



# Der „offizielle“ Leitfaden für Software-Audits

Sicher durchs Audit:

Eine Checkliste für Hersteller und Auditoren medizinischer Software

Autoren: Prof. Dr. Christian Johner, Sven Wittorf

<b>Einführung</b>	4
Wie Sie von diesem Buch profitieren	4
Ziel dieses Dokuments	5
Berücksichtigte Vorschriften	5
Haftungsausschluss	6
<b>Vorbemerkungen zu den Checklisten</b>	7
<b>Die große Checkliste</b>	8
Entwicklungsprozess	8
Anforderungsanalyse	10
Funktionale Spezifikation („Software-Anforderungen“)	14
Architektur	16
Implementierung	19

Testen: Verifikation und Validierung	20
Risikomanagement	26
Versions-, Build-, Release- und Konfigurationsmanagement	24
Gebrauchstauglichkeit	37
Produkteigenschaften	38
Qualitätsmanagement	42
<b>Vorschlag für Auditplan</b>	47
<b>Weitere Checklisten</b>	48
Die kleine Checkliste für GxP Audits	48
Fragen und Beanstandungen bei FDA Audits	50
<b>Weiterführende Hinweise</b>	56
<b>Notizen</b>	62

**Wie Sie von diesem Buch profitieren**

„Würden Sie gerne schnell und ohne die Normen studieren zu müssen prüfen, wie wahrscheinlich es ist, dass Sie das nächste Audit bestehen?“

Genau dabei unterstützt Sie dieses Buch. Sie erlangen Sicherheit beim Audit und können mögliche Abweichungen frühzeitig erkennen und beheben. Das spart Geld und Zeit, denn Sie vermeiden unangenehme Wiederholungsaudits oder Nachbesserungen. Vom Imageschaden für Ihre Abteilung ganz zu schweigen.

Dieses Buch erspart Ihnen, die Normen im Detail lesen zu müssen. Es fasst Ihnen die Forderungen zusammen – in der Reihenfolge, die für Sie wichtig ist. So finden Sie beispielsweise die Forderungen aller Normen an den Entwicklungsprozess zusammengefasst. Dabei konsolidiert dieses Buch diese Forderungen nicht nur. Es gibt Ihnen auch Tipps, wie Sie bei der Entwicklung medizinischer Software am besten nachweisen, dass Sie diese Forderungen erfüllt haben. Das spart Ihnen das mühsame Zusammentragen.

Forderungen, die keinen Bezug zur Software haben (z.B. die Sterilität von Produkten betreffend), nennt dieses Buch nicht. Dadurch ist diese Checkliste kompakt und spezifisch für medizinische Software.

Jeder Käufer dieses Buchs erhält einen Gutschein für ein kostenloses digitales Exemplar. Dieses personalisierte PDF-Dokument lässt sich beliebig oft ausdrucken. So können Sie die Checklisten in diesem Buch immer wieder ausfüllen. Käufer erhalten zudem einen 50%-igen Rabatt auf alle weiteren Versionen. So bleiben Sie auch künftig immer auf dem aktuellen Stand der Normen.

Wussten Sie, dass auch benannte Stellen diesen Auditleitfaden nutzen?

„Normen müssen interpretiert werden, um die betriebliche Realität zu erfassen.“ sagt die TÜV Süd Akademie – genau dies haben wir für Sie getan.

**Ihre Vorteile auf einen Blick**

- Erlangen Sie Sicherheit beim Audit
- Vermeiden Sie unangenehme Beanstandungen und aufwendiges Nachbessern
- Ersparen Sie sich das mühsame Interpretieren von Normen.
- Gewinnen Sie dank einfach auszufüllender Checklisten einen schnellen Überblick.
- Identifizieren Sie rasch Schwachstellen. Beheben Sie diese vor dem Audit.
- Verschaffen Sie sich einen Wissensvorsprung, denn diesen Leitfaden Auflage nutzen auch benannte Stellen.
- PDF-Version: Nutzen Sie die Checklisten so oft Sie mögen
- Profitieren Sie von 50% Rabatt bei allen weiteren Auflagen. Sie bleiben dadurch auf dem aktuellen Stand

**Ziel dieses Dokuments**

Mit diesem Buch möchten wir Ihnen ein Werkzeug an die Hand geben, mit dem Sie sich als Verantwortlicher für die Entwicklung oder Qualitätssicherung medizinischer Software optimal auf Audits vorbereiten können. Ebenso unterstützt dieser Leitfaden Auditoren bei Ihrer Arbeit, besonders bei der Vorbereitung und Durchführung von Audits.

Dieses Buch bietet Ihnen mehr als nur eine Konsolidierung und Gruppierung gesetzlicher Forderungen. Es transformiert Software-unspezifische Forderungen in Softwarespezifische. Es berücksichtigt „Best Practices“ und gibt Empfehlungen, die teilweise über die Normenforderungen hinausgehen bzw. konkreter als diese sind. Umgekehrt gibt es einige wenige Forderungen der Normen, die in diesen Checklisten keine Berücksichtigung gefunden haben. Das liegt beispielsweise darin begründet, dass diese (wenigen) Forderungen keine Relevanz bei Audits haben/hatten. Forderungen ohne Bezug zur Software fehlen. Dadurch gelingt es die Checklisten in diesem Dokument vergleichsweise kompakt und für ein Audit medizinischer Software spezifisch zu gestalten.

Es ist das erklärte Ziel dieses Buchs, dass sowohl die Hersteller als auch die Auditoren medizinischer Software sehr schnell einen repräsentativen Überblick über die Güte der Software-Entwicklung erhalten. Dabei wird weniger Wert darauf gelegt, dass jeder einzelne Satz jeder Norm geprüft wird, sondern dass Schwachstellen bei der Entwicklung medizinischer Software identifiziert werden, die mit hoher Wahrscheinlichkeit zu Qualitätseinbußen führen.

**Berücksichtigte Richtlinien, Gesetze und Normen**

Der Fokus dieses Dokuments liegt ausschließlich auf der Auditierung medizinischer Software. Dabei beschränkt sich dieser Leitfaden aber nicht auf die Forderungen der IEC62304. Er betrachtet den kompletten Entwicklungsprozess und bezieht die technische Dokumentation mit ein. Hingegen beziehen sich die Checklisten in diesem Dokument nicht auf Hardware (hierzu möchten wir auch Firmware subsumieren), sie ergänzen aber entsprechende andere Checklisten.

Dieses Buch berücksichtigt alle für die medizinische Software relevanten Vorschriften: Richtlinien, Gesetze und Normen. Dazu zählen insbesondere

- die ISO 13485 zu Qualitätsmanagementsystemen
- die ISO 14971 zum Risikomanagement
- die IEC 62304 zu den Lebenszyklusprozessen sowie zur Verifizierung
- die IEC 60601-1-6 bzw. die IEC 62366 zur Gebrauchstauglichkeit.

**Berücksichtigte Richtlinien, Gesetze und Normen**

Auch weil wir eine Konvergenz medizinischer Informationssysteme und Systeme im Pharmaumfeld beobachten, sind zudem einige GxP relevante Dokumente berücksichtigt.

Dies sind der GAMP „Best practice guide: Testing of GxP systems“ sowie PIC/S. Auch verschiedene „Guidance Documents“ der FDA z.B. „General Principles of Software Validation“ sind in die Checklisten eingeflossen.

Die ISO 9126 nennt Qualitätseigenschaften von Software. Auch wenn diese Taxonomie nicht spezifisch für medizinische Software ist, so sind die in dieser Norm genannten Eigenschaften doch so allgemeingültig, dass sie zumindest teilweise Eingang in die nachfolgenden Checklisten gefunden haben.

**Haftungsausschluss**

Dieses Dokument wurde nach bestem Wissen und Gewissen erstellt. Viele Jahre an Erfahrungen bei der Softwareentwicklung, bei der Erstellung und Überprüfung von Qualitätsmanagementsystemen und der Ausbildung von Software-Entwicklern sind eingeflossen. Dennoch können Fehler nicht ausgeschlossen werden.

Das Dokument hat nicht den Anspruch auf Vollständigkeit, wohl aber darauf, ein Hilfsmittel für effektive und effiziente Audits von Software-Entwicklungsabteilungen zu sein.

Die Interpretation und Übertragung von normativen und gesetzlichen Anforderungen auf die Entwicklung medizinischer Software hat auch einen subjektiven Charakter.

Dennoch ist die Zuordnung beider transparent dargestellt.

Die Autoren lehnen jede Haftung ab, speziell Ansprüche, die aus den Folgen fehlerhafter medizinischer Software und den Audits dieser herrühren.

**Danksagung**

Die Autoren bedanken sich herzlich bei Christian Denger, Matthias Hölzer-Klüpfel und all den treuen Kunden, die zu diesem Auditleitfaden beigetragen haben.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
-----	-------	-----------------------	---------------------

AB:C01	1	<input type="checkbox"/>	<input type="checkbox"/> OK <input type="checkbox"/> Abweichung:
↑ <b>1</b>	↑ <b>2</b>	↑ <b>3</b>	↑ <b>4</b>

Die Checklisten sind möglichst kompakt gehalten, um ein effizientes Auditieren zu ermöglichen. Daher sind die Checklisten tabellarisch gestaltet. Dabei bedeuten:

- 1 „Nr.“:** Eine eindeutige Nummer, auf die Bezug genommen werden kann.
- 2 „Prio.“:** Die Priorität stellt das Maß dafür dar, wie wichtig es ist, dass das Überprüfungskriterium eingehalten ist.
  - **1:** Hohe Priorität. Verstöße gegen das zugehörige Kriterium sind als kritisch zu erachten. Sie stehen im Widerspruch zu grundlegenden Vorschriften oder Best-Practices und stellen typische Ursachen für fehlerhafte Software dar. Bei Verstößen ist eine entsprechende „Würdigung“ beispielsweise in Form einer Abweichung empfohlen.
  - **2:** Mittlere Priorität: Verstöße gegen das zugehörige Kriterium müssen begründet sein. Sie stellen einen Hinweis darauf dar, dass relevante Vorschriften oder Best-Practices nicht eingehalten werden. Es ist empfohlen, die Auswirkungen auf das Endprodukt zu untersuchen.




- **3:** Niedrige Priorität: Verstöße gegen das zugehörige Kriterium sind nicht unmittelbar kritisch. Eine hohe Anzahl solcher Verstöße kann allerdings die Güte des Produkts wesentlich beeinflussen. Dies sollte im Audit mit dem Kunden diskutiert werden.





- 3 „Überprüfungskriterium“:** Hier finden sich ein oder mehrere Punkte gelistet, die als Hinweis für eine Einhaltung des Kriteriums zu verstehen sind. Treffen nur wenige der genannten Punkte zu, so ist davon auszugehen, dass das Kriterium nicht eingehalten ist, also ein Verstoß vorliegt. Essentielle Kriterien sind mit **!** gekennzeichnet. Ein Verstoß dagegen macht eine Einhaltung des Kriteriums unwahrscheinlich. Die meisten Überprüfungskriterien sind mit einer Fußnote, einem Verweis, versehen. Hier finden sich weiterführende Informationen, speziell die entsprechenden Kapitel/Abschnitte/Paragrafen der relevanten Normen, Gesetze und sonstiger Best-Practices und Vorschriften.

- 4 „Anmerkungen Auditor“:** Hier tragen die Prüfer (interne Prüfer oder externe Auditoren) Ihre Beobachtungen ein und bewerten, ob das jeweilige Kriterium erfüllt ist.

**ENTWICKLUNGSPROZESS**

Unter dem Entwicklungsprozess ist hier der gesamte Entwicklungsprozess, also nicht nur der Software-Entwicklungsprozess zu verstehen. Allerdings beziehen sich die folgenden Überprüfungs-kriterien nur auf Software.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Entwicklungsprozess allgemein</b>	
EP:A01		<input type="checkbox"/> Es besteht ein dokumentierter Entwicklungsprozess <sup>1,2,3</sup> .	
EP:A02		<input type="checkbox"/> Die Prozess ist entweder spezifische für das Projekt oder es existiert ein Verweis (1 Satz genügt) auf einen übergeordneten Entwicklungsplan <sup>4</sup> .	
EP:A03		<input type="checkbox"/>  <sup>1</sup> Der Entwicklungsprozess ist den Entwicklern bekannt. Diese können die Phasen benennen oder zumindest die entsprechenden Dokumente zeigen. Diese sind die aktuellsten (freigegebenen).	
EP:A04		<input type="checkbox"/>  Der Prozess (oder eine dokumentierte Variante) findet nachweislich auch für Änderungen an der Software nach der initialen Entwicklung Anwendung. <sup>5</sup> Dies muss am Beispiel einer neuen Version (1. Ziffer vor oder nach Komma) nachgewiesen werden <sup>6</sup> .	
EP:A05		<input type="checkbox"/> Der Entwicklungsprozess unterscheidet Software unterschiedlicher Risiko- bzw. Sicherheitsklassen <sup>7</sup> .	
EP:A06		<input type="checkbox"/>  Der Entwicklungsprozess sieht Modul-, Integrations-, System- und Abnahmetests vor.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
EP:A07		<input type="checkbox"/>  Es ist beschrieben, wie die Anforderungsanalyse durchzuführen und zu dokumentieren ist <sup>8</sup> .	
		<input type="checkbox"/>  Es ist beschrieben, wie die Architektur zu dokumentieren ist.	
		<input type="checkbox"/>  Es ist beschrieben, wie die Modultests, Integrationstests und Systemtests durchzuführen und dokumentieren sind.	
EP:A08		<input type="checkbox"/> (!) Es ist beschrieben, wie die Freigabe durchzuführen und zu dokumentieren ist <sup>9</sup> .	
EP:A09		<input type="checkbox"/> Die Verantwortlichkeiten sind benannt. Es ist darauf geachtet, dass nicht der Entwickler die Software selbst testet (Ausnahme Modultests).	
EP:A010		<input type="checkbox"/> Der Entwicklungsprozess sieht ein Review der Tests, des Codes, des Architekturdokuments und der Software-Anforderungen vor. (Details s.u.).	
	2	<b>Entwicklungsrichtlinien</b>	
EP:B01		<input type="checkbox"/>  Programmierrichtlinien wie Namenskonventionen und Code-Metriken existieren und sind den Entwicklern bekannt.	
EP:B02		<input type="checkbox"/> Die zu erreichenden Abdeckungsgrade sind definiert. Für Software mit mittlerem bis hohem Risiko sind mindestens 50% Zweigabdeckung vorgeschrieben <sup>10</sup> .	

**ANFORDERUNGSANALYSE**

Die Anforderungsanalyse ist nicht mit der Spezifikation zu verwechseln. Die Anforderungsanalyse ist dem Problemraum, die Spezifikation dem Lösungsraum zuzuordnen.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Allgemeines</b> 11, 12, 13, 14	
AA:A01		<input type="checkbox"/> ⚠ Alle Nutzungsanforderungen sind benannt und auf Erfordernisse zurückzuführen <sup>15</sup> . Die Nutzungsanforderungen sind nicht technisch formuliert, insbesondere wird keine Lösung skizziert. Es gibt eine von der Spezifikation unabhängige Beschreibung der (Nutzungs-) Anforderungen.	
ANA2		<input type="checkbox"/> Weitere Anforderungen sind benannt: <ul style="list-style-type: none"> <li><input type="checkbox"/> organisatorische (Zugriffsbeschränkungen, Berechtigungen),</li> <li><input type="checkbox"/> rechtliche (Bildschirmarbeitsplatz-Verordnung, Datenschutz usw.),</li> <li><input type="checkbox"/> fachliche,</li> <li><input type="checkbox"/> Marktanforderungen.</li> </ul>	
AA:A03		<input type="checkbox"/> Alle Anforderungen sind eindeutig gekennzeichnet.	
AA:A04		<input type="checkbox"/> Spezielle funktionalen Anforderungen, z.B. <ul style="list-style-type: none"> <li><input type="checkbox"/> zu implementierende Algorithmen,</li> <li><input type="checkbox"/> Präzision der Berechnung,</li> <li><input type="checkbox"/> zu erstellende Formulare, Berichte, Ausgaben sind ggf. berücksichtigt.</li> </ul>	


Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
AA:A05		<input type="checkbox"/> Nicht funktionale Anforderungen sind benannt. Diese Anforderungen beinhalten (soweit zutreffend): <ul style="list-style-type: none"> <li><input type="checkbox"/> Installation (s.u.) und Wartung (durch wen, wie oft, Aufwand, remote/lokal usw.)<sup>16</sup>,</li> <li><input type="checkbox"/> vorausgesetzte bzw. zu unterstützende Hardware (CPU, RAM, Festplatte, PC, Notebook, embedded), Betriebssysteme, andere Software (z.B. Datenbank, Office, Webserver), Netzwerk/Internetanbindungen, Personal (Ausbildungsstand, Sprachkenntnisse),</li> <li><input type="checkbox"/> zu unterstützende Peripherie (Drucker, Monitor, Eingabegeräte, ...),</li> <li><input type="checkbox"/> erwartetes und zu unterstützendes Datenvolumen,</li> <li><input type="checkbox"/> Skalierbarkeit: Reaktionszeiten (abhängig von Last (Anzahl Benutzer, Jobs), Maximalanforderungen an Hardware (RAM, CPU-Last, I/O, Netzwerklast),</li> <li><input type="checkbox"/> maximale Dauer zum Starten und Beenden des Systems,</li> <li><input type="checkbox"/> zu unterstützende Sprachen, Zeichensätze,</li> <li><input type="checkbox"/> Verfügbarkeit,</li> <li><input type="checkbox"/> Vorgaben an Benutzerschnittstelle, die nicht aus Nutzungsanforderungen abzuleiten sind (Firmenvorgaben),</li> <li><input type="checkbox"/> spezifische Vorgaben für Datensicherheit (z.B. Unterstützung von Back-up Mechanismen).</li> </ul>	




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	1	<b>Zweckbestimmung</b>	
AA:B01		<input type="checkbox"/> ⚠ Die Zweckbestimmung ist beschrieben. Insbesondere ist erwähnt, <ul style="list-style-type: none"> <li><input type="checkbox"/> wie das Produkt der Diagnose, Therapie oder Überwachung von Krankheiten oder Verletzungen oder physiologischer oder anatomischer Parameter) dient<sup>17</sup>.</li> <li><input type="checkbox"/> ob es lebenserhaltend oder lebensunterstützend wirkt<sup>2</sup>.</li> </ul>	
AA:B02		<input type="checkbox"/> ⚠ Die Zweckbestimmung beschreibt die vorgesehene Patientengruppe (einschließlich Alter, Gesundheitszustand, Gewicht).	
AA:B03		<input type="checkbox"/> Die Zweckbestimmung beschreibt, welche Körperregion bzw. welches Gewebe untersucht, diagnostiziert, therapiert oder überwacht werden soll.	
AA:B04		<input type="checkbox"/> ⚠ Die Benutzergruppen sind charakterisiert (Alter, Beruf, Funktion innerhalb Organisation, Ausbildung, Geschlecht, Sprachkenntnisse, spezielle relevante Fähigkeiten usw.).	
AA:B05		<input type="checkbox"/> Der Benutzungskontext ist beschrieben <sup>18</sup> : Kernaufgaben, Häufigkeit der Anwendung, Arbeitsbelastung, zu erzielende Ergebnisse <sup>19</sup> .	
AA:B06		<input type="checkbox"/> Ort der Anwendung <sup>20</sup> und dort vorherrschende Verhältnisse wie Helligkeit, Temperatur sind beschrieben.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Gebrauchstauglichkeit</b>	
AA:C01		<input type="checkbox"/> Die Anforderungsanalyse enthält messbare Gebrauchstauglichkeitsziele <sup>21</sup> .	
	2	<b>Validierung</b>	
AA:D01		<input type="checkbox"/> Die Benutzer sind in die Validierung der Anforderungsanalyse involviert <sup>22</sup> .	

**FUNKTIONALE SPEZIFIKATION („SOFTWARE-ANFORDERUNGEN“)**

Die funktionale Spezifikation transformiert die Anforderungen in eine konkrete Beschreibung der Lösung. Beispielsweise gilt es hier die Benutzerschnittstelle zu beschreiben.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Allgemeines</b> <sup>11, 12, 13, 14</sup>	
FS:A01		<input type="checkbox"/> Alle Systemanforderungen sind testbar.	
FS:A02		<input type="checkbox"/> Alle Systemanforderungen sind eindeutig gekennzeichnet.	
FS:A03		<input type="checkbox"/> Nicht funktionale Anforderungen sind benannt.	
	2	<b>Inhalt</b>	
		Die Spezifikation umfasst <sup>23, 24, 25</sup>	
FS:B01		<input type="checkbox"/> alle (wichtigen) Funktionen die der Benutzer ausführen kann (z.B. als Use Cases beschrieben) <sup>26</sup> . Es ist beschrieben, ob diese Funktionen sicherheitsbezogen sind <sup>27</sup> .	
FS:B02		<input type="checkbox"/> die Reihenfolge, in der die Benutzer diese Funktionen im Rahmen einer Kernaufgabe aufrufen <sup>28</sup> .	
FS:B03		<input type="checkbox"/>  die Bildschirmmasken.	
FS:B04		<input type="checkbox"/> allgemeine Vorgaben zum Aufbau der GUI („Style Guide“), die auch festlegen, wann eine Hauptbedienfunktion als gut erkennbar angesehen wird.	
FS:B05		<input type="checkbox"/> Festlegungen bezüglich Mehrsprachigkeit, kontextsensitiver Hilfe, online Hilfe, Benutzerhandbuch.	



Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
FS:B06		<input type="checkbox"/> für Eingabefelder folgende Angaben: erlaubte Werte bzw. Wertebereiche, Datentypen und Reaktionen des Systems auf Fehleingaben.	
FS:B07		<input type="checkbox"/>  Schnittstellen zu anderen Systemen.	
FS:B08		<input type="checkbox"/> vom Produkt anzufertigende Berichte und andere Ausgaben (Bildschirm, Alarm, Drucker).	
FS:B09		<input type="checkbox"/> (Datei-) Formate, welche die Anwendung einlesen und abspeichern kann.	
	2	<b>Tests</b> <sup>29</sup>	
FS:C01		<input type="checkbox"/>  Die Abnahmetests sind spezifiziert.	
FS:C02		<input type="checkbox"/> Die Tests genügen den Kriterien, wie sie weiter unten unter „Testspezifikation“ genannt sind.	
		<b>Verifikation</b> (Review der funktionalen Spezifikation)	
FS:D01		<input type="checkbox"/> Während der Verifikation werden o.g. Punkte geprüft.	
FS:D02		<input type="checkbox"/> Es ist erkenntlich, auf welche Version des Dokuments sich die Verifikation bezieht.	
FS:D03		<input type="checkbox"/>  Es gibt eine Traceability-Matrix, in der erkenntlich ist, dass alle Software-Anforderungen von System-Anforderungen bzw. Nutzungsanforderungen abgeleitet sind <sup>30</sup> .	

**ARCHITEKTUR**

Während der Architektur gilt es zu beschreiben, wie die spezifizierte Lösung technisch umgesetzt werden soll. Damit dient das Architekturdokument dem Programmierer als Anleitung. Dieser Abschnitt umfasst beide in der IEC 62304 genannten Aktivitäten, Architektur und detailliertes Design.




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	1	<b>Dokumentation, Modellierung</b> <sup>31, 32</sup>	
AR:A01	<input type="checkbox"/>	⚠ Es gibt ein Architekturdokument.	
AR:A02	<input type="checkbox"/>	⚠ Die Architektur ist mit UML oder einer anderen Modellierungssprache dokumentiert.	
AR:A03	<input type="checkbox"/>	⚠ Das Architekturdokument lässt die einzelnen Subsysteme, Komponenten und (bei Klasse C) Software-Einheitenerkennen <sup>33</sup> .	
AR:A04	<input type="checkbox"/>	⚠ Die Schnittstellen der Subsysteme, Komponenten und (bei Klasse C) Software-Einheiten sind beschrieben <sup>33</sup> .	
A\$:A05	<input type="checkbox"/>	Die funktionalen und nicht-funktionalen Anforderungen aus der Anforderungsanalyse werden in der Architektur berücksichtigt. Eine Traceability-Matrix erlaubt die rasche Überprüfung und gewährt einen Überblick.	
AR:A06	<input type="checkbox"/>	Es gibt eine Liste aller eingesetzter Fremdkomponenten (SOUP). Für jede dieser Fremdkomponenten sind deren Name, Hersteller und Versionsnummer dokumentiert <sup>34</sup> .	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
AR:A07	<input type="checkbox"/>	Die technischen Anforderungen an Fremdkomponenten (SOUP) und die Anforderungen der Fremdkomponenten sind benannt (in Bezug auf Hardware, Software, Laufzeitverhalten) <sup>35</sup> .	
AR:A08	<input type="checkbox"/>	Es ist beschrieben, wie die Komponenten verteilt sind (z.B. auf einem oder mehreren Rechnern), wie diese Komponenten kommunizieren und wie diese Kommunikation geschützt ist.	
AR:A09	<input type="checkbox"/>	Es ist erkenntlich, welcher Teil der Geschäftslogik sich außerhalb des Programmcodes befindet, beispielsweise in der Datenbank, Konfigurationsdateien und Skripten.	
AR:A10	<input type="checkbox"/>	Es ist beschrieben, in welchen Schritten das System aus den Komponenten stückweise zusammengesetzt wird <sup>36</sup> .	
AR:A011	<input type="checkbox"/>	Jeder Komponente (außer Software-Einheit) ist eine Sicherheitsklasse zugeordnet <sup>37</sup> .	
AR:A012	<input type="checkbox"/>	Wenn die Klassifizierung des Systems erniedrigt wurde, gibt es eine dokumentierte Hardwarekontrollmaßnahme <sup>37</sup> .	
AR:A013	<input type="checkbox"/>	Wenn einer Subkomponente eine niedrigere Klasse als die ihr übergeordnete zugewiesen wurde, so ist dies begründet <sup>37</sup> .	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Güte der Architektur</b>	
AR:B01		<input type="checkbox"/> Die Komponenten weisen keine zyklischen Abhängigkeiten auf.	
AR:B02		<input type="checkbox"/> Bei Schichtenarchitekturen ist jede Schicht nur von der jeweils nächsten abhängig.	
AR:B03		<input type="checkbox"/> Komponenten, von denen viele andere abhängen, weisen einen hohen Grad an Abstraktheit auf (Interfaces, abstrakte Klassen).	
	3	<b>Spezifikation der Tests</b>	
AR:C01		<input type="checkbox"/>  Es sind Integrationstests spezifiziert	
AR:C02		<input type="checkbox"/> Ein Plan beschreibt die Reihenfolge der Integration und die zugehörigen Tests	
AR:C03		<input type="checkbox"/> Es existiert für jede Komponente mindestens ein Test.	
AR:C04		<input type="checkbox"/> Die Tests genügen den Kriterien, wie sie weiter unten unter „Testspezifikation“ genannt sind.	
	2	<b>Verifikation der Architektur</b> <sup>38, 39</sup>	
AR:D01		<input type="checkbox"/>  Das Architekturdokument wurde einem Review unterzogen.	
AR:D02		<input type="checkbox"/> Es ist erkenntlich, auf welche Version des Dokuments sich das Review bezieht.	

**IMPLEMENTIERUNG**

Dieser Abschnitt gibt Prüfkriterien für die Implementierung, nicht für den Modultest.




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Einhalten der Vorgaben durch Entwickler</b> <sup>40</sup>	
IM:A01		<input type="checkbox"/>  Die Entwickler können benennen, welchen Teil des Architekturdokuments sie gerade implementieren.	
IM:A02		<input type="checkbox"/>  Die Vorgaben bezüglich Namenskonventionen und Code-Metriken sind den Entwicklern bekannt und werden eingehalten.	
	2	<b>Code Review</b>	
IM:B01		<input type="checkbox"/> Der Code wird (idealerweise) durch einen zweiten Entwickler geprüft (Code und Modultests können während eines Reviews geprüft werden).	
IM:B02		<input type="checkbox"/>  Verständlichkeit des Codes, Namenskonventionen und Code-Metriken werden geprüft.	
IM:B03		<input type="checkbox"/> Umsetzung der Architektur wird geprüft.	
IM:B04		<input type="checkbox"/> Das Code-Review bezieht sich auf eine eindeutige Version des Codes (dieser befindet sich unter Versionskontrolle). Die Version ist dokumentiert und kann zukünftig wiederhergestellt werden.	



**TESTEN: VERIFIKATION UND VALIDIERUNG**

Dieser Abschnitt umfasst die Schritte der analytischen Qualitätssicherung, vom ModulÐ bis zum Abnahmetest.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Testspezifikation</b> (gilt für alle Tests)	
TE:A01		<input type="checkbox"/> Die Voraussetzungen für das Testen sind benannt. Beispielsweise Software-Version, notwendige Daten usw.	
TE:A02		<input type="checkbox"/> ⚠ Die Spezifikation nennt genau das Vorgehen und damit das Verfahren (z.B. Review, Metrik) und die Daten, die einzugeben sind (und nicht etwa „Testen Sie, dass man sich nur mit gültigem Benutzernamen einloggen kann“) <sup>41</sup> . Lassen Sie sich je ein Beispiel für einen Systemtest und einen Akzeptanztest zeigen.	
TE:A03		<input type="checkbox"/> ⚠ Die erwarteten Ergebnisse sind genau beschrieben. Falls das Ergebnis nicht unmittelbar ablesbar ist, so ist nachvollziehbar beschrieben, wie man zum Ergebnis kommt (z.B. durch eine Rechenvorschrift).	
	1	<b>Testergebnisse allgemein</b>	
TE:B01		<input type="checkbox"/> ⚠ Die Testergebnisse sind dokumentiert einschließlich Datum, Tester, getestete Version, Testwerkzeug <sup>42</sup> . Lassen Sie sich für einen Modul-, einen System- und einen Akzeptanztest zeigen, wie die Ergebnisse dokumentiert wurden.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
TE:B02		<input type="checkbox"/> Die Ergebnisse lassen erkennen, ob der Test erfolgreich war oder nicht.	
TE:B03		<input type="checkbox"/> Die Tests decken alle Kriterien der ISO 9126 ab <sup>43</sup> . Der Auditor kann also fragen: „Wie testen Sie Wartbarkeit, Robustheit, Übertragbarkeit ...?“.	
TE:B04		<input type="checkbox"/> ⚠ Die Tests sind für die aktuelle Softwareversion durchgeführt worden. Lassen Sie sich dies zeigen.	
	1	<b>Reproduzierbarkeit Review der Testergebnisse</b>	
TE:C01		<input type="checkbox"/> Es wurde geprüft, dass alle Tests durchgeführt wurden.	
TE:C02		<input type="checkbox"/> ⚠ Lassen Sie sich an je einem Beispiel für einen Modul, Systemtest und Akzeptanztests zeigen, dass sich die Ergebnisse für eine alte Version (z.B. ein Jahr zurückliegend) wiederholen werden können.	
	2	<b>Regressionstests</b> <sup>44, 45, 46</sup>	
TE:D01		<input type="checkbox"/> ⚠ Es gibt Regressionstests.	
TE:D02		<input type="checkbox"/> Regressionstests werden mindestens täglich ausgeführt, wenn es Änderungen im Code gibt.	
TE:D03		<input type="checkbox"/> Für jeden im Feld aufgetretenen und behobenen Fehler gibt es einen Test, der als Regressionstest ausgeführt wird. Wählen Sie (als Prüfer) eine Fehlermeldung aus dem „Ticket-System aus und lassen Sie sich den Test zeigen, der die Behebung dokumentiert.	


Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
TE:D04		<input type="checkbox"/> Es gibt automatisierte Oberflächentests.	
TE:D05		<input type="checkbox"/>  Die Tests der vorangegangenen Versionen wurden auch beim letzten Release durchgeführt. Dies kann anhand von Testprotokollen nachgewiesen werden.	
	1	<b>Modultests</b> <sup>47, 48</sup>	
TE:E01		<input type="checkbox"/>  Die Modultests erfüllen die Anforderungen an die Abdeckungsgrade (s.o.).	
TE:E02		<input type="checkbox"/> Besonders bei kritischen Algorithmen wird darauf geachtet, dass durch die Tests alle möglichen Rück- bzw. Ausgabewerten erzeugt werden (mit Äquivalenzklassen der Rückgabewerte zu prüfen).	
TE:E03		<input type="checkbox"/> Für Komponenten der Sicherheitsklasse C prüfen die Modultests Speicherverbrauch, Speicherüberlauf, Fehlerbehandlung, Initialisierung von Variablen und einen möglichen Selbsttest <sup>49</sup> . Wählen Sie einen beliebigen Modultest aus und lassen Sie sich vom Entwickler erklären, welche Fehlerfälle er abfängt.	
	2	<b>Integrationstests</b> <sup>50, 51, 52</sup>	
TE:F01		<input type="checkbox"/>  Es gibt einen Integrationstestplan <sup>53</sup> .	
TE:F02		<input type="checkbox"/> Im Integrationstestplan ist die Integrationsstrategie (z.B. Bottom-up, Top-Down, Big-Bang beschrieben).	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
TE:F03		<input type="checkbox"/> Es gibt abhängig von der Integrationsstrategie Testtreiber und/oder Mock-Objekte. Die Mock-Objekte prüfen, ob die zu testende Komponente das Mock-Objekt mit den richtigen Daten, in der richtigen Reihenfolge aufruft und ob die zu testende Komponente mit den vom Mock-Objekt zurückgegebenen Werten umgehen kann.	
TE:F04		<input type="checkbox"/>  Die Ergebnisse der Integrationstests sind beschrieben.	
	1	<b>Systemtests</b> <sup>54, 55, 56</sup>	
TE:G01		<input type="checkbox"/> Die Systemtests testen alle Anforderungen einschließlich der Risikokontrollmaßnahmen. Dies wird typischerweise über eine Traceability-Matrix dokumentiert <sup>57</sup> .	
TE:G02		<input type="checkbox"/>  Alle Abläufe/Masken, die mit für Anwender oder Patienten kritischen Daten umgehen, sind über die Oberfläche getestet.	
TE:G03		<input type="checkbox"/> Die Masken sind wie spezifiziert umgesetzt, der „GUI-Style-Guide“ ist eingehalten <sup>58</sup> .	
TE:G04		<input type="checkbox"/> Äquivalenzklassen und grenzwertbasiertes Testen findet Anwendung.	
TE:G05		<input type="checkbox"/>  Offensichtliche Fehleingaben sind nicht möglich: <ul style="list-style-type: none"> <li><input type="checkbox"/> Datum in Zukunft (bei mehrschichtigen Anwendungen Datum des Clients verstellen),</li> <li><input type="checkbox"/> unmögliche Daten (z.B. 31. Februar),</li> <li><input type="checkbox"/> leere Felder, Felder mit Leerzeichen, wenn diese nicht erwartet werden,</li> </ul>	




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
		<input type="checkbox"/> unsinnig große oder kleine Zahlen (z.B. Körpergröße 3m), <input type="checkbox"/> Zahlen mit vertauschten Dezimaltrennzeichen, <input type="checkbox"/> Sonderzeichen, <input type="checkbox"/> nicht sichtbare Zeichen (mit ALT + vierstellige Zahl eingeben).	
TE:G06		<input type="checkbox"/> Die Systemtests berücksichtigen mehrere Sprachen (speziell Zahlen, Währungen, Datumsformate).	
TE:G07		<input type="checkbox"/> Bei Mehrbenutzersystemen werden in Abhängigkeit von der Benutzeranzahl überprüft: Antwortzeiten, CPU-Last und Speicherverbrauch. Diese liegen innerhalb der spezifizierten Akzeptanzgrenzen (Lasttest).	
TE:G08		<input type="checkbox"/> Es ist nachgewiesen, dass das System durch eine zu hohe Benutzerlast nicht in einen inkonsistenten Zustand geführt werden kann (Stresstest).	
TE:G09		<input type="checkbox"/> Die Systemtests werden von einem dedizierten Tester bzw. Testteam ausgeführt. <sup>59</sup>	
TE:G010		<input type="checkbox"/> Alles bisher Genannte ist dokumentiert.	
	1	<b>Abnahme-/Akzeptanztests/Validierung<sup>60</sup></b>	
TE_H1		<input type="checkbox"/> ⚠ Die Abnahme- bzw. Akzeptanztests sind spezifiziert. Diese Tests sind nicht auf ein intuitives „Durchklicken“ beschränkt.	
TE_H2		<input type="checkbox"/> ⚠ Die Validierung findet in der wirklichen oder einer simulierten Gebrauchsumgebung durch wirkliche Benutzer statt <sup>61</sup>	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
TE_H3		<input type="checkbox"/> Die Validierung erfolgt nach einem Plan, der u.a. beschreibt <sup>62</sup> : <input type="checkbox"/> die Aufgaben, die die Benutzer bearbeiten sollen, <input type="checkbox"/> ggf. welche Daten eingegeben werden sollen, <input type="checkbox"/> welche Daten bei der Validierung erhoben werden (Ergebnisse), <input type="checkbox"/> die Akzeptanzkriterien für diese Daten (z.B. die maximale Zeit zur Bearbeitung, die maximale Fehleranzahl, Ergebnisse von Berechnungen, erwarteter quantifizierbarer Erfolg für die Diagnose, Überwachung oder Therapie der Patienten).	
TE_H4		<input type="checkbox"/> Der Validierungsplan enthält zumindest alle häufigen und sicherheitskritischen Benutzungsszenarien <sup>63</sup> .	
TE_H5		<input type="checkbox"/> Die Ergebnisse der Validierung sind dokumentiert <sup>64</sup> .	
TE_H6		<input type="checkbox"/> ⚠ Der klinische Nutzen des Produkts ist nachgewiesen, z.B. durch eine klinische Validierung oder durch Literatur <sup>65</sup> .	

**RISIKOMANAGEMENT**

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	1	<b>Inhalt der Risikomanagementakte</b>	
RI:A01		<input type="checkbox"/> Die Risikoklassifizierung der Software-Komponenten ist ersichtlich <sup>66</sup> .	
RI:A02		<input type="checkbox"/> Die Risikobewertungsmatrix ist spezifisch für das Produkt: <ul style="list-style-type: none"> <li><input type="checkbox"/> Das größte und kleinste relevante Schadensmaß sind angemessen.</li> <li><input type="checkbox"/> Die Wahrscheinlichkeiten sind plausibel. Die Achse deckt Ereignisse ab, die einerseits mehrmals pro Anwendungsfall und andererseits deutlich weniger als einmal bei allen Anwendungsfälle des Medizinprodukts (über alle Produkte, alle Patienten, die komplette Lebensdauer aller Produkte) erwartet werden.</li> <li><input type="checkbox"/> Die Akzeptanzkriterien sind nicht schwächer als bei vergleichbaren Produkten oder alternativen Verfahren.</li> </ul>	
RI:A03		<input type="checkbox"/>  Die Risikobewertungsmatrix enthält die Anzahl der identifizierten Gefährdungen für jede Zelle (jede Kombination aus Wahrscheinlichkeit und Schweregrad) sowohl vor als auch nach den Risikokontrollmaßnahmen.	
RI:A04		<input type="checkbox"/> Die Risikomanagementakte enthält in tabellarischer Darstellung die Risikoanalyse (s.u.), die zugehörigen Risikokontrollmaßnahmen und deren Verifizierung und eine Bewertung des Risikos vor und nach den Maßnahmen (Die Tabelle enthält die Spalten: Eindeutige Nummer, Komponente bzw.	




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
-----	-------	-----------------------	---------------------

		Funktion, Fehler in der Komponente bzw. Funktion (Ursache für Gefährdung), Auswirkung auf Gesamtsystem, Gefährdung, Wahrscheinlichkeit, Schweregrad, Risiko, Gegenmaßnahme, Verifikation der Implementierung und Wirksamkeit der Gegenmaßnahme, neue Wahrscheinlichkeit, neuer Schweregrad, neues Risiko.)	
RI:A05		<input type="checkbox"/>  Die Risikomanagementakte enthält eine Bewertung der einzelnen verbliebenen Restrisiken.	
RI:A06		<input type="checkbox"/>  Die Risikomanagementakte enthält eine Gesamtabwägung von Risiken und Nutzen.	
RI:A07		<input type="checkbox"/>  Die Risikomanagementakte enthält eine Darlegung, in wie weit die ergriffenen Maßnahmen neue Risiken nach sich ziehen. Dies kann durch weitere Einträge in der Tabelle erfolgen.	
RI:A08		<input type="checkbox"/> Die Risikomanagementakte enthält die Anzahl der erwarteten betroffenen Patienten für jede Schadensklasse (z.B. Tod, schwere Verletzung).	
RI:A09		<input type="checkbox"/> Die Risikomanagementakte enthält eine Nennung der am Risikomanagement beteiligten Personen und einen Nachweis der Qualifizierung. Zu diesen Personen zählen ein Risikomanager, Arzt bzw. medizinisches Fachpersonal, Benutzer und Entwickler bzw. Software-Architekten.	
RI:A10		<input type="checkbox"/> Die Risikomanagementakte enthält einen Bezug zum Medizinprodukt einschließlich dessen Version.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	1	<b>Risikoanalyse</b> <sup>67, 68</sup> (bitte Hinweis <sup>69</sup> beachten) Die Risikoanalyse betrachtet Gefährdungen, die verursacht werden durch,	
RI:B01		<input type="checkbox"/> ⚠️ Unaufmerksamkeit der Benutzer (vergessen, auslassen, vertauschen, verwechseln). Diese Analyse ist für jede häufig benutzte und jede sicherheitsbezogene Funktion durchgeführt <sup>70</sup> .	
RI:B02		<input type="checkbox"/> vorhersagbaren Missbrauch.	
RI:B03		<input type="checkbox"/> mehrere Benutzer, die parallel mit einer Anwendung arbeiten.	
RI:B04		<input type="checkbox"/> die Abhängigkeit von der Reihenfolge, in der Aktionen durchgeführt werden.	
RI:B05		<input type="checkbox"/> Probleme beim Aufrufen der Hauptbedienfunktionen im häufigsten und ungünstigsten Fall <sup>71</sup> .	
RI:B06		<input type="checkbox"/> Missverständnis der Benutzer über die Funktionsweise des Medizinprodukts.	
RI:B07		<input type="checkbox"/> Missverständnis der Benutzer über die Bedienung des Medizinprodukts.	
RI:B08		<input type="checkbox"/> ⚠️ Nichtlesen der Gebrauchsanweisung.	
RI:B09		<input type="checkbox"/> ⚠️ Anwendung durch nicht dafür ausgebildete Personen (medizinische Kenntnisse, Sprache, Verständnis für IT).	
RI:B010		<input type="checkbox"/> ⚠️ Arbeitsüberlastung oder Ablenkung des Anwenders.	




Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
RI:B011		<input type="checkbox"/> ⚠️ nicht ausreichend geschulte/geeignete Nutzer	
RI:B012		<input type="checkbox"/> ⚠️ Es sind alle Nutzer berücksichtigt: Anwender, Administratoren, Service (auch Fernwartung)	
RI:B013		<input type="checkbox"/> Umgebung (Helligkeit, Geräusche, Temperatur, Luftfeuchtigkeit).	
RI:B014		<input type="checkbox"/> Viren und andere Schadsoftware.	
RI:B015		<input type="checkbox"/> (teilweisen) Ausfall von Bauteilen, speziell CPU, RAM, Festplatte, Monitor.	
RI:B016		<input type="checkbox"/> fehlerhafte Kalibrierung oder Darstellung auf dem Monitor oder Drucker.	
RI:B017		<input type="checkbox"/> für den Benutzer unleserliche Anzeige: Schrift zu klein, Farbenblindheit, verdeckte Information, ungeeignete Typographie (z.B. Verwechslung des Buchstabens „l“ mit der Ziffer „1“).	
RI:B018		<input type="checkbox"/> unklare Zuordnung von Labels zu Controls oder verwirrende Gruppierung der GUI-Elemente.	
RI:B019		<input type="checkbox"/> Benutzereingaben oder Darstellung in falschen/unerwarteten Einheiten (z.B. mmol/l – mg/dl).	
RI:B020		<input type="checkbox"/> Benutzereingaben mit falschen Dezimaltrennzeichen.	
RI:B021		<input type="checkbox"/> Wahl einer „falschen“ Einstellung/Umstellung der „Locale“ im Betriebssystem bzw. durch ein anderssprachiges Betriebssystem.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
RI:B022		<input type="checkbox"/> Installation auf ungeeigneter Hardware (Systemressourcen, Betriebssystem, Monitorauflösung).	
RI:B023		<input type="checkbox"/> Updates des Betriebssystems oder Anwendungssoftware (z.B. Austausch von DLLs).	
RI:B024		<input type="checkbox"/> Fehler in eingesetzten oder vorausgesetzten Komponenten (z.B. fehlerhafte Datenbank).	
RI:B025		<input type="checkbox"/> Daten, die von anderen Systemen fehlerhaft übertragen werden: <ul style="list-style-type: none"> <li><input type="checkbox"/> Verfälscht,</li> <li><input type="checkbox"/> zu spät/zu früh,</li> <li><input type="checkbox"/> überhaupt nicht,</li> <li><input type="checkbox"/> in falscher Reihenfolge,</li> <li><input type="checkbox"/> an falschen Empfänger,</li> <li><input type="checkbox"/> in nicht vertraulicher Weise,</li> <li><input type="checkbox"/> nicht einem (Ab-) Sender zu zuordnen,</li> <li><input type="checkbox"/> zu einem falschen Kontext (z.B. Patienten).</li> </ul>	
RI:B026		<input type="checkbox"/> Installation anderer Programme (auch Antivirusprogramme).	
RI:B027		<input type="checkbox"/> Unterlassen von Updates.	
RI:B028		<input type="checkbox"/> Zugriff durch Dritte, auch Fernwartung.	
RI:B029		<input type="checkbox"/> Ausfall/Nichtverfügbarkeit des Produkts.	
RI:B030		<input type="checkbox"/> Nichtverfügbarkeit des (in elektronischer Form vorliegenden) Handbuchs.	
RI:B031		<input type="checkbox"/> fehlerhafte Berechnung und Anzeige von Informationen.	


Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
RI:B032		<input type="checkbox"/> fehlerhafte Ansteuerung oder Beeinflussung von Medizin-geräten. Die Risikoanalyse betrachtet Gefährdungen für	
RI:B033		<input type="checkbox"/> Patienten,	
RI:B034		<input type="checkbox"/> Anwender: Benutzer, Administratoren, Dritte,	
RI:B035		<input type="checkbox"/> Güter <sup>72</sup> , Umwelt <sup>72</sup> . Die Risikoanalyse berücksichtigt bereits bekannte Gefährdungen (auch im Bezug auf die GUI) und wertet dabei aus <sup>73</sup> :	
RI:B036		<input type="checkbox"/> Meldungen von der Hotline,	
RI:B037		<input type="checkbox"/>  Fehlermeldungen (Problemberichte),	
RI:B038		<input type="checkbox"/>  BfArM-Berichte,	
RI:B039		<input type="checkbox"/> Kundengespräche,	
RI:B040		<input type="checkbox"/> (Fehler-)Log-Dateien,	
RI:B041		<input type="checkbox"/> Die Ergebnisse der Validierung der (GUI-) Prototypen.	
	1	<b>Komponenten<sup>74</sup></b>	
RI:C01		<input type="checkbox"/>  Durch eine FMEA sind die Risiken für alle Komponenten analysiert, die im Architekturdokument beschrieben sind <sup>75</sup> . Dies gilt insbesondere auch für die Fremdkomponenten (SOUPs) <sup>76</sup> .	
RI:C02		<input type="checkbox"/> Die FMEA dokumentiert tabellarisch Risiken und Gegenmaßnahmen.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
RI:C03		<input type="checkbox"/> Dies gilt insbesondere für eingekaufte Komponenten. Maßnahmen zur Risikominimierung sind umgesetzt und getestet. Die Version dieser Komponenten ist genannt und geprüft.	
RI:C04		<input type="checkbox"/>  Im Rahmen einer FTA sind die Komponenten identifiziert, deren Ausfall oder Fehlfunktion zu einer Gefährdung führen würden. Dies wird durch Gegenmaßnahmen (Selbstchecks, redundante Auslegung) kompensiert.	
	2	<b>Konfiguration</b> <sup>77, 78</sup>	
RI:D01		<input type="checkbox"/> Die Gefährdungen, die durch falsche Konfiguration entstehen können, sind analysiert und durch Gegenmaßnahmen berücksichtigt.	
	2	<b>Prozess und Risikokontrollmaßnahmen</b> <sup>79</sup>	
RI:E01		<input type="checkbox"/> Der Risikomanagementprozess ist entweder in den Entwicklungsprozess eingewebt oder nimmt auf dessen Phasen Bezug.	
RI:E02		<input type="checkbox"/>  Das Risikomanagement wird bei Software-Änderungen wiederholt <sup>80</sup> . Wählen Sie dazu eine Problemmeldung, lassen Sie sich demonstrieren, welche Teile der Anwendung geändert wurden und wo dokumentiert ist, dass die Risiken, die durch diese Änderungen entstehen, kontrolliert sind.	
RI:E03		<input type="checkbox"/> Die Folgen einer Risikokontrollmaßnahme werden berücksichtigt. Insb. wird geprüft, ob neue Gefährdungssituationen entstehen <sup>81</sup> . Dies ist üblicherweise schwer zu auditieren und kann am ehesten anhand konkreter Beispiele diskutiert werden.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
		<b>Nachgelagerte Beobachtung</b> <sup>82, 83, 84</sup>	
RI:F01		<input type="checkbox"/> Der Umgang mit Fehlern und Fehlermeldungen ist beschrieben <sup>85</sup> . Dazu gibt es einen Prozess, idealerweise ein unterstützendes IT-System.	
RI:F02		<input type="checkbox"/> Die BfArM-Meldungen werden mindestens vierteljährlich ausgewertet.	
RI:F03		<input type="checkbox"/> Updates oder Änderungen von Fremdkomponenten (SOUPS) einschließlich Fehlerlisten werden mindestens vierteljährlich ausgewertet <sup>86</sup> . Lassen Sie sich die Liste der Fremdkomponenten zeigen und bitten Sie für eine, diese Auswertung zu zeigen. Überprüfen Sie ggf. die Webseite des Herstellers.	
RI:F04		<input type="checkbox"/>  Die Fehlermeldungen und Rückfragen beim Support werden kontinuierlich schriftlich/elektronisch erfasst.	
RI:F05		<input type="checkbox"/> Die Fehlermeldungen werden mindestens vierteljährlich <ul style="list-style-type: none"> <li><input type="checkbox"/> klassifiziert<sup>87</sup>,</li> <li><input type="checkbox"/> auf Behebung geprüft<sup>88</sup>,</li> <li><input type="checkbox"/> auf Trends bewertet<sup>89</sup>,</li> <li><input type="checkbox"/> daraufhin untersucht, ob sich daraus eine Neubewertung des Risikos ergibt,</li> <li><input type="checkbox"/> auf Möglichkeiten zur Verbesserung (des Prozesses, der Methoden etc.) untersucht.</li> </ul>	
RI:F06		<input type="checkbox"/> Kritische Fehler wurden nachweisbar dem Kunden und ggf. den Behörden gemeldet.	


Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
RI:F07		<input type="checkbox"/> Es gibt eine Liste an Dokumenten (neue und überarbeitete Normen, Literatur), die für die Neubewertung des Risikos berücksichtigt wurden <sup>90</sup> .	
	1	<b>Versionsmanagement</b> <sup>91, 92, 93</sup>	
VM:A01		<input type="checkbox"/>  Es existiert ein Versionsmanagement-Werkzeug. Dies wird auch eingesetzt (Datum der letzten Aktualisierung prüfen) <sup>94</sup> .	
VM:A02		<input type="checkbox"/>  Im Versionierungssystem sind alle Beteiligten als Nutzer angelegt (Prüfen: Werden alle Entwickler genannt? Und keine Gruppennamen?)	
VM:A03		<input type="checkbox"/> Im Versionierungssystem finden sich Tests bzw. Testskripte, Testdaten, Testspezifikationen, Build-Skripte, Dokumentation, Testergebnisse.	
VM:A04		<input type="checkbox"/> Jede Softwareversion ist eindeutig durch eine Versionsnummer identifiziert. Diese Nummer enthält mindestens die Angaben Major, Minor und Revision/Build-Nummer <sup>95</sup> .	
VM:A05		<input type="checkbox"/>  Im Versionierungssystem ist erkenntlich, welche Version eines Artefakts zu welcher Version der Software gehört. Dies beinhaltet auch das Handbuch, Trainingsunterlagen, Online-Hilfe, Testdaten, Testergebnisse <sup>96</sup> . Lassen Sie sich dies exemplarisch demonstrieren.	
VM:A06		<input type="checkbox"/> Nicht freigegebene Versionen sind als solche gekennzeichnet und enthalten den Hinweis, dass sie nicht im produktiven Einsatz benutzt werden dürfen <sup>97, 98</sup> .	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
VM:A07		<input type="checkbox"/> Das Versionierungssystem verbindet die Versionen der Software mit denen des Risikomanagements.	
VM:A08		<input type="checkbox"/> Fremdkomponenten (SOUPs) sind ebenfalls unter Versionskontrolle.	
VM:A09		<input type="checkbox"/> Problembereiche sind archiviert.	
	2	<b>Build-Management</b> <sup>99</sup>	
VM:B01		<input type="checkbox"/>  Aus den Artefakten wird automatisch eine lauffähige Software erzeugt. Dazu existieren ein oder mehrere Build-Skripte. Lassen Sie sich diese zeigen.	
VM:B02		<input type="checkbox"/> Vorhergehende Versionen lassen sich reproduzieren.	
	2	<b>Freigabe</b> (Produkt und Prozess) <sup>100, 101</sup>	
VM:C01		<input type="checkbox"/>  Für alle Freigabe wird bescheinigt, dass alle Tests erfolgreich durchgeführt wurden.	
VM:C02		<input type="checkbox"/> Nicht behobene Fehler sind dokumentiert und als unkritisch bewertet. Dabei werden die Ergebnisse der Modultests, Systemtests und Abnahmetests ausgewertet. Lassen Sie sich die Ergebnisse der automatisierten Tests zeigen. Prüfen Sie, ob der automatisch erzeugte Bericht zur der frei gegebenen Softwareversion Fehler meldet.	
VM:C03		<input type="checkbox"/>  Die finale Risikobewertung und erfolgreiche Implementierung der Risikokontrollmaßnahmen ist kontrolliert und bestätigt. Prüfen Sie, ob dabei Produkte der Konkurrenz mit gleichem oder mit alternativen Verfahren in Betracht gezogen werden.	


Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
VM:C04		<input type="checkbox"/> Die Freigabe benennt die Software-Version.	
VM:C05		<input type="checkbox"/> Es existiert eine Liste mit allen freigegebenen Versionen <sup>102</sup> .	
	2	<b>Änderungen</b> <sup>103</sup>	
VM:D01		<input type="checkbox"/>  Änderungen an der Software dürfen nur nach Genehmigung erfolgen. Lassen Sie sich zeigen, wie gemeldete Probleme zur Korrektur freigegeben sind. Falls die Probleme nicht behoben sind, muss dokumentiert sein, weshalb nicht.	
VM:D02		<input type="checkbox"/> Bei Änderungen an der Software wird die Risikoanalyse überprüft und das Ergebnis dokumentiert.	
VM:D03		<input type="checkbox"/> Änderungswünsche werden bewertet. Diese Bewertungen werden dokumentiert <sup>104</sup> .	
VM:D04		<input type="checkbox"/> Änderungen, die kritische Fehler beheben, werden Kunden und ggf. Behörden mitgeteilt <sup>105</sup> .	
VM:D05		<input type="checkbox"/> Die Quelle von Änderungswünschen ist bekannt. (Anmerkung: Quelle für einen Änderungswunsch können z.B. Fehlerberichte, Marktanalysen oder Kundenrückmeldungen sein) <sup>106</sup> .	




**GEBRAUCHSTAUGLICHKEIT**<sup>107</sup>


Die meisten Forderungen zur Gebrauchstauglichkeit sind in anderen Kapiteln, beispielsweise zum Risikomanagement eingearbeitet.

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
		<b>Gebrauchstauglichkeitsakte</b>	
GT:A01		<input type="checkbox"/>  Es gibt eine Gebrauchstauglichkeitsakte <sup>108</sup> .	
GT:A02		<input type="checkbox"/> Diese enthält Verweise auf die Zweckbestimmung	
GT:A03		<input type="checkbox"/> Diese enthält Verweise auf die Spezifikation der Gebrauchstauglichkeit	
GT:A04		<input type="checkbox"/> Diese enthält Verweise auf die Verifizierung der Gebrauchstauglichkeit	
GT:A05		<input type="checkbox"/> Diese enthält Verweise auf die Validierung der Gebrauchstauglichkeit	
GT:A06		<input type="checkbox"/> Diese beschreibt oder nennt die Verfahren zur Verifikation und Validierung	
GT:A07		<input type="checkbox"/> Diese enthält Verweise auf das Risikomanagement	
GT:A08		<input type="checkbox"/> Diese enthält Verweise auf die Produktdokumentation	
GT:A09		<input type="checkbox"/> Diese enthält Verweise auf die Spezifikation des Produkts (v.a. Nennung der häufig verwandten und sicherheitskritischen Funktionen)	

**PRODUKTEIGENSCHAFTEN**

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	3	<b>Datensicherheit</b> <sup>109</sup>	
PE:A01		<input type="checkbox"/> Das System hat einen eigenen Backup-Mechanismus. Alternativ ist beschrieben, wie die Daten sonst gesichert werden.	
PE:A02		<input type="checkbox"/> Das System führt ein Auditlog, das einen Zeitstempel, angemeldeten Benutzer, durchgeführte Aktion, den alten und den neuen Wert dokumentiert.	
PE:A03		<input type="checkbox"/> Das Auditlog ist durch eine Integritätsprüfung vor Manipulation geschützt.	
	2	<b>Datenschutz</b>	
PE:B01		<input type="checkbox"/>  Das System kann nur mit Benutzernamen und Passwort benutzt werden.	
PE:B02		<input type="checkbox"/> Das System verbietet triviale Passwörter (z.B. mit weniger als 6 Zeichen).	
PE:B03		<input type="checkbox"/> In der Benutzerliste sind keine unpersönlichen Namen eingetragen (z.B. Abteilung A, Ärzte, Studie X).	
PE:B04		<input type="checkbox"/> Falls das System eine Fremdwartung vorsieht, ist sichergestellt, dass der Hersteller keine Patientendaten einsehen kann.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>Benutzbarkeit</b>	
PE:C01		<input type="checkbox"/> Es gibt eine (kontextsensitive) Hilfe.	
PE:C02		<input type="checkbox"/>  Die Beschriftungen von Feldern machen klar, was einzugeben ist. Bei Zahlen sind Einheiten genannt.	
PE:C03		<input type="checkbox"/> Die Benutzer bekommen Rückmeldung vom System, beispielsweise bei Fehleingaben, was zu tun ist.	
	3	<b>Installation</b> <sup>110</sup>	
PE:D01		<input type="checkbox"/> Die Anforderungen an die Zielhardware sind benannt.	
PE:D02		<input type="checkbox"/> Die zugelassenen Betriebssysteme bzw. Betriebssystemversionen sind dokumentiert.	
PE:D03		<input type="checkbox"/>  Der Installationsprozess ist beschrieben.	
PE:D04		<input type="checkbox"/> Es ist beschrieben, wer Systemupdates durchführen darf (z.B. Hersteller, Anwender).	
PE:D05		<input type="checkbox"/> Die Software ist in der Lage, zu überprüfen, ob sie korrekt installiert wurde <sup>111</sup> .	
	3	<b>Benutzerhandbuch</b> <sup>112, 113, 114</sup>	
PE:D01		<input type="checkbox"/>  Es gibt ein Benutzerhandbuch	
PE:D02		<input type="checkbox"/> Das Handbuch beinhaltet den bestimmungsgemäßen Gebrauch <sup>115</sup> . Dieser enthält <ul style="list-style-type: none"> <li><input type="checkbox"/> das vorgesehene Benutzerprofil,</li> <li><input type="checkbox"/> die Funktionsweise des Produkts,</li> </ul>	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
		<input type="checkbox"/> die medizinische Zielsetzung (Diagnose, Therapie, Überwachung usw.), <input type="checkbox"/> das vorgesehene Patientenkollektiv,	
PE:D03		<input type="checkbox"/> Voraussetzungen für die Anwendung: Anwender, Hardware, Betriebssystem, sonstiges Software (Virenschutz, Firewall, Datenbank, ...), Netzwerk/Internetanbindung,	
PE:D04		<input type="checkbox"/> Installation, Update, Deinstallation (falls nicht in einem eigenem Dokument beschrieben),	
PE:D05		<input type="checkbox"/> Hinweise, wie nach einer Installation die korrekte Funktionsweise des Produkts geprüft werden kann,	
PE:D06		<input type="checkbox"/> Hinweise, wie nach einem Update die korrekte Funktionsweise des Produkts geprüft werden kann,	
PE:D07		<input type="checkbox"/> (Rest-) Risiken und ggf. deren Vermeidung,	
PE:D08		<input type="checkbox"/> Handhabung des Produkts,	
PE:D09		<input type="checkbox"/> Kontaktdaten (Hersteller, Support).	
PE:D010		<input type="checkbox"/> Das Handbuch stimmt mit dem im Abschnitt „Anforderungen“ Beschriebenen überein.	
PE:D011		<input type="checkbox"/> Die Screenshots im Benutzerhandbuch stimmen mit der Anwendung überein.	
PE:D012		<input type="checkbox"/>  Das Benutzerhandbuch ist in einer Sprache geschrieben, die der typische Anwender versteht.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
PE:D013		<input type="checkbox"/> Das Benutzerhandbuch benennt die Versionsnummer der zugehörigen Software.	
PE:D014		<input type="checkbox"/> Es gibt (ggf.) Trainingsunterlagen und/oder Beschreibungen von Schulungen <sup>116</sup> .	
PE:D015		<input type="checkbox"/> Die Trainer sind qualifiziert (auch für die aktuelle Version des Produkts).	
PE:D016		<input type="checkbox"/> Der Trainingserfolg ist dokumentiert.	

**QUALITÄTSMANAGEMENT**

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	1	<b>Kontinuierliche Verbesserung durch Fehleranalyse</b> <sup>117, 118</sup>	
QM:A01		<input type="checkbox"/> <b>!</b> Es gibt ein System, in dem alle Fehler dokumentiert werden <sup>119</sup> .	
QM:A02		<input type="checkbox"/> Dieses System lässt erkennen, ob und in welchem Zeitraum die Fehler behoben wurden.	
QM:A03		<input type="checkbox"/> <b>!</b> Mindestens einmal jährlich werden Fehler, Kundenrückmeldungen und Auditergebnisse systematisch ausgewertet, Verbesserungsmaßnahmen beschlossen und die Umsetzung und Wirksamkeit früherer Verbesserungsmaßnahmen kontrolliert. Die Ergebnisse dieser Auswertung werden dokumentiert <sup>120</sup> .	
		<b>Lenkung von Dokumenten</b>	
QM:B01		<input type="checkbox"/> Jedes Dokument enthält Titel, Zweck, Zielgruppe, Freigabe, Änderungshistorie <sup>121</sup> . Prüfen Sie dies am Beispiel der Software-Anforderungen, Architektur, Gebrauchstauglichkeitsakte, Risikomanagementakte, Software- und Produktfreigabe.	
QM:B02		<input type="checkbox"/> <b>!</b> Es gibt eine Liste aller Dokumente und eine Beschreibung, wie diese gelenkt werden (d.h. es werden die Fragen beantwortet: Was ist im Versionsmanagementsystem? Wer gibt ein Dokument frei?).	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	3	<b>Werkzeuge</b> <sup>122, 123</sup>	
QM:C01		<input type="checkbox"/> Es existiert eine Liste an eingesetzten Werkzeugen einschließlich deren Version.	
QM:C02		<input type="checkbox"/> Die Entscheidung für die Auswahl der Werkzeuge ist dokumentiert.	
QM:C03		<input type="checkbox"/> Gekaufte Werkzeuge wurden validiert <sup>124</sup> .	
QM:C04		<input type="checkbox"/> Gekaufte Werkzeuge werden in regelmäßigen Abständen auf Fehlerberichte überprüft <sup>125</sup> .	
QM:C05		<input type="checkbox"/> <b>!</b> Eigenentwickelte Werkzeuge wurden verifiziert und validiert. Lassen Sie sich eine Liste aller Werkzeuge geben. Befragen Sie dann die Entwickler, welche diese verwenden. Fragen Sie nach, welche davon selbst entwickelt sind	
QM:C06		<input type="checkbox"/> Es steht eine dedizierte Testumgebung zur Verfügung.	
QM:C07		<input type="checkbox"/> Es ist dokumentiert, mit welcher Version der Werkzeuge die Tests durchgeführt wurden <sup>126</sup> .	
		<b>Einkauf</b> <sup>127, 128</sup>	
QM:D01		<input type="checkbox"/> <b>!</b> Gekaufte Fremdkomponenten SOUPs wurden validiert. Lassen Sie sich die Liste der Fremdkomponenten zeigen.	
QM:D02		<input type="checkbox"/> Der Hersteller wurde im Hinblick auf seine Erfahrung und auf die Reife des Produkts ausgewählt.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
	2	<b>QM-Handbuch</b>	
QM:E01	<input type="checkbox"/>	❗ Es existiert ein Qualitäts-Handbuch <sup>129</sup> .	
QM:E02	<input type="checkbox"/>	❗ Das Qualitäts-Handbuch enthält eine Beschreibung der Prozesse <sup>130</sup> (Entwicklungsprozess, Problemlösungsprozess, Risikomanagement, ...)	
QM:E03	<input type="checkbox"/>	❗ Das Qualitäts-Handbuch enthält einen Verweis auf die Beschreibung, wie Kundenrückmeldungen erfasst und ausgewertet werden <sup>131</sup> .	
QM:E04	<input type="checkbox"/>	Das Qualitäts-Handbuch enthält die Qualitätspolitik und Qualitätsziele <sup>132</sup> .	
QM:E05	<input type="checkbox"/>	Der Umgang mit Dokumenten und Aufzeichnungen ist beschrieben. Im Qualitäts-Handbuch wird darauf verwiesen <sup>133</sup> .	
QM:E06	<input type="checkbox"/>	Von Kunden zur Verfügung gestellte, vertrauliche Dokumente (wie z.B. zu implementierende Geschäftslogik, Algorithmen, Parameter) sind nur Personen zugänglich, die diese zur Umsetzung des Produkts benötigen <sup>134</sup> .	
		<b>Ausbildungsstand der Entwickler</b> <sup>135</sup>	
QM:F01	<input type="checkbox"/>	Der Software-Architekt hat idealerweise ein Hochschulstudium der Informatik absolviert.	
QM:F02	<input type="checkbox"/>	Die Mehrzahl der Entwickler verfügt über eine Aus- oder Weiterbildung in der eingesetzten Programmiersprache oder einer verwandten Sprache <sup>136</sup> .	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
QM:F03	<input type="checkbox"/>	Die Notwendigkeit und Wirksamkeit von Ausbildungsmaßnahmen wird ermittelt und dokumentiert. Prüfen Sie, wie viele Prozent der Entwickler in den vergangenen Jahren eine Weiterbildung besucht hat (Empfehlung > 10%).	
QM:F04	<input type="checkbox"/>	Bescheinigungen über Aus- und Weiterbildungsmaßnahmen der Mitarbeiter werden gesammelt und sind verfügbar.	
QM:F05	<input type="checkbox"/>	Die einschlägigen Normen wurden geschult und/oder sind bekannt.	
QM:F06	<input type="checkbox"/>	❗ Mindestens ein Software-Tester verfügt über eine entsprechende Qualifizierung.	
QM:F07	<input type="checkbox"/>	Das Entwicklungsteam verfügt über medizinische Kenntnisse oder hat Zugriff darauf <sup>137</sup> .	
QM:F08	<input type="checkbox"/>	Ein Software-Tester kann erklären, welches die beiden größten Risiken sind, die vom zu testenden Produkt ausgehen.	
	1	<b>Aufgaben</b>	
QM:G01	<input type="checkbox"/>	❗ Das Personal hat dokumentierte Verantwortlichkeiten und Aufgaben <sup>138</sup> . Das betrifft auch das Risikomanagement <sup>139</sup> .	
QM:G02	<input type="checkbox"/>	Es gibt in der Organisation mindestens die Rollen Entwickler, Tester, QMB und Reviewer <sup>140</sup> .	
QM:G03	<input type="checkbox"/>	❗ Es gilt bei Reviews das Vier-Augen-Prinzip. Lassen Sie sich dies am Beispiel der Reviews der Anforderungen, der Architektur und der Systemtests zeigen.	

Nr.	Prio.	Überprüfungskriterium	Anmerkungen Auditor
-----	-------	-----------------------	---------------------

**Wissen über QM**

- QM\_H1  Die Mitarbeiter kennen die Qualitätspolitik und die Qualitätsziele des Unternehmens<sup>141</sup>.
- QM\_H2  Der Qualitätsmanagement-Beauftragte kann seine Aufgaben nennen<sup>142</sup>.

**VORSCHLAG FÜR EINEN AUDITPLAN**

Es ist sicher nicht realistisch, alle Punkte der Checkliste in einem Audit zu prüfen. Daher sei folgendes Vorgehen vorgeschlagen:

Zu überprüfender Bereich	Audit 1	Audit 2	Audit 3	Legende
Entwicklungsprozess	++	+	0	0 Nicht prüfen + Kurze Prüfung ++ Intensive Prüfung (Audit-Schwerpunkt)  Die Tabelle ist so aufgebaut, dass pro Audit 9 „+“-Zeichen abzuarbeiten sind, wobei jeweils zwei bis drei Schwerpunkte („++“) gebildet werden. Jeder der wichtigsten Bereiche wird einmal schwerpunktmäßig geprüft.
Zweckbestimmung, Anforderungsanalyse, Funktionale Spezifikation	+	++	+	
Architektur, Implementierung, Testen	+	+	++	
Risikomanagement	++	+	+	
Gebrauchstauglichkeit	+	++	0	
Version, Build, Release und Konfigurationsmanagement	+	0	++	
Produkteigenschaften	+	+	+	
Qualitätsmanagement	0	+	++	

## DIE KLEINE CHECKLISTE FÜR GXP AUDITS

Die folgende Checkliste ergibt sich aus der Auswertung zahlreicher Audits im FDA-Umfeld. Sie enthält Fragen, denen sich ein Auditierter stellen können muss. Wären auch sie dazu in der Lage?

Beachten Sie auch das nachfolgende Kapitel, das konkrete Beanstandungen in Form von Warning Letters nennt.

- If I press M, how can I be sure that M arrives at the server?
- In data center: Is that server qualified?
- Do you have an overall assessment of the network security risks?
- What are the measures to secure your network?
- Could you show me your WAN documentation?
- Is that networks sketch still up to date? Where do I find this device in that sketch?
- How did you validate your WAN?
- Where and how do you document changes to your network components?
- Are there no GxP relevant devices connected by the network? How do you make sure that these devices are not overburdening your network's capacity?
- Are there vendors directly accessing your machines?
- How do you restrict access to the data center? Who has a key? Where is that documented?
- How do you ensure that your air conditioning in the data center is working?
- Where do you store your data? How often? What backup strategy do you have?
- Which parts of your IT infrastructure did you outsource? Can I see the contracts and operation procedures?
- What would happen if I accidentally enter a wrong number here? Could I correct that? How can I see later when this mistake was done (and corrected), and by whom?
- Who did release this document? How did you make sure that the previous version is not used any more.
- Please show me the organigram, your SOPs, ...
- Can I see the protocols (measurement) for your network installation?
- How do you ensure that this file format still can be read in x years?
- How did you validate your backup procedure?
- Can I have the system inventory, risk assessment?
- Select a networked system with high impact on product quality.

## DIE KLEINE CHECKLISTE FÜR GXP AUDITS

- Can I have the description of the system, its intended use and specifications (user requirement and functional)?
- Can I have the network qualification plan?
- Can I have the qualification summary report?
- Verify if the network infrastructure is documented.
- Ask for topological diagrams.
- Check procedures for system security.
- Ask for password convention ( number of characters, expiration).
- Check if authorized access has been validated.
- Do you have a list of authorized users?
- Is the list updated?
- Has it been signed?
- Check user specific time-outs or equivalent – „What happens if a user walks away from the system?“
- Ask which operating system and application software and which versions are being used.
- Ask what the difference is to the previous software version and how users did make sure, that the new version worked as intended.
- Ask for change control procedure and change control documents.
- Verify that IT staff and operators have been trained (incl. GMP) and successful completion of the training has been documented.
- Ask to take you to the system you have examined before,
- Watch people at their work,
- Try to get access to the system (without password or commonly used passwords).
- Point to any network device and ask about purpose of the device.
- Ask where this is located in the diagram.
- Who has installed this software? When? Why? Who gave authorization?
- (to IT professional to check knowledge of GMP regulations) „What is your company's approach for...“?
  - Manufacturing site master plan
  - Laboratory
  - Training
  - Validation (computer, networks, equipment)

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

Dieses Kapitel nennt Beispiele für konkrete Beanstandungen bei FDA Audits.

**VALIDATION, DQ, IQ, OQ, PQ**

Your firm failed to establish and maintain procedures to ensure that equipment is routinely calibrated, inspected, checked, and maintained.

Failure to assure that when computers or automated data processing systems are used as part of the production or quality system the manufacturer shall validate computer software for its intended use according to an established protocol, as required by 21 CFR 820.70(i). For example, electronic records are used, but there was no software validation. No procedures are established to validate for its intended purpose the Microsoft Word or Microsoft Excel software used in creating and maintaining nonconformance records, product return records, internal audit corrective action records, or preventive action records

Inspection and Testing of Manufacturing Equipment, xxx do not fully describe the requirements for equipment qualification, including environmental conditions for equipment operation

Lacks documentation of installation and operation qualification of equipment

The Validation Master Plan does not contain an operational qualification

There is no requirement for a Performance Qualification protocol  
There was no validation showing this configuration to be acceptable

Validation of the system did not include critical system tests such as volume, stress, performance, boundary, and compatibility

Failure to use fully validated computer spreadsheets to calculate analytical results for in-process and finished product testing [21 CFR 211.165(e)]. For example, the computer spreadsheets used to calculate analytical results for... have not been validated.

Spreadsheet Validation, is deficient in that only a small range of values are being used to challenge computerized spreadsheet mathematical calculations.

The functional, operational and security features of the data acquisition and storage ... software have not been challenged or validated for accuracy or for reliability

No validation after hardware and software upgrades and configuration changes

The firm does not have a written procedure that includes requirements for the performance verification of HPLC and GC systems

Acceptance test results for the xxx System were not adequately documented

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

Specifically, final acceptance records for release of the xxx System did not document the results of the acceptance activities or equipment/software used in conducting the tests, and were not signed by the individual who performed the acceptance activities  
A manufacturer is required to validate computer software for its intended use according to an established protocol. For example, databases that are maintained for data analysis and other tracking and trending functions, including complaint and services access databases, have not been validated for their intended use.

For example, your firm has not validated the software used to produce labels

Failure to adequately validate the intended use of this PC and its software, as required by 21 CFR 820.70(i).

**DATA SECURITY (BACK-UP, CONFIDENTIALITY, AUDIT TRAIL, COMPLETENESS)**

For example: the dedicated PC [redacted] attached to the [redacted] was not secure in that access to the data on [redacted] was not granted by a unique username and password or equivalent method; there was no documentation associated with the electronic data for whom was responsible for collection of the analytical results as several quality control personnel have access to the [redacted] no software changes in the study data could be detected as there was no audit trail capability; and finally, the electronic data did not correlate with the paper records.

Records are not maintained so that the data can be reviewed annually

The functional, operational and security features of the data acquisition and storage ... software have not been challenged or validated for accuracy or for reliability

Data transfer of a client server system not validated

Additionally, please provide copies of your written procedures describing system security

No current listing of individuals who have access to the database program or to what level of access each individual has

Failure to establish and implement adequate security in allowing the software vendor unrestricted modem access and not consistently documenting this access

Laboratory records do not include all raw data. For example, weights determined during the preparation of standard solutions were not recorded

Appropriate controls are not exercised over computers or related systems to assure that changes in analytical methods or other control records are instituted only by authorized personnel [21 CFR 211.68(b)]

There was a failure to validate the [redacted] software to assure that all data generated by the system was secure

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

User access levels for the [redacted] software were not established and documented. Currently, laboratory personnel use a common password to gain access to the system and there are no user access level restrictions for deleting or modifying data. Furthermore, your system does not have an audit trail to document changes.

There was no raw data to substantiate all computer generated tables generated for the Preservative Validation Report

Failure to store records so as to minimize deterioration, prevent loss and back up of automated data processing systems as required by 21 CFR 820.180.

For example: the electronic data did not correlate with the paper records; you had not established an electronic data back-up procedure; and finally, data was copied onto the server from one system to the next via floppy: therefore, no limited access or data protection had been established.

**NETWORK**

To date the firm has failed to generate and approve sufficient design control documentation for complete definition of the network (i.e. high level diagrams identifying all sites/equipment making up the network)

Data transfer of a client server system not validated

The xxxx computer system is currently used to manage the computer network. The firm has no procedure defining the use of the system

(Networked) system testing was not conducted to ensure that each system as configured could handle high sample rates.

Validation of the (networked) system did not include critical system tests such as volume, stress, performance, boundary, and compatibility

The network ... module design limitations, which can only support up to four chromatographic acquisition systems, had up to five chromatographic systems connected. There was no validation showing this configuration to be acceptable

Wide Area Network diagrams (WAN) with appropriate definition documentation identifying corporate sites on the network that use XXX have not been included in any XXX validation documents

There was a failure to validate the [redacted] software to assure that all data generated by the system was secure

Additionally, please provide copies of your written procedures describing system security.

No current listing of individuals who have access to the database program or to what level of access each individual has.

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

Failure to establish and implement adequate security in allowing the software vendor unrestricted modem access and not consistently documenting this access.

There are no records to document that the Information Technology (IT) service provider staff personnel have received training that include current good manufacturing practice regulations and written procedures referred by the regulations.

**RISK MANAGEMENT, IMPACT ANALYSIS**

For example, a formal risk analysis of the original system design and software changes to correct software bugs that caused incorrect functionality or performance problems, and to enhance the product, has not been documented.

Although your software release notes briefly describe the nature of unresolved software bugs in a particular software version, they do not explain the impact of these software bugs on user needs and intended uses

**CHANGE MANAGEMENT**

The designated project leader did not maintain or update the file as required by your firm's design control procedure. There were unsigned computer generated copies for design activities (e.g. approval of design output, approval of 12/31/03 minutes for release of device to market).

System design documentation has not been maintained or updated throughout of the software dating back to 1985 despite significant changes and modification that have taken place

No validation after hardware and software upgrades and configuration changes

Written procedures to differentiate between revision or version changes are not employed

There was inadequate software version control

Failure to document changes to written specifications

**QUALITY MANAGEMENT AND DOCUMENTATION IN GENERAL**

You have failed to establish a policy of overall intentions and direction of your firm with respect to quality

Management with executive responsibility has not established a quality policy and objectives

Other FDA reports mention that SOPs are not available, not adequate or are not followed.

During the inspection, our investigation requested to see investigations of process deviations and out of specification laboratory results. She was informed that these investigations are conducted but not documented

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

These diagrams are not dated, have no document controls number, and have no indication of review or approval

There is no record to document that the protocol was reviewed and approved

There is no documentation of the Batch Production Records being reviewed and approved by the Quality Control Unit

**TRAINING**

There is no evidence that all laboratory personnel have been observed annually for performance competency as required by the „Training Program“ procedure for the production laboratory and the “Training Program” procedure for the compliance department

Employee training needs were not addressed and training was not documented

There are no records to document that the Information Technology (IT) service provider staff personnel have received training that include current good manufacturing practice regulations and written procedures referred by the regulations

Your firm fails to have sufficient personnel with the necessary training to assure that all activities required by ... are correctly performed

Your formalized training program is inadequate in that it does not address current good manufacturing practices

Failure to ensure that the quality policy is understood, implemented, and maintained at all levels of the organization, as required by 21 CFR 820.20(a).

Your firm’s response [...] stated that it would retrain employees. There was no documented assurance that training occurred or when it would occur.

There are no procedures defining training, qualification, disqualification and requalification of sterility suite operators when they exceed the microbial limits defined

There are no cGMP training SOPs in place and at least one employee denied knowledge of cGMP regulations

Your firm failed to establish procedures identifying training needs and/or criteria to be met that ensure that all personnel are trained adequately to perform their assigned responsibilities as required by 21 CFR 820.25. Training is also not documented

Further, your supervisory employees have not documented any of their subordinates as being qualified to execute the analytical work to which they have been assigned

The center director had not received any training on this computers system even though he retains a high security level for data entered on this computer system

## FRAGEN UND BEANSTANDUNGEN BEI FDA AUDITS

Failure to effectively train employees in laboratory operations to assure that original records are accurate, complete and in compliance with established specifications.

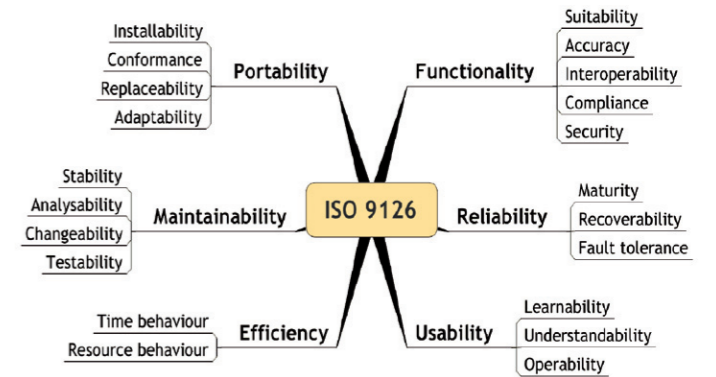
Our investigator noted the training record checklists for two production laboratory employees did not use the defined checklists. One employee’s record had three checklists, which differed from the procedure’s checklist, while the other employee’s record had two lists that differed.

**HINWEISE VON 1 – 20**

- 1 ISO 13485 Kapitel 7.3.1
- 2 IEC 62304 Kapitel 5.1.1
- 3 FDA Software Validation Kapitel 4.4 und 4.5
- 4 IEC 62304 Kapitel 5.1.1
- 5 IEC 62304 Kapitel 6 in Gänze
- 6 Laut FDA werden 70% (!) der Fehler in einer Nachfolgeversion eingeführt. D.h., bei der Weiterentwicklung einschließlich Bug-Fixing muss die gleiche Sorgfalt angewendet werden wie bei der Erstentwicklung. Die IEC 62304 fordert einen Softwarewartungsprozess, der dem Entwicklungsprozess nahezu gleicht. Die 62304 kennt drei Risikoklassen, die unterschiedlich intensive Grade an Überprüfung bedeuten.
- 7 IEC 62304 nennt drei Software-Sicherheitsklassen (A, B, C), die FDA ebenfalls (minor, moderate, major level of concern).
- 8 IEC 62304 Kapitel 5.2
- 9 IEC 62304 Kapitel 5.8
- 10 GAMP Testing of GxP systems Appendix T1.2, FDA
- 11 ISO 13485 Kapitel 7.2.1 verlangt, dass die Kundenanforderungen (auch die nicht explizit formulierten – typischerweise nicht-funktionale Anforderungen) bestimmt werden
- 12 Die IVENA Datenbank liefert eine umfassende Checkliste für nicht-funktionale Anforderungen.
- 13 IEC 62304 Kapitel 5.2 für den Fall, dass Software mit dem Produkt identisch und nicht ein Teil dessen ist. Als nicht funktionale Anforderungen nennt sie explizit Zielhardware und Timing-Anforderungen
- 14 FDA Software Validation Kapitel 5.2.2
- 15 Der DATech Leitfaden Usability sei zur weiteren Lektüre empfohlen. Erfordernisse („implied needs“) können Sie mit Sätzen formulieren wie „Der <Rollenbezeichnung> muss <Voraussetzung> <Verb, z.B. haben/kennen/tun können/ usw.>, um <Beschreibung des zu erreichenden Zwecks>. Erfordernisse haben nichts mit einem System zu tun.  
  
Hingegen formuliert man Anforderungen wie folgt: <Rollenbezeichnung> muss am System <sehen, eingeben, angezeigt bekommen>. Dabei wird das System aber noch nicht im Detail spezifiziert.
- 16 ISO 13485 Kapitel 7.2.1a
- 17 IEC 62366 Kapitel 5.1
- 18 IEC 62366 Kapitel 5.1
- 19 Setzen Sie hierzu Kontextinterviews mit mindestens 4 Personen ein. Formulare und Personen, mit denen die Benutzer zusammenarbeiten, geben Ihnen wichtige Hinweise auf Arbeitsergebnisse.
- 20 IEC 62366 Kapitel 5.1

**HINWEISE VON 21 – 43**

- 21 IEC 62366 Kapitel 5.4. Ein Beispiel wäre „X% der Benutzer können in weniger als Y Minuten die Aufgabe Z am System erledigen.“
- 22 ISO 13485 Kapitel 7.2.2
- 23 IEC 62304 Kapitel 5.2
- 24 IEC 60601-1-6 Kapitel 7.1.1
- 25 PIC/S Kapitel 10.2
- 26 IEC 62304 Kapitel 5.2
- 27 IEC 62366 Kapitel 5.4
- 28 IEC 62366 Kapitel 5.5
- 29 FDA Software Validation Kapitel 4.1
- 30 IEC 62304 Kapitel 5.1.1c. Es gibt auch bei reinen Softwareprodukten Systemanforderungen, die nicht in Software realisiert sind, z.B. Handbuch.
- 31 ISO 13485 Kapitel 7.3.2
- 32 IEC 62304 Kapitel 5.2, 5.3 und 5.4. Wir haben hier nicht zwischen Softwarearchitektur und Feinentwurf unterschieden.
- 33 IEC 62304 Kapitel 5.4.1
- 34 IEC 62304 Kapitel 8.1.2
- 35 IEC 62304 Kapitel 5.3.3, 5.3.4
- 36 IEC 62304 Kapitel 5.1.5
- 37 IEC 62304 Kapitel 4.3
- 38 IEC 62304 Kapitel 5.3.6
- 39 FDA Software Validation Kapitel 3.5
- 40 IEC 62304 Kapitel 5.5
- 41 IEC 62304 Kapitel 5.5.2
- 42 IEC 62304 Kapitel 5.6.7, 5.7.5
- 43 Die ISO 9126 ist nicht normativ, dennoch benennt sie wichtige Qualitätskriterien von Software:



## HINWEISE VON 44 – 77

44	IEC	62	IEC 62366 Kapitel 5.6
45	GA	63	IEC 62366 Kapitel 5.6
46	FD	64	IEC 62366 Kapitel 5.9
47	IEC	65	ISO 13485 Kapitel 7.3.6, MDD Anhang I 6a.
48	FD	66	IEC 62304 Kapitel 4.3c
49	IEC	67	IEC 62366 Taxonomien an Handlungen
50	ISO	68	ISO 14971 Kapitel 4.2, 4.3
51	IEC 62304 Kapitel 5.6	69	Die Liste umfasst die Software-spezifischen Gefährdungen. Sie sollte durch Gefährdungen ergänzt werden, die spezifisch für eine eventuell angesteuerte Hardware bzw. ein externes Medizinprodukt sind.
52	PIC/S Kapitel 13.2	70	IEC 62366 Kapitel 5.2-5.4
53	IEC 62304 Kapitel 5.1.5	71	IEC 62366 Kapitel 5.5
54	ISO 13485 Kapitel 7.3.6	72	ISO 14971 Kapitel 2.2, 2.4
55	IEC 62304 Kapitel 5.7	73	IEC 62366 Kapitel 5.3.2
56	GAMP Testing of GxP systems Appendix T1: 2, 3.2, 3.3.4 und T2: 3.1, 4.4 und T3: 2.2	74	IEC 62304 mehrfach, beispielsweise Kapitel 7.1
57	IEC 62304 Kapitel 5.2.3, 5.7.1, 5.7.4	75	IEC 62304 Kapitel 7.3.3
58	IEC 62366 Kapitel 5.8	76	IEC 62304 Kapitel 5.3.5
59	IEC 60601D1 (Kapitel zur Verifikation und Validierung)	77	Konfigurationen finden sich in Konfigurationsdateien, Inhalte von Datenbanken oder in Skripten.
60	ISO 13485 Kapitel 7.3.3c		
61	IEC 62366 Kapitel 5.6		

## HINWEISE VON 78 – 105

78	IEC 62304 Kapitel 8	92	IEC 62304 Kapitel 8, 5.7.5, 5.8.7, 8.1, 9.5
79	ISO 14971 allgemein	93	GAMP Testing of GxP systems Appendix T6
80	IEC 62304 Kapitel 7.4	94	Typische Versionsmanagementsysteme sind CVS, Subversion (SVN), Visual SourceSafe und ClearCase.
81	IEC 62304 Kapitel 7.3.2	95	ISO 13485 Kapitel 7.5.3.1
82	ISO 13485 Kapitel 7.2.3 verlangt, dass Kundenbeschwerden bestimmt werden.	96	IEC 62304 Kapitel 5.8.8
83	ISO 1385 Kapitel 8.2.1	97	ISO 13485 Kapitel 7.5.3.3
84	ISO 14971 Kapitel 9	98	Hinweis: Dies kann z.B. durch ein Flag im Buildprozess erreicht werden. Falls eine Software freigegeben werden soll, verschwindet abhängig von diesem Flag beispielsweise im Splash Screen ein entsprechender Warnhinweis. Alternativ kann die Freigabe auf die Freigabe von DVDs/CDs beschränkt werden.
85	IEC 62304 Kapitel 6.1f, 6.2.2, 6.2.3	99	IEC 62304 Kapitel 5.8
86	IEC 62304 Kapitel 6.1f	100	ISO 14971 Kapitel 7 und 8
87	Beispiele für Klassen können sein: Art des Fehler, Schwere des Fehlers, Ort des Auftretens (z.B. Geschäftslogik, Datenbank, Kommunikation), Phase, in der Fehler eingeführt wurde, Phase, in der Fehler hätte gefunden werden müssen, wer den Fehler fand (Tester, Kunde, ...).	101	IEC 62304 Kapitel 5.8, 6.3.2
88	IEC 62304 Kapitel 9.1, 9.2 und 9.6	102	IEC 62304 Kapitel 5.8.4
89	IEC 62304 Kapitel 9.3	103	IEC 62304 Kapitel 6
90	ISO 14971 Kapitel 9	104	IEC 62304 Kapitel 6.2.3, 6.2.4
91	ISO 13485 an vielen Stellen, beispielsweise Kapitel 7.3.5 und 7.3.7	105	IEC 62304 Kapitel 6.2.5

## HINWEISE VON 106 – 135

- <sup>106</sup> IEC 62304 Kapitel 8.2.4
- <sup>107</sup> Die meisten Aspekte sind bereits in den Kapiteln zur Gebrauchstauglichkeit, zur Spezifikation, zu den Anforderungen und zur Risikoanalyse behandelt.
- <sup>108</sup> IEC 62366 Kapitel 4.2. Die Akte kann auf andere Dokumente verweisen, beispielsweise auf die Risikoanalyse, Spezifikation, Anforderungsanalyse.
- <sup>109</sup> PIC/S Kapitel 20
- <sup>110</sup> ISO 13485 Kapitel 7.3.3, 7.5.1.1, 7.5.1.2.3
- <sup>111</sup> ISO 13485 Kapitel 7.5.1.2.2
- <sup>112</sup> ISO 14971 Kapitel 4.2
- <sup>113</sup> ISO 13485 Kapitel 7.5.1
- <sup>114</sup> IEC 60601-1-6 Kapitel 6
- <sup>115</sup> IEC 62366 Kapitel 7
- <sup>116</sup> IEC 62366 Kapitel 7
- <sup>117</sup> Siehe auch Risikomanagement – nachgelagerte Beobachtung
- <sup>118</sup> PIC/S Kapitel 18 (teilweise)
- <sup>119</sup> ISO 13485 Kapitel 8.2.1
- <sup>120</sup> ISO 13485 Kapitel 8.2.2, 5.6
- <sup>121</sup> IEC 62304 Kapitel 5.1.8, ISO 13485 Kapitel 4.2
- <sup>122</sup> ISO 13485 Kapitel 7.6
- <sup>123</sup> FDA Software Validation Kapitel 6.3
- <sup>124</sup> Die FDA verlangt sogar, dass eigenentwickelte Werkzeuge den gleichen Qualitätssicherungsmaßnahmen unterliegen wie die zu entwickelnde medizinische Software.
- <sup>125</sup> ISO 13485 Kapitel 7.6
- <sup>126</sup> IEC 62304 Kapitel 5.1.4
- <sup>127</sup> ISO 13485 Kapitel 7.4.1, 7.4.2 und 7.4.3
- <sup>128</sup> GAMP Testing of GxP systems Appendix C1.1
- <sup>129</sup> ISO 13485 Kapitel 4.2.2
- <sup>130</sup> ISO 13485 Kapitel 4.2.2c, 7.3.1
- <sup>131</sup> ISO 13485 Kapitel 8.2.1
- <sup>132</sup> ISO 13485 Kapitel 4.2.1a
- <sup>133</sup> ISO 13485 Kapitel 4.2.3, 4.2.4
- <sup>134</sup> ISO 13485 Kapitel 7.5.4
- <sup>135</sup> Forderungen nach einer dokumentierten Ausbildung des Personals finden sich beispielsweise im GMP Annex 11, FDA Guidance Clinical Trails, 21 CFR part 11, ISO 13485 Kapitel 6.2 und 7.3.4.

## HINWEISE VON 136 – 142

- <sup>136</sup> Unter verwandter Programmiersprache sind beispielsweise die Vertreter objektorientierter Sprachen oder die Vertreter von Skriptsprachen zu verstehen. So sind die Sprachen Java und C#, PHP und ASP und mit Einschränkungen auch C und C++ als verwandt zu sehen.
- <sup>137</sup> ISO 14971 Kapitel 3.2 und 3.3
- <sup>138</sup> ISO 13485 Kapitel 6.2.2
- <sup>139</sup> ISO 14971 Kapitel 3.4
- <sup>140</sup> ISO 13485 Kapitel 7.3.1c
- <sup>141</sup> ISO 13485 Kapitel 5.3
- <sup>142</sup> ISO 13485 Kapitel 5.5.2



A series of horizontal dotted lines for writing notes, filling the main body of the page.



A series of horizontal dotted lines for writing notes, filling the main body of the page.

