Risk management for medical devices and the new BS EN ISO 14971

Author: Jos van Vroonhoven, Philips.
Updated in July 2022.

BSI White Paper Series

By Royal Charter

Contents

Introduction

Risk management is an important aspect in the life cycle of medical devices. Patients are already in a vulnerable position, and during diagnosis and treatment, they should be protected from risks that could further impact their health. International standard BS EN ISO 14971 [1] was developed to provide a process to assist manufacturers in identifying the hazards associated with medical devices, assessing the corresponding risks, controlling these risks where needed, and monitoring the effectiveness of the risk control measures. The third edition of this standard was published in December 2019, followed in June 2020 by the updated companion report ISO/TR 24971 [2], which provides extensive guidance on the application of the standard. A transitional period of 3 years following publication is usual to allow all stakeholders to adapt to the requirements in the new edition.

The standard is adopted in the European Union as a new edition of BS EN ISO 14971, and the guidance report is adopted as CEN ISO/TR 24971. EN ISO 14971:2019 and its amendment A11:2021 is listed in the Official Journal of the European Union (OJEU) as a harmonized standard in support of the European Regulations 2017/745 [6] for medical devices (MDR) and 2017/746 [7] for in vitro diagnostic medical devices (IVDR). Since national standards bodies are obliged to adopt European Norms as national standards, BS EN ISO 14971:2019 is adopted in the United Kingdom as a new edition of BS EN ISO 14971 with identical technical content as BS EN ISO 14971:2019 and a national foreword. The guidance report is adopted in the United Kingdom as PD CEN ISO/TR 24971:2020. In this paper, we will refer to the international documents BS EN ISO 14971 and ISO/TR 24971 for brevity.

This paper starts with a brief overview of the development of risk management over the past centuries, from elementary risk awareness in the early days to the structured stepwise process of planning, assessment, control and monitoring that we have today. This includes a review of how regulations and standards for medical devices have developed over the recent decades. The risk management process as described in BS EN ISO 14971 [1] is discussed in detail and the main changes in the third edition are indicated and explained. The broader context of BS EN ISO 14971 and its use in conjunction with other international standards to demonstrate compliance with regulatory requirements is also discussed.

History of risk management

Risk perception in early days

Risk management has evolved over many centuries. It started with awareness and the recognition that sometimes things go wrong, and gradually progressed with the application of more structured approaches and finally developed into a field of science in its own right. Elaborate historical reviews of risk management can be found in [8, 9, 10]. In the times of ancient history, people recognized that they could have good luck on some days and bad luck on other days. They consulted priests and oracles to learn if the gods would favour their actions and which would be the right day to build a house or to embark on a long journey. The advice was often cryptic and ambiguous, but it provided confidence when their decisions were based on the advice given. This way of dealing with uncertainty should be seen more as an early and limited kind of 'risk awareness' than as an effective form of risk management. Failures and damages that occurred were accepted and regarded as part of their unavoidable fate, but there were no attempts to understand or even eliminate the underlying causes.

In later years, people would apply 'trial and error' methods and use experience from previous failures to improve their decisions and actions. The focus was on analysing and learning from previous mistakes and failures and on improving product designs to prevent new failures, but there was less focus on reducing the consequences of the failures. This can be seen as a simple but effective application of post-production feedback. The industrial revolution of the 19th century opened a new era of mechanization. The invention of the steam engine enabled the development of locomotives and large machines for a wide variety of industrial applications. These machines made of iron introduced new risks that were not present before. The brittleness of cast iron and the power of pressurized steam frequently resulted in accidents with severe injuries and often with many people being injured or killed, which revealed the need to develop safety principles and to perform reliability engineering. This led to the development of safer designs and better materials (wrought iron, steel alloys) and to the implementation of protective measures with the machinery.

The development of statistical methods in the 17th century by Pascal [11] and later refinements by Laplace [12] provided a mathematical basis for probability theory. This theory enabled the analysis of the probability of occurrence of failures and deviations from the expected. Statistical methods came into use by banks and insurance companies to support decision making and to manage financial risks. Nevertheless, it was not until after World War II that more structured approaches to risk analysis and risk management came into use for product development. This was stimulated for a large part by the growth of the aviation and aerospace industries and the concerns on the safety of nuclear power plants. Structured approaches for risk analysis were developed, such as Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA) and Hazard and Operability Study (HAZOP). Safety engineering also became an important topic in the defence sector, where the first edition of the US military standard MIL-STD-882 on system safety [13] was published in 1977, and even more prominently in the aviation sector, where a United Nations specialized agency for civil aviation safety [14] was established already in 1944.

Risk management for medical devices

Performing risk management became an essential requirement for medical device manufacturers with the publication of the European Directives AIMDD [3], MDD [4] and IVDMDD [5]. The risk management requirements only covered risk analysis and were expressed in general, not very specific terms. Risks needed to be reduced as far as possible while taking account of the generally acknowledged state of the art and maintaining a high level of protection of health and safety. Similar requirements can be found in the regulations of other countries. European standard EN 1441 [15] provided a procedure for manufacturers to investigate the safety of medical devices by identifying hazards and estimating risks based on available information. The scope of this standard was restricted to risk analysis because it was intended for conformity assessment purposes, i.e. to support demonstrating conformity with the essential requirements related to risk analysis in the European medical device directives. Unfortunately, the directives provide little guidance on further steps in the risk management process and on the acceptability of residual risks.

ISO Technical Committee 210 (Quality management and corresponding general aspects for medical devices) and IEC Subcommittee 62A (Common aspects of electrical equipment used in medical practice) recognized the need to develop an international standard for risk management of medical devices and established their Joint Working Group 1. EN 1441 [15] was taken as a starting point and was converted with minimal editing to BS EN ISO 14971-1 [16] in 1998, which thus also covered risk analysis. BS EN ISO 14971-1 was intended to be the first part in a series of standards. It was decided later that, instead of publishing separate parts, it would be better to publish one document covering all elements of the risk management process. This effort led to the first edition of BS EN ISO 14971 [1] in 2000, in which the principles of risk management for medical devices were elaborated further and the entire risk management process was described. This standard provided a complete framework for risk management including monitoring risks in the post-production phase. The standard was amended with a rationale in 2003.

The second edition of ISO 14971 was published in 2007 and the third edition in 2019, followed by the revised companion document ISO/TR 24971 [2] in 2020, containing extensive guidance on the application of ISO 14971. The requirements in the third edition of BS EN ISO 14971 [1] are expressed more accurately and are elaborated with more detail compared to the second edition. The requirements are in line with the recognized essential principles of safety and performance of medical devices (see ISO 16142-1 [17]) and in vitro diagnostic medical devices (see ISO 16142-2 [18]). They are also aligned with the general safety and performance requirements of the European Regulations, MDR [6] and IVDR [7]. In view of the improved and more detailed risk management requirements in these regulations compared to the European Directives [3, 4, 5], it is more accurate to say that the general safety and performance requirements in [6, 7] have been aligned with the globally accepted risk management framework and principles that have evolved over the past decades. As result of this alignment, there are no content deviations between the risk management requirements of the European MDR and IVDR and those in the third edition of BS EN ISO 14971.

Risk management by BS EN ISO 14971

General

The risk management process described in BS EN ISO 14971 [1] consists of several steps, as illustrated in Figure 1, which apply to the design, development, production and post-production stages of every medical device. The distinct process steps are numbered from 1 to 6 and discussed in detail in this paper. It is important to recognize that these steps need to be documented in procedures in the manufacturer's organization. The procedures for risk management can be embedded in a quality management system, but this is not required by BS EN ISO 14971. The reason is that regulations in some countries do not oblige manufacturers of low-risk medical devices to implement a quality management system. However, if a manufacturer has implemented a quality management system, it is recommended to integrate the risk management procedures into that system. In this context, it is emphasized that the European MDR and IVDR [6, 7] require the manufacturer to implement a quality management system that addresses risk management.

Figure 1 – The six process steps in the risk management process of BS EN ISO 14971 [1].

A selection of important definitions in BS EN ISO 14971 [1] is given in Table 1. These defined terms are frequently used in this paper. The definitions for benefit and reasonably foreseeable misuse are new in the third edition of the standard. It is further noted that the numbering of the clauses has changed in the third edition of BS EN ISO 14971, because a clause on normative references has been inserted following requirements by the ISO/IEC Directives.

Table 1 – Important definitions in BS EN ISO 14971 [1]

Term	Definition
Benefit	Positive impact or desirable outcome of the use of a medical device on the health of an individual, or a positive impact on patient management or public health **Note:** Benefits can include positive impact on clinical outcome, the patient's quality of life, outcomes related to diagnosis, positive impact from diagnostic devices on clinical outcomes, or positive impact on public health
Harm	Injury or damage to the health of people, or damage to property or the environment
Hazard	Potential source of harm
Hazardous situation	Circumstance in which people, property or the environment is/are exposed to one or more hazards
Intended use	Use for which a product, process or service is intended according to the specifications, instructions and information provided by the manufacturer **Note:** The intended medical indication, patient population, part of the body or type of tissue interacted with, user profile, use environment and operating principle are typical elements of the intended use
Reasonably foreseeable misuse	Use of a product or system in a way not intended by the manufacturer, but which can result from readily predictable human behaviour **Note:** Readily predictable human behaviour includes the behaviour of all types of users, e.g. lay and professional users. Reasonably foreseeable misuse can be intentional or unintentional
Residual risk	Risk remaining after risk control measures have been implemented
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Risk control	Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels
Safety	Freedom from unacceptable risk

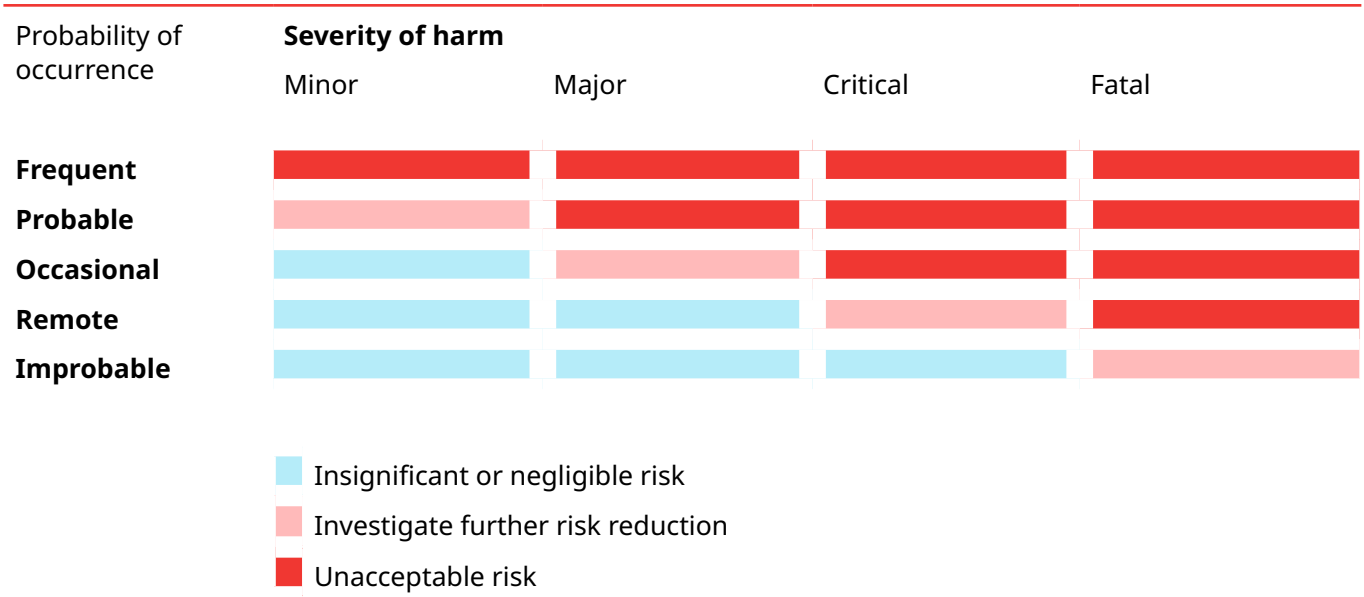
Top management responsibilities

The commitment of top management is indispensable for proper risk management. Large corporations can consist of separate entities (such as divisions or business units), where each entity can have its own risk management process and its own quality management system. In such cases, top management refers to those individuals who direct and control that entity.

Top management is responsible for the provision of adequate resources and the assignment of competent personnel. This means that personnel need to have appropriate training and also the tools and the time to perform the risk management tasks assigned to them. Top management is further responsible for the continued effectiveness of the risk management process and, therefore, needs to regularly review its suitability at planned intervals. Information from the post-production phase can be valuable input for this review.

Top management also needs to define the policy on how to establish the criteria for risk acceptability. These criteria need to be based on relevant international standards and the regulations of the countries or regions where the medical devices are intended to be marketed. Considerations of the generally acknowledged state of the art and known stakeholder concerns need to be taken into account as well. Local regulations can impose that risks must be reduced as far as possible or as low as reasonably practicable (i.e. technically feasible in practice). A well-known concept for exposure to ionizing radiation is that the resulting radiation dose to any person must be as low as reasonably achievable (the ALARA principle, see [19, 20]). Where applicable, these concepts need to be incorporated in the criteria for risk acceptability. This means that the criteria need to provide guidelines on how far the risks shall be reduced. The end points for risk reduction 'as far as possible' can be determined based on international standards that provide specific state-of-the-art technical solutions or on local regulations that have specific requirements or limits. These concepts and the end points for risk reduction should be described in the policy.

Figure 1 – Important definitions in BS EN ISO 14971 [1]



A risk chart or risk matrix shown in Figure 2 can be useful in supporting the estimation and evaluation of residual risk, especially those risks for which no requirements and no technical solutions exist in international standards or local regulations. In such cases, the criteria can require risk reduction as far as possible where the end point is based on the combination of the probability of occurrence of harm and the severity of possible harm, as indicated in a risk chart. However, it is emphasized that the criteria for risk acceptability need to take the applicable regulations and standards into account and need to be more comprehensive than only a risk chart, and that a risk chart by itself is not the criteria. It is further noted that the descriptors of the severity and probability levels in Figure 2 are just examples, and that more or fewer levels and different descriptors can be chosen (e.g. Negligible, Moderate, Significant, Serious, Catastrophic for the severity levels and Inconceivable, Unlikely, Rare, Possible, Often for the probability levels). ISO/TR 24971 [2] provides guidance on defining the policy and on establishing the criteria for risk acceptability.

The severity levels need to be described in relation to the possible harm (injury to people, or damage to property or the environment). These levels can distinguish between life-threatening injuries, serious injuries that are not life-threatening but needing immediate medical attention, major injuries that can result in permanent damage or impairment, minor injuries that are transient or reversible, minor injuries needing limited medical care, pain and discomfort. Concerning damage to property or the environment, the severity levels can distinguish between leakage of radioactive substances, leakage of or contact with hazardous chemicals, contamination with blood or other bodily fluids (possible infection with blood-borne viruses or bacteria), loss of x-ray images (where retaking adds radiation dose), loss of other images, loss of data, unauthorized access to data, destruction of the medical device or repairable damage to the medical device. The probability range can be divided into discrete levels based on the probability of occurrence of harm per use, per procedure, per device, per hour of use or within a population. The choice can depend on the type of medical device.

Risk management plan (process step 1)

All risk management activities must be planned. The plan provides a roadmap for the risk management activities to be conducted during the life cycle of the medical device. The risk management plan has to include among others the criteria for risk acceptability for the medical device to be developed. These criteria are established based on the policy defined by top management. The inclusion of the criteria in the risk management plan is helpful in ensuring an objective evaluation of the residual risks later in the process. Moreover, having a plan ensures an organized approach to risk management and prevents essential activities from being forgotten. For this purpose, a review of the execution of the risk management plan is required to be performed at the end of the design and development process and before commercial distribution of the medical device. This review ensures that the risk management plan has been properly executed so far, and that the final medical device is safe. The risk management plan further includes activities for the verification of the implementation and effectiveness of the risk control measures and activities for the collection and review of information during the production and post-production phases.

A risk management file needs to be created and maintained. Important parts of the risk management file are the risk management plan and the risk management report, which is created after the review of the execution of the plan. The risk management file further contains (references to) all records and other documents that are produced during the risk management process. The risk management file needs to provide traceability for each identified hazard to the risk analysis, the risk evaluation and the implemented risk control measures, including the evaluation of the residual risks. Traceability is necessary to ensure completeness of the risk management process, i.e. that all hazards are appropriately addressed and that every risk is adequately controlled.

Risk assessment (process step 2)

Risk assessment is a key element of the risk management process, consisting of a risk analysis and a risk evaluation. The first step in the risk analysis is documenting the intended use of the medical device (see definition in Table 1). It is important that the manufacturer carefully thinks about the purpose of the planned medical device. clear description of the intended use is helpful in determining the boundaries of the correct use or correct application of the medical device. Any use beyond those boundaries determines the ‘misuse’ of the medical device.

The intended use includes:

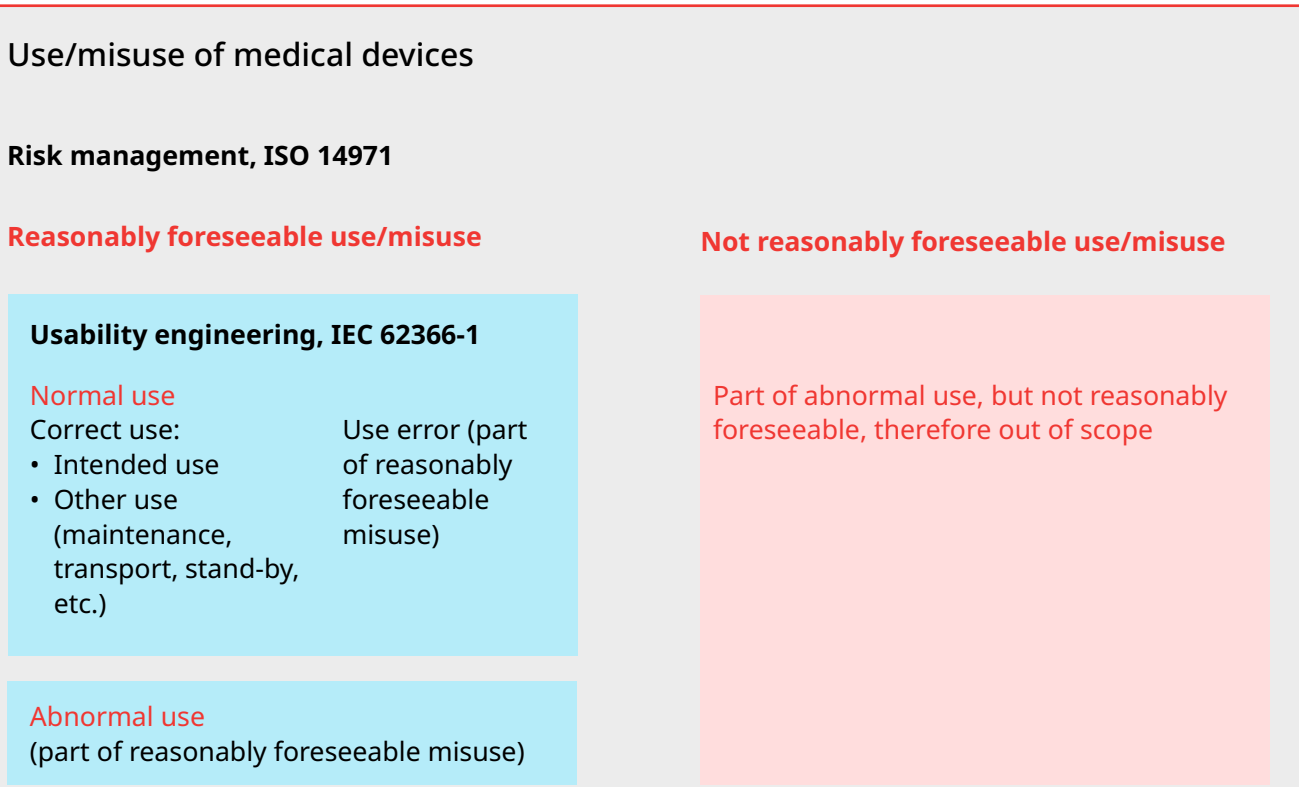
- the medical indication and application (disease type, tissue and part of the body)
- the intended patient population (children, adults, elderly or specific patient groups, which can include limitations in dexterity or cognition)
- the users and the use environment (lay users at home, professional users in a hospital or outside hospitals for emergency care)
- the operating principle (how the diagnosis or treatment is achieved)

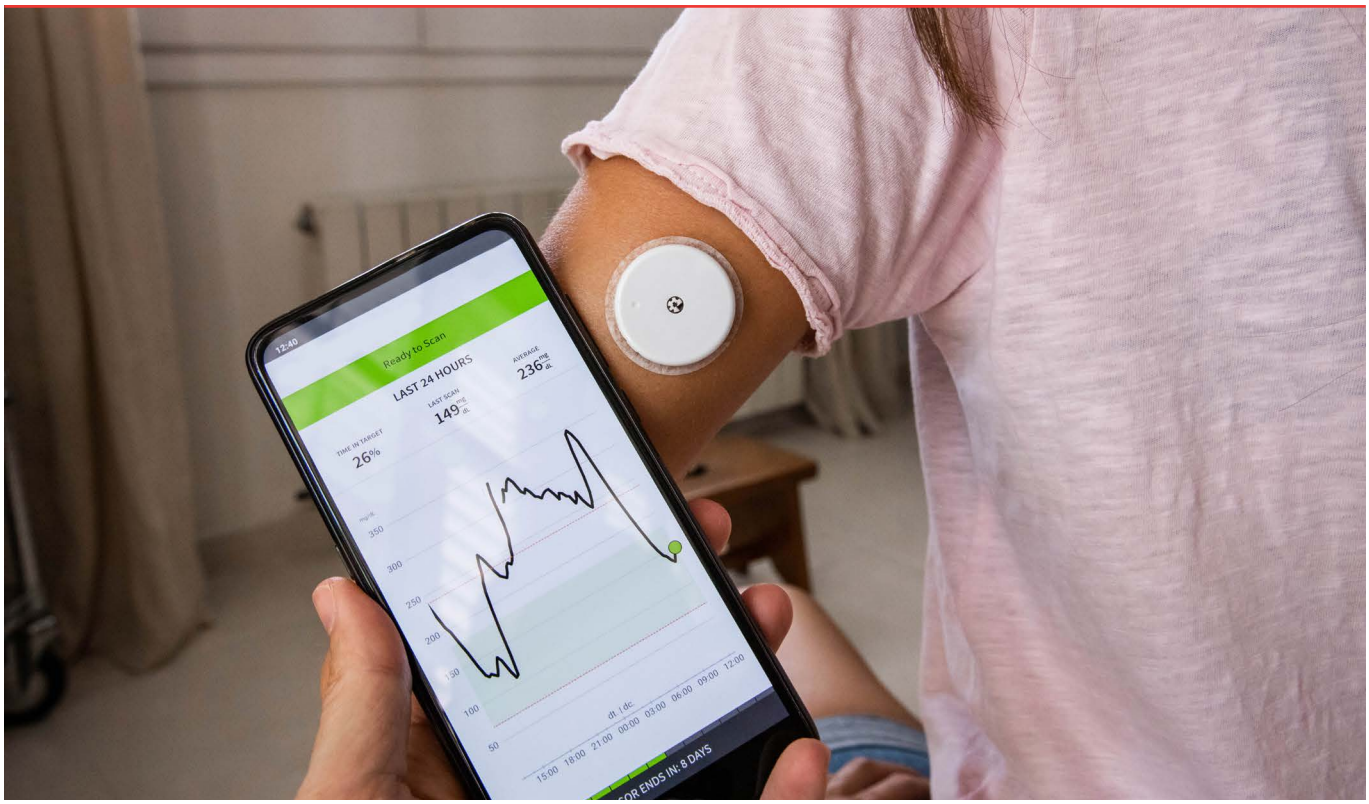
Table 2 – Definitions related to use from IEC 62366-1 [21]

Term	Definition
Abnormal use	Conscious, intentional act or intentional omission of an act that is counter to or violates normal use and is also beyond any further reasonable means of user interface-related risk control by the manufacturer **Examples:** Reckless use or sabotage or intentional disregard of information for safety are such acts **Note:** An intended but erroneous action that is not abnormal use is considered a type of use error. Abnormal use does not relieve the manufacturer from considering non-user interface-related means of risk control
Correct use	Normal use without use error
Normal use	Operation, including routine inspection and adjustments by any user, and stand-by, according to the instructions for use or in accordance with generally accepted practice for those medical devices provided without instructions for use **Note:** Normal use should not be confused with intended use. While both include the concept of use as intended by the manufacturer, intended use focuses on the medical purpose while normal use incorporates not only the medical purpose, but maintenance, transport, etc. as well
Use error	User action or lack of user action while using the medical device that leads to a different result than that intended by the manufacturer or expected by the user **Note:** User error includes the inability of the user to complete a task. Use errors can result from a mismatch between the characteristics of the user, user interface, task or use environment. Users might be aware or unaware that a use error has occurred. An unexpected physiological response of the patient is not by itself considered use error. A malfunction of a medical device that causes an unexpected result is not considered a use error
User	Person interacting with (i.e. operating or handling) the medical device
User interface	Means by which the user and the medical device interact **Note:**User interface includes all the elements of the medical device with which the user interacts, including the physical aspects of the medical device as well as visual, auditory, tactile displays and is not limited to a software interface

Definitions related to use from the international standard for usability engineering IEC 62366-1 [21] are given in Table 2. The different kinds of use and misuse are illustrated in the diagram of Figure 3. Correct use of the medical device includes the documented intended use, i.e. the medical purpose for which the device is intended to be used and also other uses that are necessary but not directly for medical purposes, such as maintenance, calibration, transport, stand-by, etc.

Figure 3 – Different kinds of use and misuse of a medical device considered in usability engineering and risk management





Some forms of misuse can be foreseen based on readily predictable human behaviour and are called reasonably foreseeable misuse in BS EN ISO 14971 [1] (see Table 1). The manufacturer needs to document the reasonably foreseeable misuse and consider it in the risk management process as well. Such misuse can be a use error which is performed unintentionally. However, use error can also arise from an intentional action, for example when the user consciously presses a button which appears to be the wrong button. Since errors can normally occur, both use error and correct use are considered to be part of normal use. Risks related to use error can be analysed and evaluated using a usability engineering process, such as the one described in IEC 62366-1 [21]. Those risks can often be controlled effectively in the user interface (see definition in Table 2). It has to be recognized, however, that some risks related to use error cannot be reduced sufficiently in this way and may need further control by other measures outside the user interface. Therefore, the results of the usability engineering process have to be fed back into the risk management process of BS EN ISO 14971. Reasonably foreseeable misuse can also include instances of abnormal use, which are not regarded as use error and cannot be controlled in the user interface. Abnormal use is a term from usability engineering (see Table 2) and concerns, for example, the intentional use of the medical device for an application that is unspecified or unintended by the manufacturer. This is sometimes called 'off-label use'. Other intentional acts like sabotage cannot be foreseen by any reasonable means and are also part of abnormal use. Those acts can be outside the scope of risk management and are usually not included in the reasonably foreseeable misuse. But this is not a fixed rule, because breaches of data and systems security by hackers can be regarded acts of sabotage but can also be reasonably foreseen.

The second step in the risk analysis is identifying the characteristics of the medical device that can affect its safety. Such characteristics can be related to the performance or the operating principle of the medical device, its intended use or reasonably foreseeable misuse. This can concern among others the materials used in parts coming into contact with the patient, moving parts, the use of radiation for diagnosis or treatment, the accuracy of measurements, the need for calibration or maintenance, the security of data or the required skills of the user. These characteristics need to be considered in the risk management process. The characteristics can be qualitative or quantitative and it may be necessary to establish limits that should not be exceeded. An extensive list of questions that can assist the manufacturer in identifying the characteristics related to safety is contained in ISO/TR 24971 [2]. It is emphasized that those questions are examples and the list should not be used as a checklist.

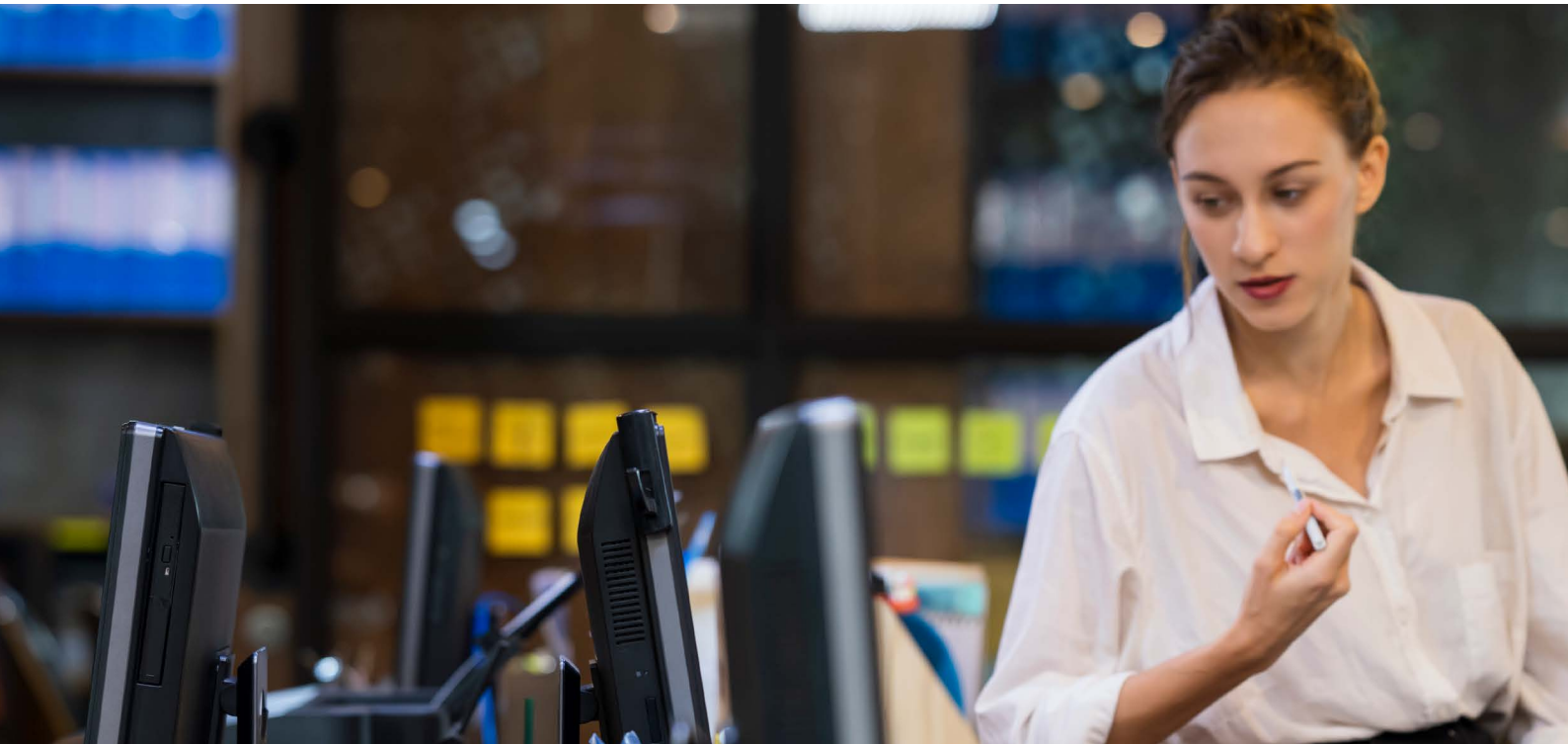
The third step is identifying the hazards associated with the medical device and identifying the reasonably foreseeable sequences or combinations of events that can lead to hazardous situations. It is important to consider the medical device not only in its normal condition, but also when a defect is present or in a fault condition that could occur. The intended use, the reasonably foreseeable misuse and the characteristics related to safety are important inputs in this step. It has to be emphasized that different sequences of events can lead from one hazard to different hazardous situations, and that one hazardous situation can lead to different kinds and severities of harm depending on the circumstances. These situations need to be considered as separate risks and should not be combined and assessed together.

The fourth and final step in the risk analysis is estimating the risk for each of the identified hazardous situations. The severity of any possible harm and the probability that this harm occurs need to be estimated. The probability of occurrence of harm (P) can be decomposed into the probability that a hazardous situation occurs (P1) and the probability that the hazardous situation leads to harm (P2). Such decomposition ($P = P1 \times P2$) can be helpful but is not mandatory. Data and experience with previous or similar medical devices on the market can be useful in estimating the risks, either qualitatively or quantitatively. A risk chart as shown in Figure 2 can be useful in risk estimation.

All hazardous situations and all kinds of harm need to be considered, not only the worst-case scenarios with the highest severity of harm, because scenarios with less severe harm could have a higher probability of occurrence and could thus lead to a higher risk.

Risk evaluation is also part of risk assessment. It is the step where the estimated risks are evaluated using the criteria for risk acceptability as defined in the risk management plan. The criteria for risk acceptability are established based on the policy defined by top management and are documented in the risk management plan. The criteria can incorporate the concept that risks have to be reduced as far as possible (see earlier section on top management responsibilities). The conclusions of the evaluation are documented in the risk management file. If the risk is judged acceptable, the estimated risk becomes the residual risk. If the risk is not judged acceptable, it is mandatory to perform risk control.

Experience shows that there is confusion about estimating risk when a particular risk control measure is always part of the medical device design. In this case it is sufficient to estimate and evaluate the risk after implementation of the risk control measure. It is not useful and therefore discouraged to estimate the (theoretical) risk for a medical device without the particular risk control measure in place, because it has become an integral part of the medical device design.



Risk control (process step 3)

The manufacturer has several risk control options for eliminating or reducing risks to an acceptable level. Many international standards provide specific technical solutions to address particular risks. Those standards should be considered in selecting the most appropriate options.

- The first and preferred option is to eliminate the risk by making the design of the medical device and its manufacturing process inherently safe. This ensures that a hazardous situation cannot occur. This is often related to the operating principle of the medical device. Examples include designing medical devices for single use such that they cannot be reused, designing medical electrical equipment such that live parts and high-voltage parts cannot be touched, and designing surfaces without sharp edges.

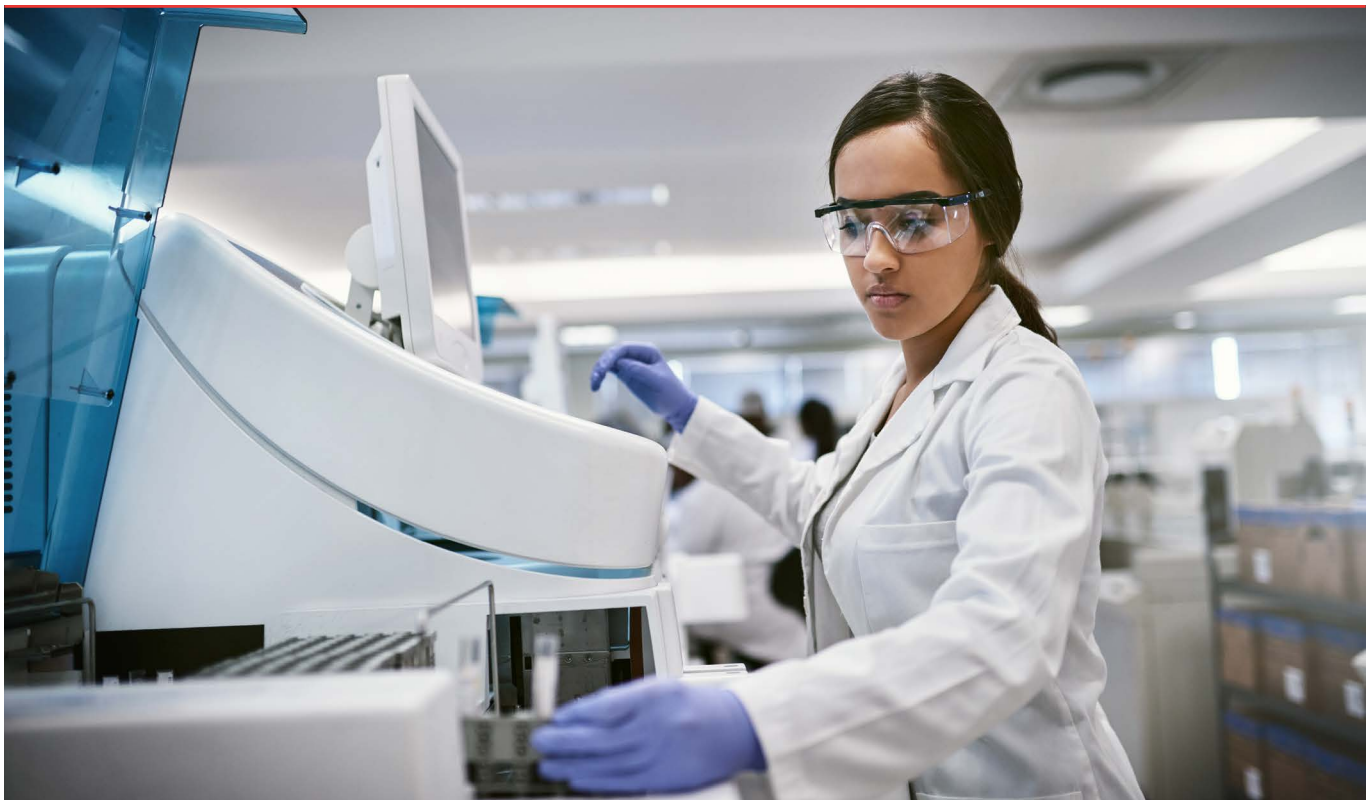
- If this is not possible, the second option is to implement protective measures in the design of the medical device or in the manufacturing process. Such measures can reduce the probability of occurrence of a hazardous situation or harm and/or the severity of the harm. Examples of such measures include gloves and special clothing to protect against contamination, covers to protect against electrical shock, barriers to prevent collision or trapping between moving parts, lead aprons and screens to protect against radiation. Protective measures also include alarms to alert people of a hazardous situation needing immediate attention to avoid any harm from occurring.

- If protective measures do not sufficiently reduce the risk, the third option is to provide information for safety to the users of the medical device. The information for safety can be given in the form of warnings or contraindications, or as instructions how to handle and use the medical device. This information can concern in particular actions that the user needs to take or to avoid to prevent the occurrence of a specific hazardous situation or harm. Some examples are warnings against reuse of single-use medical devices, warnings for high voltage, high temperature or radiation, instructions to use personal protective equipment, and instructions for calibration and maintenance of medical devices performing measurements. Training of users can be an important means of providing the information for safety.

The risk control measures selected have to be implemented, and the implementation verified. This can be done as part of design and development verification in a quality management system. The effectiveness of the risk control measures implemented also have to be verified, which can be done as part of design and development validation in a quality management system. The results of these verifications are documented in the risk management file.

After implementation of the risk control measures, the residual risk has to be estimated and evaluated again using the criteria for risk acceptability. If the risk is not judged acceptable, it is necessary to consider more risk control. These iterations are indicated in Figure 1 with the arrows back and forth between risk control and risk assessment. If, after careful analysis, it is concluded that further risk control is not practicable, the manufacturer may perform a benefit–risk analysis. Data and literature can be gathered and analysed to determine if the benefits of using the medical device outweigh the residual risk. If this is not the case, the manufacturer needs to go back in the process and consider to modify the medical device or to restrict the intended use (for example, to exclude vulnerable patient groups). Otherwise, the risk remains unacceptable and the medical device development needs to be abandoned.

Completeness is an important aspect in risk management. Therefore, the manufacturer is required to check that all identified hazardous situations have been addressed and all risk control activities have been completed. In addition, it has to be checked that the selected and implemented risk control measures do not introduce new risks and do not affect other risks.



Evaluation of overall residual risk (process step 4)

When one arrives at this process step, all individual risks have been controlled and judged acceptable. In some cases, a benefit–risk analysis has been performed with the conclusion that the benefits outweigh a particular risk. Although each risk is acceptable, it is important to also consider the contributions of all risks together (i.e. the overall residual risk). The reason is that the combination of several small risks could pose an unexpected big risk. For example, there could be too many risks in the yellow area of Figure 2 that were each investigated and for which no further risk reduction is possible. Another example is a particular risk control measure that is designed to control two independent risks simultaneously, which could be deemed unacceptable.

The clause on the evaluation of the overall residual risk has undergone considerable change in the third edition of BS EN ISO 14971 [1]. The second edition provided for a two-step approach, where the overall residual risk was first evaluated against the acceptability criteria. Second, if the overall residual risk was not judged acceptable, the manufacturer could gather data and literature to determine if the benefits of using the medical device would outweigh the overall residual risk. In this approach it was unclear which criteria for risk acceptability should be used and if the benefits of the intended use should or could also be considered in the first evaluation. Further, it was not clear which individual risks should be included in the evaluation of the overall residual risk.

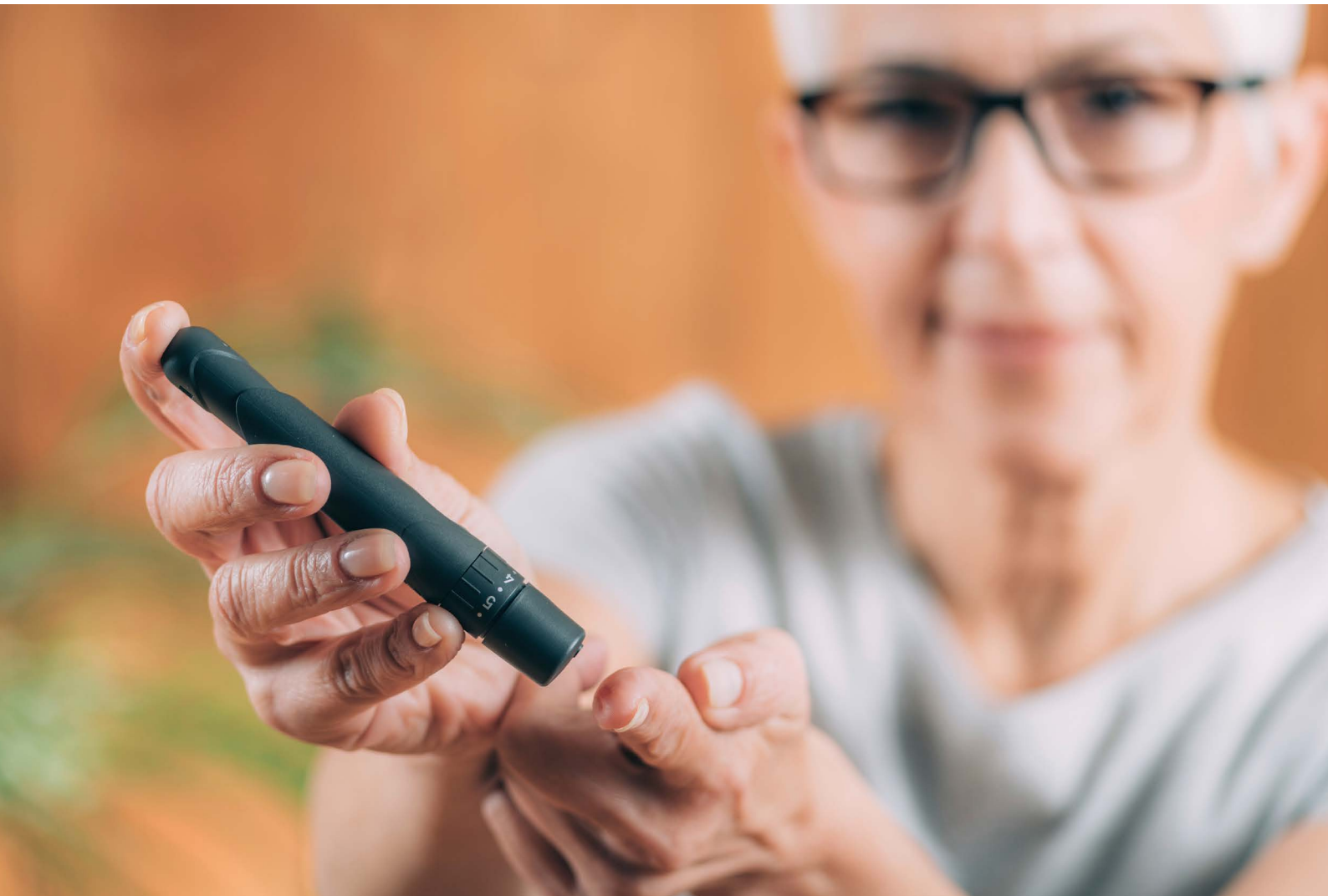
The two-step approach is replaced with one evaluation in the third edition of BS EN ISO 14971. It is required that the contributions of all individual residual risks are taken into account, and that the overall residual risk is evaluated in relation to the benefits of the intended use of the medical device. The manufacturer is required to document the evaluation method and the criteria for acceptability of the overall residual risk in the risk management plan. This ensures an objective evaluation. The method can include gathering data and literature for similar medical devices available on the market and judgement by a cross-functional team of experts with knowledge of and experience in application of the medical device.

ISO/TR 24971 [2] provides further guidance on possible approaches that can be used in the evaluation and on inputs and other considerations that can be taken into account. It is explained that the criteria for acceptability of the overall residual risk can be different from the criteria for acceptability of individual risks. In any case, these criteria have to be based on the manufacturer's policy for acceptable risk. If the overall residual risk is not judged acceptable, the manufacturer needs to go back in the process and apply additional risk control measures. These iterations are indicated in Figure 1 with the arrows back and forth between risk control and evaluation of overall residual risk. The manufacturer can also consider to modify the medical device or to restrict the intended use (for example, excluding vulnerable patient groups). Otherwise, the overall residual risk remains unacceptable and the medical device development needs to be abandoned.

The manufacturer is instructed to inform users of any significant residual risks and to disclose those risks by providing relevant information in the accompanying documentation. Since BS EN ISO 14971 [1] focuses on risks related to the design of the medical device and how the manufacturer can control them, it is important to disclose the residual risks inherent to the use of the medical device after all risk control measures have been implemented. The residual risks can relate to side-effects or after-effects of using the medical device in a particular procedure, for example, erythema, that can occur after radiation therapy, patients experiencing blood in their urine after lithotripsy of kidney stones and swelling or inflammation of the eye after ophthalmic surgery. The disclosed information enables the user to make informed decisions on whether to use this medical device in a particular situation or to choose for a different medical device, taking account of the condition of the individual patient. The disclosure of residual risks needs to be distinguished from information for safety, which is a risk control measure. While the disclosure of residual risk is descriptive and provides the user with information on risks inherent to the use of the medical device, information for safety is instructive and provides the user with information on how to use the medical device and on actions to take or to avoid to prevent a particular hazardous situation or harm from occurring. ISO/TR 24971 [2] provides further guidance on information for safety and the disclosure of residual risk.

Risk management review (process step 5)

As emphasized before, completeness is an important aspect of risk management. Therefore, after the design and development of the medical device and before its commercial distribution, BS EN ISO 14971 requires the manufacturer to review that the risk management plan was properly executed and appropriately implemented. It also needs to be ensured and recorded that the overall residual risk is acceptable. Methods to collect and review production and post-production information need to be in place before the medical device is finally released and placed on the market. The results of this review are documented as the risk management report, which forms a crucial part of the risk management file. The risk management report is signed off by persons with the appropriate authority and serves as the high-level document providing evidence that the risk management plan has been satisfactorily executed and the objectives have been achieved. Information from the production and post-production phases could reveal the need to adapt and improve the medical device during its life cycle and thus also to update the risk management report.



Production and post-production activities (process step 6)

The clause on production and post-production information has undergone considerable modification in the third edition of BS EN ISO 14971 [1]. The principles of collecting and reviewing information have not changed, but the requirements and the activities are described more elaborately and more precisely. The clause is divided into four sections corresponding to the steps that the manufacturer needs to take.

- The first step is to establish a system to collect and review relevant production and post-production information. This system must include appropriate methods for the collection and processing of data, which can include statistical methods for trend analysis. The system can be integrated with the monitoring and feedback processes required by a quality management system. The necessary activities to set up the system for collecting and reviewing information has to be included in the risk management plan.

- The second step is to collect relevant information for the medical device under consideration. A non-exhaustive list of sources is given in the standard, including information from users, from the supply chain and on the generally acknowledged state of the art (such as new or revised standards, alternative medical devices or alternative therapies). Publicly available information about similar medical devices and similar other products on the market should be considered as well. Those other products are not necessarily medical devices, but they can have a similar (non-medical) application or similar operating principles. It is required that the manufacturer actively collects the information and does not wait passively until such information becomes known.

- The third step is to review if the information is relevant to the safety of the medical device. In particular, the manufacturer needs to determine whether a previously unidentified hazard or hazardous situation exists, an estimated risk is no longer acceptable, the benefits of the medical device no longer outweigh the overall residual risk, or the generally acknowledged state of the art has changed. For example, the benefit in practice could appear to be less than anticipated or new technologies could have become available with smaller associated risks. In such cases, it needs to be investigated whether the medical device under consideration still has a favourable benefit-risk balance.

- If any of the above situations occurs, the manufacturer needs to take action. This is the fourth step. The required actions are described in more detail in the third edition of the standard. The manufacturer has to review the risk management file for the medical device and determine if any new risk needs to be assessed or any previously estimated risk needs to be assessed again, and if it is necessary to implement additional risk control measures. Actions regarding medical devices already on the market can be required as well. The manufacturer has to also evaluate the impact on the risk management activities that were previously performed. This evaluation can provide valuable input for top management when they review the suitability of the risk management process.

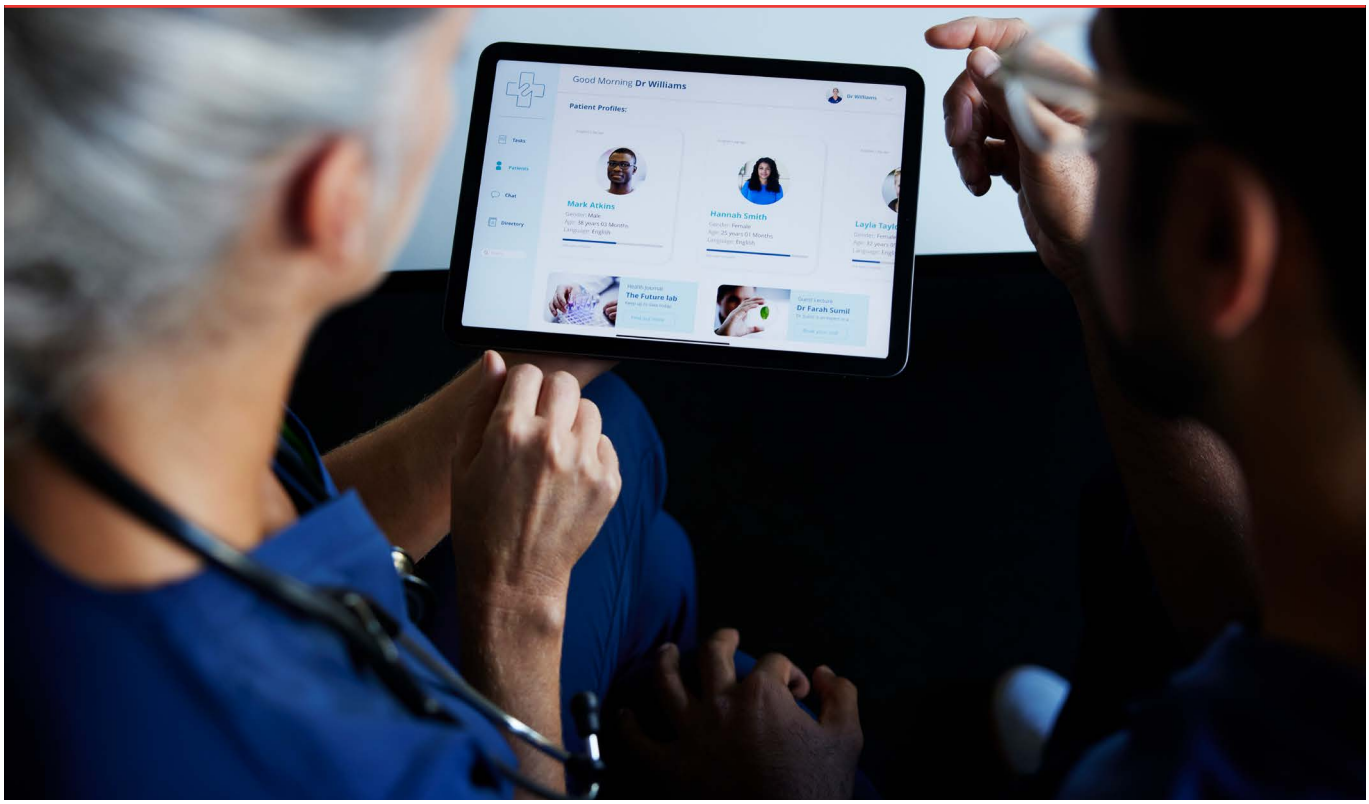
Relation of BS EN ISO 14971 with other standards

Other standards for medical devices and processes

BS EN ISO 14971 [1] provides a generic process for risk management of all kinds of medical devices, applicable to the entire life cycle from design and development through production and post-production until decommissioning and disposal. The standard is primarily aimed at medical device manufacturers, but it can also be used by other parties involved in the life cycle of the medical device such as suppliers. It can also be applied to other products that are not necessarily considered as medical devices in all jurisdictions but that can be subject to medical-device regulations or similar regulations, such as the products without an intended medical purpose listed in Annex XVI of the EU MDR [6]. Due to its generic character, BS EN ISO 14971 needs to be applied in combination with other process standards and device-specific standards in order to ensure the safety of the medical device and to demonstrate compliance with all regulatory requirements.

As indicated above in Risk assessment (process step 2) where reasonably foreseeable misuse was discussed, it is important to investigate use errors in the medical device development. The kind and type of use errors are difficult to predict, as is the probability that they will actually occur. The usability engineering process described in IEC 62366-1 [21] can replace some steps in the risk management process, because this standard provides dedicated methods to identify hazardous situations related to use error and to evaluate the effectiveness of the risk control measures in the user interface of the medical device. Similarly, other process standards can be used in conjunction with BS EN ISO 14971. For example, BS EN ISO 10993-1 [22] provides the general principles of and a process for the evaluation of biological risks of materials expected to come in contact with the patient or the user of the medical device. BS EN ISO 14155 [23] applies to the clinical investigation of medical devices on humans and provides the principles for good clinical practice. This includes ethical considerations, responsibilities of the parties involved and requirements for planning, conduct, recording and reporting of clinical investigations. IEC 62304 [24] defines a common framework for the life-cycle processes of medical device software, which can be embedded software intended to be incorporated in a medical device or standalone software intended to be used as a medical device. This framework includes requirements for development and maintenance planning, documentation, classification and risk management.

Device-specific standards need to be applied together with BS EN ISO 14971. These standards can be regarded as representing the generally acknowledged state of the art, providing technical solutions to control specific risks that are typical for the given category of medical devices. Compliance with such standards can be used to deduce that the corresponding risks are reduced to acceptable levels, unless there is objective evidence to the contrary. Many device-specific ISO standards exist for a wide range of (mostly non-electrical) medical devices and their components. Also, there are many particular standards – IEC 60601-2-x and IEC/ISO 80601-2-x – for the basic safety and essential performance of medical electrical equipment. Each of these particular standards applies to a specific category of medical electrical equipment and has been developed as a dedicated version of the general safety standard IEC 60601-1 [25]. The manufacturer needs to consider which combination of process standards and device-specific standards is appropriate for the medical device or medical equipment that is being developed.

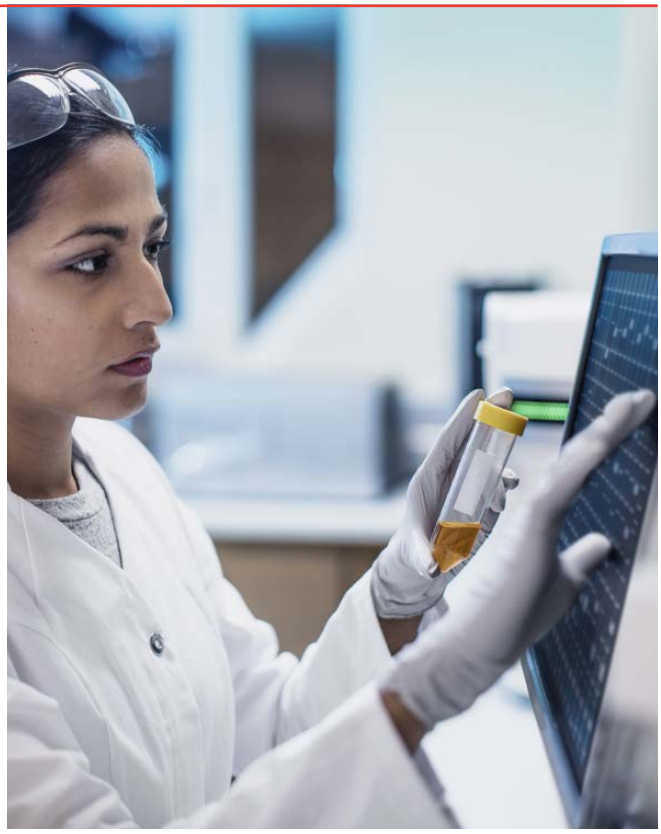


Other standards and guides for safety and risk management

As a risk management standard, the purpose of BS EN ISO 14971 [1] is to assist manufacturers in achieving safety (i.e. freedom from unacceptable risks) for the medical devices that they develop and place on the market. BS EN ISO 14971 is based on ISO/IEC Guides 51 and 63. ISO/IEC Guide 51 [26] is addressed to writers of international standards for all sectors and provides guidelines on how to include safety aspects. ISO/IEC Guide 63 [27] provides guidelines on how safety aspects should be included in standards specifically for the medical device sector. This guide was developed based on ISO/IEC Guide 51 and is addressed to writers of international standards for medical devices. This was considered necessary in view of the high importance of safety and the strict regulatory requirements in this sector. The two standards expressing the essential principles for safety and performance of medical devices [17] and in vitro diagnostic medical devices [18] are based on BS EN ISO 14971 and ISO/IEC Guides 51 and 63. Risk in all these documents is defined in terms of the probability of occurrence of harm and the severity of possible harm. In all safety standards directly or indirectly derived from ISO/IEC Guide 51, harm can be injury or damage to the health of people, but also damage to property or the environment (see Table 1). Thus, we can say that the concepts of risk in these documents are based on well-established safety principles.

The concepts and definition of risk in BS EN ISO 14971 are in strong contrast with those in ISO Guide 73 [28] (risk management vocabulary) and BS ISO 31000 [29] (risk management guidelines). Risk in [28, 29] is defined as the effect of uncertainties on (business) objectives. Since these effects can be positive or negative, the risk in the latter documents can be related to threats as well as opportunities. The guidelines in BS ISO 31000 are expressed in general, high-level language and are intended for business risk management and dealing with uncertainties. This makes BS ISO 31000 not suitable for applying safety principles and managing risks in product development. Nevertheless, one can recognize the typical process steps that are present in any risk management process [1, 10, 13, 26, 27]. However, the general guidelines of BS ISO 31000 need to be ‘translated’ carefully to each specific situation and each specific product being considered. For the application of risk management to medical devices, this translation has already been performed in ISO/IEC Guide 63 [27] and BS EN ISO 14971.

Conclusion



The science of risk management has developed and matured over the past centuries. This holds for all industry sectors including the medical device sector. It is now impossible to imagine that a medical device would be developed and placed on the market without thorough risk assessment or post-production monitoring. BS EN ISO 14971 [1] has established itself as the globally recognized standard for applying risk management to medical devices. It provides a complete and comprehensive process for manufacturers to identify hazards associated with the medical devices under development, to assess the risks involved, to control those risks and to monitor the effectiveness of the risk controls throughout the life cycle of the medical device. The companion report ISO/TR 24971 [2] provides guidance on the application of the standard.

The requirements in the third edition of BS EN ISO 14971 are aligned with the general safety and performance requirements of the European Regulations MDR [6] and IVDR [7] and are in accordance with the regulatory requirements for medical devices in most other jurisdictions. The requirements also support demonstrating compliance to the essential principles of safety and performance for medical devices and in vitro diagnostic medical devices [17, 18]. Therefore, BS EN ISO 14971 will continue to be the globally recognized risk management standard. Further, the third edition of BS EN ISO 14971 has been harmonized and listed in the Official Journal of the European Union as providing a presumption of conformity to the European MDR and IVDR without content deviations.

References

1. ISO 14971, *Medical devices – Application of risk management to medical devices* (Edition 1:2000, 2:2007, 3:2019)
2. ISO/TR 24971, *Medical devices – Guidance on the application of ISO 14971* (Edition 1:2013, 2:2020)
3. Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices (1990, last amended 2007)
4. Council Directive 93/42/EEC concerning medical devices (1993, last amended 2007)
5. Directive 98/79/EC of the European Parliament and of the Council on in vitro diagnostic medical devices (1998, last amended 2011)
6. Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices (2017)
7. Regulation (EU) 2017/746 of the European Parliament and of the Council on in vitro diagnostic medical devices (2017)
8. Covello, V.T. & Mumpower, J. (1985) Risk analysis and risk management: An historical perspective. *Risk Analysis*, 5, 103-120.
9. Zachmann, K. (2014) 'Risk in historical perspective: Concepts, contexts, and conjectures', in C. Klüppelberg, D. Straub and I.M. Welpe (eds.) Risk – *A Multidisciplinary Introduction*. Switzerland, Springer International Publishing.
10. Aven, T. (2016) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research,* 253, 1-13.
11. Ore, O. (1960) Pascal and the invention of probability theory. *The American Mathematical Monthly*, 67, 409-419.
12. Laplace (1814) *Théorie analytique des probabilités*, 2nd ed. Paris, Courcier Imprimeur-Libraire.
13. Department of Defense, *Military standard on system safety*. MIL-STD-882 (Edition A:1977, B:1984, C:1993, D:2000, E:2012)
14. International Civil Aviation Organization. Available from: https://www.icao.int
15. EN 1441, *Medical devices* – Risk analysis (Edition 1:1997, withdrawn)
16. ISO 14971-1, Medical devices – Risk management – Part 1: Application of risk analysis (Edition 1:1998, withdrawn 2000)
17. BS ISO 16142-1:2016, *Medical devices – Recognized essential principles of safety and performance of medical devices – Part 1: General essential principles and additional specific essential principles for all non-IVD medical devices and guidance on the selection of standards*
18. BS ISO 16142-2:2017, M*edical devices – Recognized essential principles of safety and performance of medical devices – Part 2: General essential principles and additional specific essential principles for all IVD medical devices and guidance on the selection of standards*
19. International Atomic Energy Agency (IAEA), *Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards*, General Safety Requirements, Part 3 (2014)
20. Council Directive 2013/59/EURATOM laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation (2013)
21. BS EN 62366-1:2015+A1:2020, *Medical devices – Part 1: Application of usability engineering to medical devices*

22. ISO 10993-1, *Biological evaluation of medical devices – Part 1: Evaluation and testing within a risk management process* (Edition 5:2018)

23. BS EN ISO 14155:2011, *Clinical investigation of medical devices for human subjects – Good clinical practice*
24. BS EN 62304:2006+A1:2015, *Medical device software – Software life cycle processes*

25. IEC 60601-1, *Medical electrical equipment – Part 1: General requirements for basic safety and essential performance* (Edition 3:2005, Amendment 1:2012)

26. ISO/IEC Guide 51, Safety aspects — *Guidelines for their inclusion in standards* (Edition 1:1990, 2:1999, 3:2014)

27. ISO/IEC Guide 63, *Guide to the development and inclusion of safety aspects in International Standards for medical devices* (Edition 1:1999, 2:2012, 3:2019)

28. 2ISO Guide 73, Risk management – *Vocabulary* (Edition 1:2009)

29. BS ISO 31000:2018, *Risk management – Guidelines*

Author

Jos van Vroonhoven, Senior Manager Standardization, Philips, The Netherlands

Jos has had a 30-year career with Philips in The Netherlands, of which 15 years have been spent in Research and Development and 15 years in Healthcare. He became increasingly involved in the application of x-ray safety standards when working as a radiation protection specialist. He participated in several IEC working groups to develop IEC 60627 (anti-scatter grids), IEC 60601-2-54 (x-ray diagnostic equipment), IEC/TR 60601-4-1 (equipment with a degree of autonomy) and the first amendment to IEC 60601-1. In his current position, Jos focuses on international and European standardization for medical electrical equipment in IEC, ISO, CEN and CENELEC. He is chair of the NEN national mirror committee for IEC/TC 62 and its subcommittees and an expert member of the national mirror committee for ISO/TC 210. Since 2016 he is also the convener of Joint Working Group 1 (JWG1) between ISO/TC 210 and IEC/SC 62A on the application of risk management to medical devices, working on the revision of ISO 14971 and ISO/TR 24971. JWG1 has also prepared ISO/IEC Guide 63 with guidance for standards writers on the inclusion of safety aspects in international standards for medical devices.

Reviewers

Jane Edwards, Head of Communications, Global Product Management, BSI

Jane holds a BSc in Chemistry and an MBA from Durham University. She has over 13 years' experience in the medical device industry, having previously worked for Coloplast in their ostomy and continence business. Jane's experience includes working within the pharmaceutical, chemical and telecoms industries for Glaxo Wellcome, ICI and Ericsson, allowing her to bring depth of knowledge from across many industries and technologies. Her current role in BSI allows her to work with technical reviewers across all disciplines ensuring that all BSI communications are accurate and relevant. She is a member of the European Medical Writers Association.

Jeremy Tinkler, Director of Regulatory Consultancy and Quality Assurance, MedPass International SAS, Paris

Jeremy joined MedPass International, a Clinical Research Organisation and regulatory consultancy, in 2007 after 20 years at MHRA, where he was Principal Specialist in Biosciences and Implants. Since 1987, he has taken a leading role in the development of international standards in risk management, biological safety, clinical investigation and implants, and MEDDEV 2.7/1 on clinical evaluation. He has been involved in writing risk management standards since the 1990s and is Chairman of ISO Technical Committee 194 (biological and clinical evaluation), responsible for ISO 14155 and ISO 10993.

Paul Sim, Medical Devices Knowledge Manager, BSI Standards

Paul has worked in the healthcare industry for over 35 years, joining BSI in 2010 to lead the organization in Saudi Arabia where it had been designated as a Conformity Assessment Body. Later, he managed BSI's Unannounced Audits programme. Since October 2015, he has been working with both the Notified Body and Standards organizations looking at how best to use the knowledge, competencies and expertise in both. Previously he held senior RA/QA leadership positions at Spacelabs Healthcare, Teleflex Medical, Smiths Medical and Ohmeda (formerly BOC Group healthcare business). Paul is a member of the Association of British Healthcare Industries (ABHI) Technical Policy Group and Convenor of the ABHI ISO TC 210 Mirror Group. He is Convenor of the BSI Committee that monitors all of the work undertaken by ISO TC 210, and Convenor of the BSI Subcommittee dealing with quality systems. As UK Delegation Leader to ISO TC 210, he is also actively involved in the work of national, European and international standards' committees.

Eamonn Hoxey, Director, E V Hoxey Ltd

Eamonn is a technical author, trainer and consultant in a range of life science areas including regulatory compliance, quality management, sterility assurance and standards development. He worked for Johnson & Johnson for 17 years in positions of increasing responsibility for Quality and Regulatory Compliance for medical devices, pharmaceuticals and consumer products, including Vice President of Compliance, Vice President of Market Quality and leading quality implementation for the EU medical devices regulation for J&J's Medical Devices companies. Prior to joining J&J, Eamonn spent 16 years with the UK Medical Devices Agency, including six years as Head of Device Technology and Safety. Eamonn is currently chair of ISO TC 198, Sterilization of Healthcare products, chair of CEN TC 204 'Sterilization of medical devices' and past chair of ISO TC 210 'Quality management and related general aspects for medical devices'. He received the BSI Wolfe-Barry medal in 2016 for his contribution to standards development.

Published white papers

- *The growing role of human factors and usability engineering for medical devices: What's required in the new regulatory landscape?* Bob North
- *The differences and similarities between ISO 9001:2015 and ISO 13485:2016: Can we integrate these quality management standards?* Mark Swanson
- *Planning for implementation of the European Union Medical Devices Regulations – Are You Prepared?* Eamonn Hoxey
- *Cybersecurity of medical devices: Addressing patient safety and the security of patient health information,* Richard Piggin
- *The European Medical Devices Regulations: What are the requirements for vigilance reporting and post-market surveillance?* Eamonn Hoxey
- *General Safety and Performance Requirements (Annex 1) in the New Medical Device Regulation: Comparison with the Essential Requirements of the Medical Device Directive and Active Implantable Device Directive,* Laurel Macomber and Alexandra Schroeder
- *Do you know the requirements and your responsibilities for medical device vigilance reporting? A detailed review on the requirements of MDSAP participating countries in comparison with the European Medical Device Regulation 2017/745,* Cait Gatt and Suzanne Halliday
- *Technical Documentation and Medical Device Regulation: A Guide for Manufacturers to Ensure Technical Documentation Complies with EU Medical Device Regulation 2017/745,* Dr Julianne Bobela, Dr Benjamin Frisch, Kim Rochat and Michael Maier
- *Nanotechnology: What does the future look like for the medical devices industry?* Professor Peter J Dobson, with Dr Matthew O'Donnell 23
- *Developing and maintaining a quality management system for IVDs,* Melissa Finocchio
- *Recent advancements in AI – implications for medical device technology and certification,* Anil Anthony Bharath
- *The impact and potential for 3D printing and bioprinting in the medical devices industry,* Kenny Dalgarno
- *Sterilization – Regulatory requirements and supporting standards, Eamonn Hoxey*
- *Medical device clinical investigations – What's new under the MDR?* Maria Donawa
- *The convergence of the pharmaceutical and medical devices industries: Navigating the innovations and regulations,* Barbara Nasto and Jonathan Sutch
- *Phthalates and endocrine disruptors – An overview of their safety requirements and evaluations and the standards that support them,* Benjamin Seery
- *European Union Medical Device Regulation and In Vitro Device Regulation: unique device identification: What is required, and how to manage it,* Mary Gray
- *Person responsible for regulatory compliance (PRRC) – MDR/IVDR Article 15: An overview of the requirements and practical considerations,* Anne Jury and Maddalena Pinsi
- *Guidance on MDCG 2019-9: Summary of Safety and Clinical Performance,* Amie Smirthwaite
- *Clinical evaluation under EU MDR,* Amie Smirthwaite
- *Medical device clinical investigations — What's new under the MDR? An update,* Maria Donawa
- *Using Standards to Demonstrate conformity with Regulations,* Eamonn Hoxey

Forthcoming white papers

- *Requirements of EU-GDPR and PMCF studies, registries and surveys under the MDR (working title),* Richard Holborow
- *Performance Evaluation for IVD,* Fiona Gould

About BSI Group

BSI (British Standards Institution) is the business standards company that equips businesses with the necessary solutions to turn standards of best practice into habits of excellence. Formed in 1901, BSI was the world's first National Standards Body and a founding member of the International Organization for Standardization (ISO). Over a century later it continues to facilitate business improvement across the globe by helping its clients drive performance, manage risk and grow sustainably through the adoption of international management systems standards, many of which BSI originated. Renowned for its marks of excellence including the consumer recognized BSI Kitemark™, BSI's influence spans multiple sectors including aerospace, construction, energy, engineering, finance, healthcare, IT and retail. With over 70,000 clients in 150 countries, BSI is an organization whose standards inspire excellence across the globe.

BSI is keen to hear your views on this paper, or for further information please contact us here: julia.helmsley@bsigroup.com

This paper was published by
BSI Standards Ltd

For more information please visit:
bsigroup.com/en-GB/our-services/medical-device-services/BSI-Medical-Devices-Whitepapers/

bsi.

Read more about our services and products on our website