The “Official” Guide to Software Audits

The “Official” Guide to Software Audits

Software audits step by step:
A checklist for manufacturers and auditors of medical software

Prof. Dr. Christian Johner and Sven Wittorf

Johner Institut GmbH
www.johner-institut.de
Phone: +49(0)7531 94500 -20
Email: info@johner-institut.de

Christian Johner und Sven Wittorf

Johner Institut GmbH

Konstanz

Germany

ISBN 978-3-948117-04-7

The German National Library lists this publication in the German National Bibliography; detailed bibliographic data are available at dnb.dnb.de.

The publisher and the authors assume that the data and information in this work are complete and correct at the time of publication. Neither the publisher nor the authors accept any liability for the content of the work, any errors or statements.

Editorial: Vera Palmer, Berlin

Typesetting: Datagrafix GmbH, Berlin

Production: NEUNPLUS1-Verlag+Service, Berlin

Printed in EU

New regulatory requirements

With the first edition of the guide, many medical device manufacturers successfully mastered their audits and approvals. As there have been numerous regulatory changes, we are happy to present a new edition of this guide.

The following examples illustrate which new and amended regulatory requirements manufacturers must take into account:

- The EU has replaced the previous EU directives with EU regulations **(MDR and IVDR)** and has significantly tightened the requirements.
- All relevant **standards** have been published in new versions, which entail significant changes. This concerns IEC 62304 as well as IEC 62366 1. Some Notified Bodies also demand conformity with IEC 82304, although there is no legal basis for this.
- The **FDA** has created many new **guidance documents**, and revised existing ones.
- The requirements of the **General Data Protection Regulation (GDPR)** affect manufacturers of medical devices at least indirectly, whilst affecting their customers, the operators, directly.

Technological trends

Current technologies — especially their application and effects on daily life — were barely conceivable as recently as the mid-2000s. These technologies find applications in medical devices:

- The issue of **IT security** has become substantially more important in recent years. Many best practice guidelines have been developed, and EU regulations explicitly demand IT security.
- Since 2018, medical devices based on **artificial intelligence**, in particular machine learning, have become state-of-the-art. A consensus on the specific requirements for these products has yet to be established.
- Both the MDR and IVDR have recognized the specific challenges and risks that arise and have to be overcome by **mobile platforms** (smartphones, tablets, wearables, etc.). The same applies to the **networking** of medical devices with each other, and of medical devices with other products and systems, including cloud storage.

Integration of the guidelines on IT security and artificial intelligence

The Johner Institut actively contributes to the establishment and standardization of best practices in order to make the advantages of technical progress available through medical devices without exposing patients to unacceptable risks. The active participation in standardization committees and the guidelines on both IT security and artificial intelligence bear witness to this.

These guidelines have been developed by the Johner Institut together with or on behalf of Notified Bodies such as TÜV SÜD. They are already incorporated into this audit checklist.

New area of focus: “Post-market” activities

This second version of the checklist also takes into account the more specific requirements for **post-market surveillance**, **clinical evaluation**, and **post-market clinical follow-up**.

Digital version of the guide

In order to be able to cater for the rapid changes, the Johner Institut is making a **digital version of this guide** available. Details can be found at www.johner-institut.de.

How to benefit from this book

Would you like to quickly check how likely you are to pass the next audit without studying the standards?

This book will help you do just that. You will gain certainty regarding audits and be able to both detect and correct possible deviations at an early stage. This is going to save you money and time, because you will avoid unpleasant repetition of audits or reworking, not to mention damage to your department's image.

This guide will also save you having to read the laws and standards in detail. It summarizes the requirements in the order that is important to you. For example, you will find a summary of the requirements of all development process standards. This book compiles all these requirements. Furthermore, it provides advice on how best to prove that you have met these claims when developing medical software. This saves you the tedious process of compiling the requirements yourself.

Please note: This book does not include requirements that are not related to software (e.g. those concerning the sterility of products). This makes this checklist compact and specific to medical software.

Every buyer of this book will receive a voucher for a free digital copy. This is a personalized PDF document which can be printed out as often as you like. Hence, you will be able to use the checklists in this book again and again.

Did you know that Notified Bodies also use this guide?

Your advantages at a glance

- Gaining certainty during the audit.
- Avoiding unpleasant complaints and costly reworking.
- Sparing the tedious interpretation of standards and laws.
- Gaining a quick overview thanks to easy-to-fill checklists.
- Identifying weak points quickly and correcting them before the audit.
- Acquiring a knowledge advantage, because Notified Bodies also use this guide.
- PDF version: Use the checklists as often as you like.

Benefit from a 50 % discount on all further editions, so that you can keep up to date.

Be prepared for the future

Regulatory requirements change, as do technologies and processes. This guide has been written to meet these changes meets:

- Buyers get a 50% discount on all future issues.
- Errata and a history of changes can be accessed on our website: www.johner-institut.de/auditleitfaden
- Depending on your membership, you can access the digital and continuously expanded version of the guide, use filters to extract the parts relevant to you and use them for your audits.

Stay up to date with the latest technology and regulations!

Aim of this document

When you are a person responsible for the development or quality assurance of medical software, this book will help you to optimally prepare for audits. This guide also supports auditors in their work, especially in the preparation and execution of audits.

This book does more than just consolidate and group legal claims. It transforms software-unspecific requirements into software-specific ones. It takes into account best practices and gives recommendations, some of which go beyond or are more concrete than the standard requirements. Conversely, there are some requirements of the standards that have not been considered in these checklists. This is, for example, due to the fact that these (few) requirements have or have had no relevance for audits. Requirements that are not related to software have not been included. This makes it possible to keep the checklists in this document both compact and specific to auditing medical software.

The goal of this book that both manufacturers and auditors of medical software can quickly access a representative overview of software life cycle process components. Emphasis is placed on identifying weaknesses in the development of medical software that are highly likely to lead to a loss of quality rather than on checking every single sentence of each standard.

Regulations taken into account

The focus of this document is on the auditing of medical software. However, this guide is not limited to the requirements of IEC 62304. It covers the complete development process, the technical documentation, and the relevant quality management requirements.

The checklists in this document also refer to hardware and contain aspects of IEC 60601-1.

This book considers all regulations relevant to medical software: directives, laws, and standards. These include in particular:

- Medical Device Regulation MDR (Regulation 2017/745 on Medical Devices)
- In Vitro Diagnostics Medical Device Regulation IVDR (Regulation 2017/746 on In Vitro Diagnostics)
- ISO 13485:2016 Quality Management Systems
- ISO 14971:2019 Risk Management
- IEC 62304:2015 Life Cycle Processes and Verification
- IEC 62366-1:2015 Serviceability
- Corresponding requirements of the FDA such as its guidance documents, e.g. General Principles of Software Validation, Human Factors Engineering, and Cybersecurity Guidance

As we are observing a convergence of medical information systems and systems in the pharmaceutical environment, some GxP-relevant documents have been considered, as there the GAMP Best Practice Guide: Testing of GxP Systems and PIC/S.

ISO 25010 specifies quality characteristics of software. Even though this taxonomy is not specific to medical software, this standard is still relevant: One reason is that Chapter 5.2 of IEC 62304 is based on it. Furthermore, the properties mentioned in ISO 25010 are generally valid, hence they should at least partly be included in these checklists.

Disclaimers

This document has been prepared to the best of our knowledge and belief. It is based on many years of experience in software development, the creation and review of quality management systems, and the training of software developers. Nevertheless, errors cannot be ruled out.

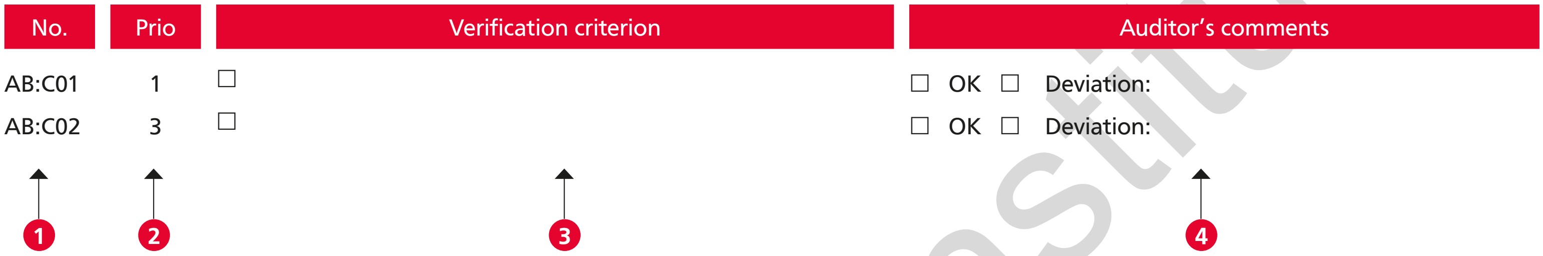
The document does not claim to be exhaustive. It has been compiled to serve as a guide for effective and efficient audits of software development departments.

The interpretation and transfer of normative and legal requirements to the development of medical software also has a subjective character. Nevertheless, the assignment of both is transparently presented.

The authors disclaim any liability, especially claims arising from the consequences of faulty medical software and its audits.

Acknowledgments

The authors would like to thank Christian Denger, Matthias Hölzer-Klüpfel, and all our loyal customers who have contributed to this guide.



No.	Prio	Verification criterion	Auditor's comments
AB:C01	1	□	□ OK □ Deviation:
AB:C02	3	□	□ OK □ Deviation:

The checklists are kept as compact as possible to allow efficient auditing. For this reason, the checklists are in tabular form:

1 **No.:** A unique number that can be referred to.

2 **Prio:** The priority represents the measure of how important it is that the verification criterion is met.

- **1:** High Priority. Violations of High Priority criteria are to be considered critical. They are in conflict with basic regulations or best practices and are typical causes of faulty software. In the case of infringements, an appropriate “assessment” is recommended, for example in the form of a deviation.
- **2:** Medium Priority. Violations of Medium Priority criteria must be justified. They are an indication that relevant regulations or best practices are not being followed. It is recommended to investigate the impact on the final product.
- **3:** Low Priority. Infringements of Low Priority criteria are not directly critical. However, a high number of such infringements can significantly affect the quality of the product. This should be discussed with the customer during the audit.

3 **Criterion for review:** Here, points which are to be understood as an indication of compliance with the criterion are listed. If only a few of the points apply, it must be assumed that the criterion has not been met, i.e. that a violation has occurred. Essential criteria are marked with an exclamation mark (!) Failure to meet such criteria makes compliance with the criterion unlikely. Most of the verification criteria include a reference. Here you will find further information, specifically the relevant chapters, sections, or paragraphs of the relevant standards and laws, as well as other best practices and regulations.

4 **Auditor's notes:** This is where the auditors (internal or external) enter their observations and evaluate whether the respective criterion is met.

The Big Checklist for Software Audits

INTENDED USE

No.	Prio	Verification criterion	Auditor's comments
	1	**Medical indication**	
ZB:A01		□ (!) The intended use is documented.[1]	□ OK □ Deviation:
ZB:A02		□ The intended use clearly refers to a product or a product version, e.g. by its UDI-DI.	□ OK □ Deviation:
ZB:A03		□ The intended use specifies the benefit of the product, e.g. whether it is used for diagnosis, therapy, alleviation, and/or monitoring.[2]	□ OK □ Deviation:
ZB:A04		□ The intended use specifies the indication, i.e. the diseases or injuries for which it is useful.[3, 4, 5]	□ OK □ Deviation:
ZB:A05		□ The intended use describes how the product serves the diagnosis, therapy or monitoring of diseases or injuries (or physiological or anatomical parameters) (e.g. physical principle).[6]	□ OK □ Deviation:
ZB:A06		□ The intended use specifies the circumstances (e.g. diseases) in which the use of the product is contraindicated.[7]	□ OK □ Deviation:
ZB:A07		□ (!) The intended use describes the intended patient group (including age, health status, weight).	□ OK □ Deviation:
ZB:A08		□ The intended use describes which body region or tissue is to be examined, diagnosed, treated, or monitored.	□ OK □ Deviation:

No.	Prio	Verification criterion	Auditor's comments
	2	**Users, context of use**	
ZB:B01		□ (!) The intended use characterizes the primary and secondary[8] user groups.[9]	□ OK □ Deviation:
ZB:B02		□ The characterization includes demographic features (age, gender) of the intended users.	□ OK □ Deviation:
ZB:B03		□ The characterization identifies the profession or function within the organization of the intended users.	□ OK □ Deviation:
ZB:B04		□ The characterization specifies necessary skills and knowledge of the intended users including education, language skills, special relevant skills, and experience with identical or similar products.	□ OK □ Deviation:
ZB:B05		□ The characterization describes possible physical or other limitations and characteristics of the intended users.	□ OK □ Deviation:
ZB:B06		□ The intended use describes the context of use[10] including core tasks, frequency of use, and results to be achieved.[11]	□ OK □ Deviation:
ZB:B07		□ The intended use specifies the intended location of the application[12] and, if relevant, the prevailing physical parameters such as brightness, temperature, volume, humidity, pollution, and air pressure.[13, 14, 15, 16, 17]	□ OK □ Deviation:
ZB:B08		□ The intended use characterizes the environment of use, e.g. stress level, shift work, emergency situations, wearing of gloves.	□ OK □ Deviation:
ZB:B09		□ The intended use documents whether the product is to be used in ambulances, helicopters, or medical rooms such as operating theaters.[18]	□ OK □ Deviation: