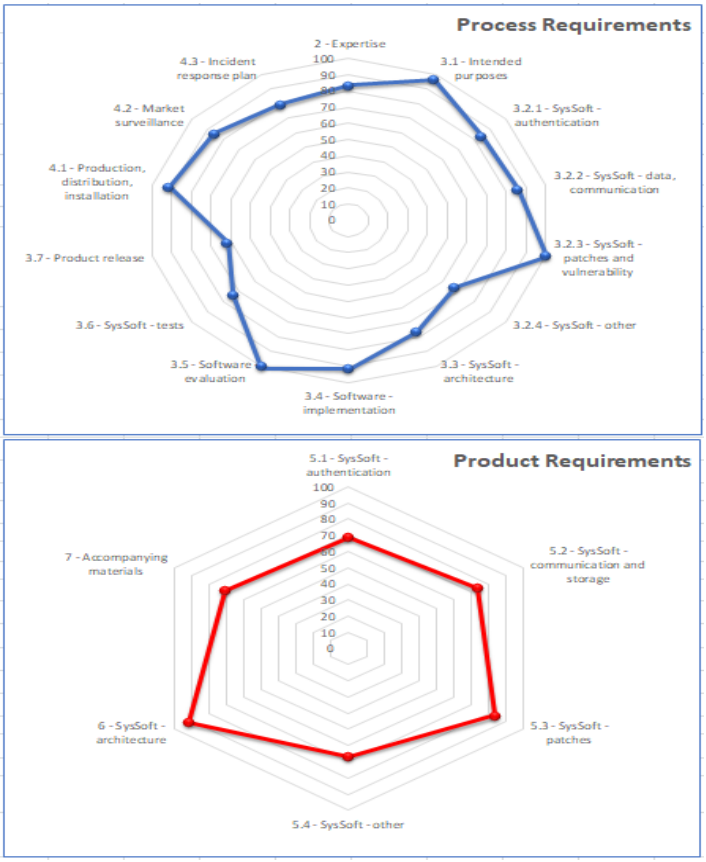


**Figure 12. Example of different compliance level for *process* and *product* requirements**

In order to obtain a wider vision and a final result of the data assessment about compliance level, it is possible to calculate the assessment result resulting from scores assigned to each requirement of the checklist, as reported in the Figure 13:

| % | Assessment result |
|---|---|
| ≤ 15 | Not compliant |
| 16 - 50 | Partially compliant |
| 51 - 85 | Largely compliant |
| > 85 | Fully compliant |

**Figure 13. Compliance criteria**

The logic of the assessment result is the following:

- **Not compliant**: little or no evidence of achievement of the requirements in the assessed processes;
- **Partially compliant**: some evidence of an approach to, and some achievement of, the requirements in the assessed processes. Some aspects of the achievement of the requirements may be unpredictable;
- **Largely compliant**: evidence of a systematic approach to, and significant achievement of, the requirements in the assessed approach. Some weaknesses related to requirements exist in the assessed processes;
- **Fully compliant**: evidence of a complete and systematic approach to, and full achievement of, the requirements in the assessed processes. No significant weaknesses related to requirements exist in the assessed processes [14].

As to be noticed from the Figure xx above, the final assessment score is expressed in percentage and the maximum level of compliance is achieved by reaching an assessment result greater than 85%. Obviously, the ***fully compliant*** result is what medical device manufacturer has to strive for, to consider satisfying the overall assessment of its software.

The final result can be also assessed through the compliance level with respect each level of requirements as shown in the figure below:

# 4 Case of study

The checklist described in this work was applied and tested on a medical device developed by BiMind srl. The medical device concerned is a software (MDSW) for the control in the prescription of chemotherapy, and it has the aim to calculate the dose for chemotherapy. The data assessment was carried out through two videoconferences, due to Covid-19, by conducting an interview first and then an audit with two software developers.

Before starting the assessment, the medical device manufacturers described the general information of the MDSW reported in the Figure 14.

| | | | |
|---|---|---|---|
| 1.1 | Manufacturer Name | BiMind | |
| 1.2 | Device Description | Software for the control in the prescription of chemotherapy | |
| 1.3 | Device Model | DOSSIER THERAPY | |
| 1.4 | Document ID | 4.20 | |
| 1.5 | Manufacturer Contact Information | info@bimind.it | |
| 1.6 | Intended use of device in network-connected environment: | Calculation of the dose for chemoterapy | |
| 1.7 | Document Release Date | 2014-07-30 | |
| 1.8 | Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device? | Yes | |
| 1.9 | ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization? | No | |
| 1.10 | Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources? | See Notes | The software is stand alone |
| 1.11 | SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)? | Yes | |
| 1.12 | Does the SaMD contain an operating system? | No | |
| 1.13 | Does the SaMD rely on an owner/operator provided operating system? | Yes | |
| 1.14 | Is the SaMD hosted by the manufacturer? | No | |
| 1.15 | Is the SaMD hosted by the customer? | Yes | |

**Figure 14. General information about the MDSW**

Then, the checklist of the toolkit was explained to them in order to understand which were the assessment criteria and the meaning of maturity levels for requirements (see Tables 5 and 7).

After a general explanation of the preliminary concepts, the checklist was applied to the MDSW. Requirements of each excel sheet (intended as subcategories) of the work were checked and for each of them were assigned the corresponding scores, according to the pre-established criteria (Table 7).

| Q# | REQUIREMENT | NORM/STANDARD | LEVEL | COMPLIANCE |
|---|---|---|---|---|
| | **PROCESS REQUIREMENTS**<br>**3.Development process**<br>**3.7.Product release** | | | |
| 3.7.1 | The manufacturer has addressed the most common vulnerabilities and the resulting hazards in the risk analysis or can at least explain how these risks are controlled. | (EU) 2017/745, Annex I, section 3-4<br>IEC TR 80001-2-2:2012, Section 5.16 | 1 | F |
| 3.7.2 | The manufacturer discusses the risks posed by all relevant attack vectors (see above) in the risk analysis and shows how these risks are controlled. | (EU) 2017/745, Annex I, section 3-4<br>IEC TR 80001-2-2:2012, Section 5.16 | 1 | F |
| 3.7.3 | The manufacturer has checked the effectiveness of all risk-control measures. | (EU) 2017/745, Annex I, section 3-4<br>IEC 80001-1:2010 | 1 | F |
| 3.7.4 | The manufacturer has created a traceability matrix it uses to document that there are measures that control all identified risks related to IT security. | (EU) 2017/745, Annex I, section 3-4<br>IEC 80001-1:2010 | 2 | F |
| 3.7.5 | The manufacturer has prepared the risk management report and the IT security report. | (EU) 2017/745, Annex I, section 3-4<br>IEC 80001-1:2010 | 2 | P |
| 3.7.6 | The manufacturer has drawn up the necessary plans for the post-development phase (e.g. post-market surveillance and incident response plan). | (EU) 2017/745, Annex I, section 3<br>IEC 80001-1:2010<br>IEC TR 80001-2-2:2012, Section 5.15 | 1 | F |
| 3.7.7 | The manufacturer has evaluated the completeness of the tests using a traceability matrix that links the tests to the requirements. | (EU) 2017/745, Annex I, section 3<br>IEC 80001-1:2010 | 2 | F |

**Figure 15. Example of a completed checklist section**

As described in the previous chapter, once made the score attribution for each requirement, it was possible to calculate the compliance status of the medical device concerned for both *process* and *product* requirements.

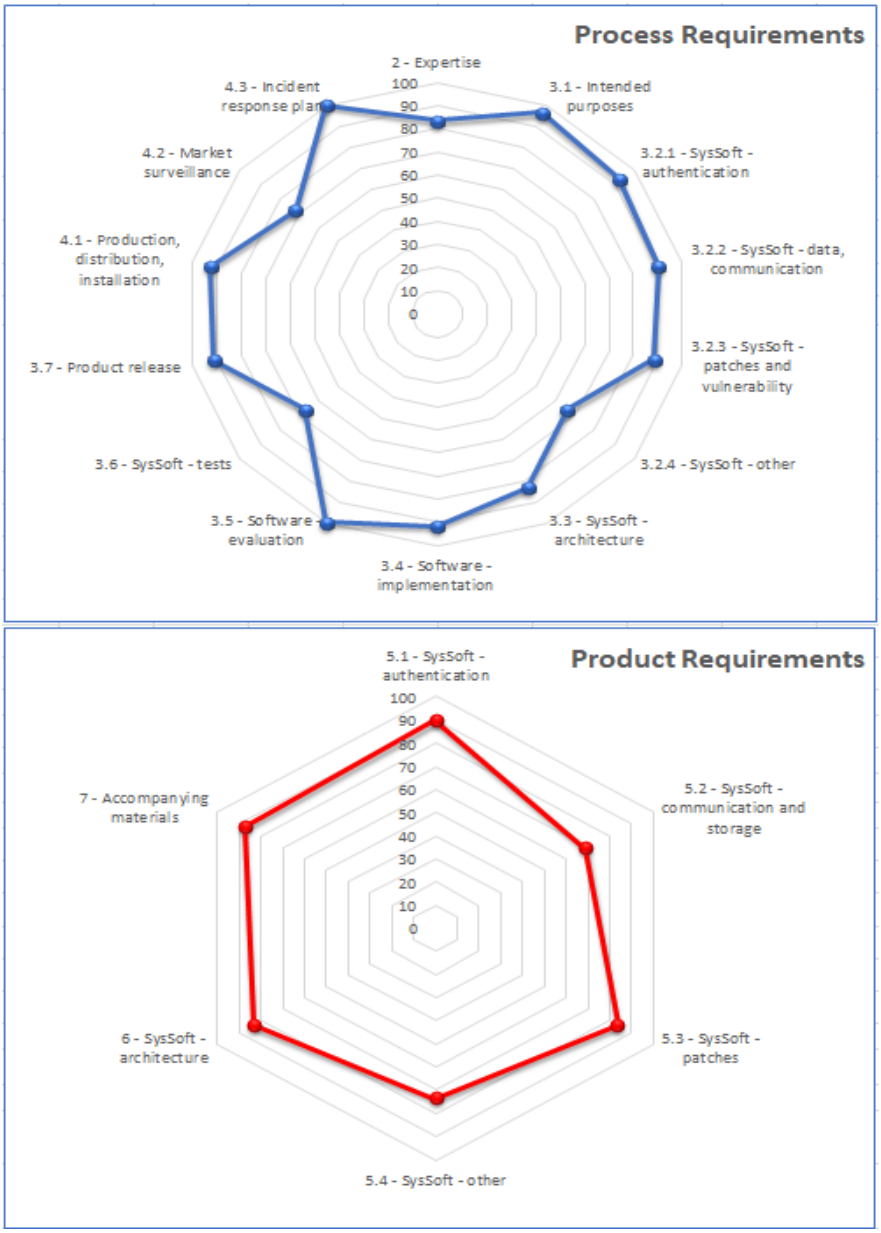


**Figure 16. Compliance status of the software for both *process* and *product* requirements**

Spider diagrams show different levels of compliance among the several subcategories of attributes. It can be noticed that there are only two subcategories (*software evaluation* and *incident response plan*) which are compliant for the 100%, while all the others don't reach the 100%. This fact

suggests to the MDM in which aspects the software has to be improved to reach the maximum compliance with each subcategory of requirements.

Finally, since all the basic level requirements are *fully achieved* the overall result of the assessment was calculated.

| | | 0 | 1 | 2 | 3 | | | | total score | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | TOPIC | N Not Achieved | P Partially | L Largely Achieved | F Fully Achieved | n° of requirements | n° of basic requirements | n° of Fully Compliant basic requirements | achievable | achieved | % |
| PROCESS REQUIREMENTS | 2 - Expertise | 0 | 1 | 0 | 3 | 4 | 0 | 0 | 12 | **10** | 83 |
| | **3.1 - Intended purposes** | 0 | 0 | 1 | 8 | 9 | 3 | 3 | 27 | **26** | 96 |
| | **3.2.1 - SysSoft - authentication** | 0 | 0 | 2 | 8 | 10 | 4 | 4 | 30 | **28** | 93 |
| | 3.2.2 - SysSoft - data, communication | 0 | 0 | 2 | 5 | 7 | 0 | 0 | 21 | **19** | 90 |
| | 3.2.3 - SysSoft - patches and vulnerability | 0 | 0 | 1 | 2 | 3 | 0 | 0 | 9 | **8** | 89 |
| | 3.2.4 - SysSoft - other | 0 | 0 | 2 | 0 | 2 | 0 | 0 | 6 | **4** | 67 |
| | 3.3 - SysSoft - architecture | 0 | 1 | 5 | 8 | 14 | 0 | 0 | 42 | **35** | 83 |
| | **3.4 - Software - implementation** | 0 | 0 | 1 | 3 | 4 | 1 | 1 | 12 | **11** | 92 |
| | 3.5 - Software - evaluation | 0 | 0 | 0 | 6 | 6 | 0 | 0 | 18 | **18** | 100 |
| | 3.6 - SysSoft - tests | 0 | 0 | 9 | 0 | 9 | 0 | 0 | 27 | **18** | 67 |
| | 3.7 - Product release | 0 | 1 | 0 | 6 | 7 | 0 | 0 | 21 | **19** | 90 |
| | 4.1 - Production, distribution, installation | 0 | 0 | 1 | 3 | 4 | 0 | 0 | 12 | **11** | 92 |
| | **4.2 - Market surveillance** | 0 | 1 | 4 | 2 | 7 | 1 | 1 | 21 | **15** | 71 |
| | 4.3 - Incident response plan | 0 | 0 | 0 | 8 | 8 | 0 | 0 | 24 | **24** | 100 |
| PRODUCT REQUIREMENTS | **5.1 - SysSoft - authentication** | 0 | 1 | 3 | 12 | 16 | 3 | 3 | 48 | **43** | 90 |
| | 5.2 - SysSoft - communication and storage | 0 | 4 | 5 | 5 | 14 | 0 | 0 | 42 | **29** | 69 |
| | 5.3 - SysSoft - patches | 0 | 1 | 0 | 3 | 4 | 0 | 0 | 12 | **10** | 83 |
| | 5.4 - SysSoft - other | 0 | 1 | 2 | 2 | 5 | 0 | 0 | 15 | **11** | 73 |
| | 6 - SysSoft - architecture | 0 | 0 | 2 | 2 | 4 | 0 | 0 | 12 | **10** | 83 |
| | 7 - Accompanying materials | 0 | 1 | 1 | 6 | 8 | 0 | 0 | 24 | **21** | 88 |
| | Sum: | 0 | 12 | 41 | 92 | 145 | 12 | 12 | 435 | 370 | |

**Figure 17. Overview of overall assessment of the MDSW**

In the picture above, the highlighted value corresponds to the total score achieved, given by the sum of points achieved for each subcategory of requirements. In this case, the medical devices scored a value of 370/435 and according to the Figure 13 was obtained the following overall result:

| | |
|---|---|
| Assessment score | ***85%*** |
| Compliance result | ***Fully compliant*** |

**Figure 18. Overall result of medical device**

As shown in the Figure 18, the assessment score is equal to 85%, meaning that the total compliance is considered as *fully compliant*, according to the Figure 11. About this, the result obtained by the assessment can be considered good as desired.

# 5 Conclusion

The interoperability of medical devices and the incorporation of these medical devices onto IT-networks are becoming widespread. This coupled with the increase in cyber-attacks on HDOs, rises the risks to patient safety and data and system security. Since there is not harmonized standard about this topic, there is not a specific procedure to follow for ensuring the security of MD and for this purpose, it is difficult to achieve an optimal level in terms of cybersecurity.

Usually, most of works are intended for the HDOs which buy and use the medical device, instead the tool developed in this work is intended in particular for MDMs, for medical devices incorporated in an IT-network. Moreover, it focuses on the IT security of the medical device and not the organization's IT security.

The most interesting part of the tool relays on the fact that the requirements of the checklist are related to standards which are innovative. Indeed the ISO/IEC 80001 series is more diffused in the American Countries than the European ones ,and the MDR 2017/745 will be enter in force from May 2021. So, to be compliant with these regulations could allow MDMs to ensure that their medical devices have an additional feature regarding the cybersecurity. In the tool, this aspect is treated in a very accurate manner allowing MDMs to know if the control measures adopted during the development and post-development phases are suitable for considering the cybersecurity risks and for an acceptable level along its total life cycle.

With regard to the further development of the tool, could be useful to integrate it with the ISO 27000 series of standards, regarding the health informatics. This because the increase of several attempts by professional attackers, who in the future could introduce malware into medical devices through the manufacturing organization's IT infrastructure, by means of communication, configuration tools, software tools and libraries.

Furthermore, in the context of tenders in healthcare, the need for medical device companies to manufacture their products in accordance with the privacy discipline has emerged. It is therefore essential to have a report or an audit report on the corporate adjustment in order not to risk losing business opportunities. In particular, *privacy by design* aspect has to be treated, in order to be compliant with GDPR, so having another advantage with respect to medical devices which don't consider profiles of data protection.

# *List of References*


[1] G. Shabot et a. *Patient-Monitoring Systems. In: SHORTLIFFE, E. H. & PERREAULT, L. E. (eds.) Medical Informatics: Computer Applications in Health Care and Biomedicine. New York, NY: Springer New York, 2001.*

[2] A. Buxò, 2012. *Projecte del St. Olavs Trondheim University Hospital. Health & Medicine.*

[3] S. Rod. *The Benefits Of IT Convergence In Healthcare, 2016.*

[4] K. Delvecchio. *Step-by-step risk management for medical IT networks. Biomed Instrum Technol, Suppl, pp. 37-43, 2011*

[5] International Electrotechnical Commission (IEC). S*tandard 80001-1, 2010.*

[6] Medical Device Coordination Group. *Guidance on Cybersecurity for medical devices, 2019.*

[7] McKinsey&Company. *Reforming hospitals with IT investments, 2010.*

[8] CLUSIT. *Rapporto sulla Sicurezza ICT in Italia, pp. 24-25, 2020*

[9] International Medical Device Regulators Forum. *Principles and Practices for Medical Devices Cybersecurity, 2020.*

[10] European Council. *Medical Devices Regulations n. 745/2017 (MDR).*

[11] International Electrotechnical Commission (IEC). Technical Report *80001-2-5, 2014.*

[12] International Electrotechnical Commission (IEC). Technical Report *80001-2-8, 2016.*

[13] A. Purde, O. Teichert, C. Johner, G. Heidenreich. *It security guideline for medical devices*, *January 6,2020*.

[14] *ISO/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Guidance for*

*Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1.*