Checkliste

2-040

V1.0

Audit

Dokument Typ Checkliste	Dokument Titel Checkliste Audit	Dokument Nr. 2-040
Gültig ab:		Version 1.0

	Name	Unterschrift	Datum
Autor:			
Prüfung:			
Prüfung:			
Genehmigung:			

Ersetzt Dokument Nr.:

Änderungshinweise:

Zusammenfassung:
Diese Checkliste dient zur Unterstützung von Fremd- und Selbstaudits.

Folgende Ziele werden mit dieser Bewertung verfolgt:

- Sicherstellung der Voraussetzungen für einen validen Zustand
- Erhöhung der Transparenz
- Kontinuierliche Leistungsüberprüfung der Forschungsverbünde.

Anzahl Seiten: 81

Dokument Typ Checkliste	Dokument Titel Checkliste Audit	Dokument Nr. 2-040
Gültig ab:		Version 1.0

Inhaltsverzeichnis:

ALLGEMEINE INFORMATIONEN

Auditierte Einheit (Name und Adresse):

_____

System / Software: _____

Projekt / Zweck: _____

Beim Audit anwesend:

_____

****

Auditor(en): _____

Datum des Audit: _____

Datum des Berichts: _____

Bericht von:

_____

(Name und Adresse)

Auditresultate berichtet an:

_____

Einschl. Bericht: ja ☐ nein ☐

(Abkürzungen siehe Bericht).

1 ZWECK

Diese Checkliste enthält im ersten Teil einen allgemeinen Teil zum Audit computergestützter Systeme. Der zweite Teil umfasst Erläuterungen zu den Anforderungen des Anhangs 11 und Fragen, die bei einem Audit gestellt werden können, welche kommentiert sind. Die Kommentare sollen als Grundlage für die Bewertung der erhaltenen Antworten dienen. Diese Struktur soll den Einstieg in die Inspektion computergestützter Systeme (CS) erleichtern.

Die Gliederung des Fragen-und Kommentierungsteiles richtet sich nach dem Aufbau des Anhangs 11 „Computergestützte Systeme“ des EU GMP-Leitfadens. Der Text der deutschen Übersetzung des Anhangs 11 wird den jeweiligen Fragen bzw. Kommentierungen in kursiv vorangestellt. Soweit erforderlich, wird auf die relevanten Abschnitte des revidierten Kapitels 4 „Dokumentation“ des EU GMP-Leitfadens verwiesen.

Die Checkliste enthält zudem einen Abschnitt Definitionen und Abkürzungen, in dem das Glossar aus dem Anhang 11 des EU GMP-Leitfadens enthalten ist. Die Terminologie kann in einzelnen Unternehmen von den hier verwendeten Begriffen abweichen. Beispielsweise werden in Übereinstimmung mit Anhang 11 die Begriffe „Validierung“ und „Qualifizierung“ und nicht der Begriff „Verifizierung“ verwendet.

Die stetige Weiterentwicklung von Regelungen für den Bereich computergestützter Systeme kann in dieser Checkliste nicht immer aktuell abgebildet werden. Die Checkliste wird periodisch aktualisiert.

2 ALLGEMEINES

2.1 Personal

Es sollte eine enge Zusammenarbeit zwischen maßgeblichen Personen, wie z. B. Prozesseignern, Systemeignern und Sachkundigen Personen sowie der IT stattfinden. Alle Personen sollten über eine geeignete Ausbildung und Zugriffsrechte sowie festgelegte Verantwortlichkeiten zur Wahrnehmung der ihnen übertragenen Aufgaben verfügen.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Das gesamte Personal soll bezüglich der Verwendung und des Umgangs mit Computersystemen innerhalb des eigenen Verantwortungsbereichs angemessen geschult sein. Insbesondere muss beim Personal (z. B. Beschäftigte in der IT bzw. Systemadministration), das für Planung, Entwicklung, Programmierung, Validierung, Installation, Betrieb, Wartung und Außerbetriebnahme von Computersystemen verantwortlich ist, ausreichend Sachkenntnis vorhanden sein. Die Sachkenntnis sollte in regelmäßigen Abständen durch Fortbildungen vertieft werden. Zwischen allen maßgeblichen Personen sollte eine enge Zusammenarbeit stattfinden.					
	Zur Wahrnehmung der Aufgaben sollten alle Mitarbeiter/innen über festgelegte Verantwortlichkeiten und angemessene Zugriffsrechte verfügen.					
	Zugriffsrechte sollten nur an Mitarbeiter/innen vergeben werden, die ausreichend geschult sind.					

	Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die diesbezüglich ausreichend geschult sind.					
2.1	Welche Qualifikation besitzt das IT-Personal?	Der Grundsatz von GMP, das Personal nur entsprechend seiner Kenntnisse und Fähigkeiten eingesetzt werden soll, gilt auch für IT-Personal.				
2.2	Wie ist das Personal geschult?	Das verantwortliche Personal hat sicherzustellen, dass die Bedienung der CS durch das eingesetzte Personal unter Beachtung der GMP-Regeln und der betriebsinternen Arbeitsanweisungen erfolgt. Das Personal, das an CS eingesetzt wird, muss mit den Arbeitsprozessen vertraut sein und muss bei Störungen die Grenzen zwischen Selbsthilfe und Inanspruchnahme von Hilfe aus dem Betrieb oder von außerhalb erkennen und beachten. Aus dem Schulungsplan sollte abzuleiten sein, dass die IT-spezifischen Themen auch abgedeckt werden.				
2.3	In welcher Art und Weise umfasst der Schulungsplan die Anforderungen an den Umgang mit computergestützten Systemen?	Das IT-Personal sollte insbesondere zur Dokumentation und zum Änderungsmanagement geschult sein.				
2.4	Welche Personen/Rollen sind festgelegt, die in Entwicklung, Planung und Implementierung von CS involviert sind?	Die Benennung von System-und Prozessverantwortlichen für komplexere CS hat sich als gute Praxis etabliert.				
2.5	Wie sind die Verantwortlichkeiten bei den involvierten Personen festgelegt?	Es kann kritisch hinterfragt werden, ob den festgelegten Verantwortlichkeiten auch die erforderlichen Kompetenzen gegenüberstehen.				

2.6	Welche Personen sind zur Eingabe oder Änderung von Daten ermächtigt?	Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die dazu ermächtigt und geschult sind. Nur Personen, die laut Arbeitsplatzbeschreibung am jeweiligen System arbeiten, sollten zur Eingabe von Daten berechtigt sein. Es kann kritisch hinterfragt werden, welche Personen Änderungen vornehmen dürfen und wie der Prozess der Änderung abläuft.				
2.7	In wieweit ist die Sachkundige Person / sind Sachkundige Personen eingebunden?	Zumindest bei der Systemfreigabe sollte, sofern freigaberelevante Daten erzeugt oder verarbeitet werden, eine Beteiligung der Sachkundigen Person(en) gegeben sein.				

2.2 Organisation

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
2.8	Sind aktuelle Organigramme der Gruppe / Firma / des Entwicklungsbereichs verfügbar?					
2.9	Hat der FV ausreichend qualifiziertes und erfahrenes Personal, um laufende und zukünftige Projekte adäquat durchführen zu können?					
2.10	Hat der FV einen stabilen finanziellen Hintergrund?					
2.11	Sind dem FV entsprechende regulatorische Anforderungen geläufig?					
2.12	Hat der FV bereits Erfahrung mit Computersystemvalidierung (CSV; mit anderen Kunden, früheren Audits, Inspektionen)?					
2.13	Liegen bereits Berichte von früheren Audits oder Inspektionen vor? (Wenn ja, unter ‚Kommentare' näher benennen)?					
2.14	Ist der FV mit weiteren Audits und/oder Inspektionen einverstanden?					
2.15	Arbeitet der FV oder ist er vertraut mit elektronischen Dokumenten/digitalen Unterschriften bzw. unterstützt er diese?					
2.16	Wenn ja, ist ein System nach FDA 21 CFR Part 11 funktionabel eingerichtet und werden die Anforderungen des Signaturgesetzes eingehalten?					

2.3 Entwicklungsstandards

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
2.17	Wird die S/W nach einem SDLC entwickelt/gewartet/weiterentwickelt? Wenn ja, nach welchem Modell?					
2.18	Gibt es einen Validierungs-Master-Plan (VMP)?					
2.19	Enthält dieser eine Risikoanalyse? Wenn ja, nach welchem Modell (z.B. FMEA, FTA)?					
2.20	Ist der SDLC eindeutig dokumentiert?					
2.21	Ist die Nachvollziehbarkeit zwischen Anwenderanforderungen, Design und S/W-Modulen dokumentiert nachgewiesen (traceability matrix)?					
2.22	Existieren Vorgaben für Datenbanksysteme?					
2.23	Gibt es Vorgaben für Source-Code-Reviews?					

2.4 Programmierstandards

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
2.24	Existieren Programmierstandards für jede Programmiersprache, die verwendet wird?					
2.25	Beinhalten die Standards folgende Details: • Namenskonventionen für Dateien? • Namenskonventionen für Variablen? • Lay-Out-Konventionen? • Versionierung (welche tools), einschl. Dokumentation/Historie? • Fehlerbehandlung? • Regeln für Kommentarzeilen? Konventionen über Plattform/ Bildschirmoberfläche?					
2.26	Wird nachgewiesen, dass diese Standards eingehalten bzw. berücksichtigt werden?					
2.27	Wird zum Review und/oder Audit der Programmierung eine unabhängige Person hingezogen, die ausreichende Programmierkenntnisse hat?					

2.5 Lieferanten und Dienstleister

Werden Dritte (z. B. Lieferanten, Dienstleister) herangezogen, um z. B. ein computergestütztes System bereitzustellen, zu installieren, zu konfigurieren, zu integrieren, zu validieren, zu warten (z. B. Fernwartung), zu modifizieren oder zu erhalten, Daten zu verarbeiten oder im Zusammenhang stehende Serviceleistungen zu erbringen, müssen formale Vereinbarungen abgeschlossen sein, in denen die Verantwortlichkeiten des Dritten eindeutig beschrieben sind. [2]IT-Abteilungen sollten analog zu Dritten behandelt werden.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
2.28	Welche Pflichten sind vertraglich vereinbart worden?	Die Vertragsgestaltung soll eindeutig sein, die Aufgaben/Verantwortlichkeiten sollen detailliert beschrieben sein. Reaktionszeiten sollen definiert sein.				
2.29	Welche Personen wurden einbezogen?	Mindestens Prozesseigner und Systemeigner sollten in die Vertragsgestaltung eingebunden sein.				
2.30	Wie werden im Unternehmen Dienstleister definiert?	Dienstleister sind alle diejenigen, die Serviceleistungen erbringen unabhängig davon, ob diese zum Firmenverbund / Konzern gehören oder nicht.				
	Kompetenz und Zuverlässigkeit des Lieferanten sind Schlüsselfaktoren bei der Auswahl eines Produktes oder eines Dienstleisters. [2]Die Notwendigkeit eines Audits sollte auf einer Risikobewertung basieren.					
2.31	Wie wurde die Bewertung des Lieferanten bzw. des Dienstleisters vorgenommen?	Es können Referenzen und Zertifizierungen des Lieferanten bzw. des Dienstleisters mit einbezogen werden. Eine Zertifizierung ersetzt keine Lieferantenbewertung. Methoden einer				

		Lieferantenbewertung sind z. B. Erfahrungsberichte bisheriger Lieferungen, Übermittlung und Auswertung von Fragebögen und Audits				
2.32	Wurde ein Audit durchgeführt?	Es sollte interne Festlegungen geben, in welchen Fällen ein Audit erforderlich ist. In der Regel wird mindestens bei Kategorie 5 Software ein Audit beim Lieferanten erforderlich sein.				
	Die bei kommerziell erhältlichen Standardprodukten bereitgestellte Dokumentation sollte durch Nutzer im regulierten Umfeld dahingehend überprüft werden, ob die Benutzer-anforderungen erfüllt sind.					
2.33	Wie wurde überprüft, ob das Standardprodukt die Benutzeranforderungen erfüllt?	Es soll ein dokumentierter Abgleich der Benutzer-anforderungen gegen die vom Lieferanten zur Verfügung gestellte Dokumentation durchgeführt werden. Abweichungen sollen einer Risikobe-trachtung unterzogen werden.				
	Die Informationen zum Qualitätssystem und zu Audits, die Lieferanten oder Entwickler von Software und verwendeten Systemen betreffen, sollten Inspektoren auf Nachfrage zur Verfügung gestellt werden.					
2.34	Die Lieferantenbewertung, das Pflichtenheft und weitere Qualifizierungsdokumente sollen chronologisch plausibel vorliegen. Auditberichte können eingesehen werden.					

2.6 Qualitätsmanagement / Dokumentation

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
2.35	Betreibt der FV eine "Qualitätspolitik"?					
2.36	Existiert ein klar dokumentiertes Qualitäts-management-System (QMS; gibt es z.B. ein QM-Handbuch?					
2.37	Wenn ja, ist das QMS zertifiziert? Wenn ja, nach welchem Standard? (z.B. ISO 9000: 2000)					
2.38	Gibt es eine eigenständige und unabhängige Abteilung / Funktion „Qualitätssicherung"?					
2.39	Wenn ja, führt diese interne Audits / Selbst-inspektionen durch und gibt es darüber Berichte?					
2.40	Verfügt diese Einheit über ausreichendes Personal?					
2.41	Werden Mitarbeiterschulungen geplant, durchgeführt und dokumentiert?					
2.42	Existieren Stellenbeschreibungen oder gleichwertige Dokumente, die die Verantwortlichkeiten entscheidender Funktionsträger festlegen?					
2.43	Ist eine Person des Management benannt, die für die Implementierung und Aufrecht-erhaltung des QMS verantwortlich ist ?					
2.44	Unterliegt das QMS einem periodischen Review?					
2.45	Wird die QMS-Dokumentation regelmäßig gepflegt und aktualisiert?					
2.46	Werden Korrekturmaßnahmen innerhalb interner Audits definiert und die Umsetzung terminlich überwacht?					

2.6 Qualitätsmanagement / Dokumentation

2.47	Beinhaltet des QMS die Anforderung, dass projektbezogen ein Qualitätsplan erstellt wird, der die folgenden Punkte definiert: Rollen und Verantwortlichkeiten? • Lebenszyklus (SDLC)? • Dokumentationsstandards? • Qualitätssichernde Maßnahmen? Entwicklungs-Tools, -methoden und –standards?				
2.48	Sind beim FV folgende Punkte klar definiert: • Entwicklungsstandards • Programmierstandards • Teststandards				
2.49	Existieren schriftlich niedergelegte Standards bzw. Anweisungen (SOPs) für: • Software (S/W) Entwicklung? • Produktion und Wartung von Hardware (H/W) Komponenten? • Kontrollierten Änderungen (change control)? • Konfigurationsmanagement? • Dokumenten-Review und –genehmigung? • S/W Problem Unterstützung? • Vertrags-Review? • Überwachung von Projektplänen? • Aufbewahrung und Archivierung von qualitätsrelevanten Dokumenten? • Archivierung von S/W (Quellcode)? • Backup und Recovery-Pläne?				

2.6 Qualitätsmanagement / Dokumentation

	• Störfallmanagement? • Zugangsberechtigungen und physikalische/logische Sicherheit? • Behandlung von Beanstandungen? • Ablauf von Audits durch Kunden? Beurteilung von Lieferanten und Sub-Auftragnehmern?				
2.50	Existieren Standards für die Technische und Anwender-Dokumentation (User Manual)?				

2.7 Risikomanagement

Ein Risikomanagement sollte über den gesamten Lebenszyklus des computergestützten Systems unter Berücksichtigung von Patientensicherheit, Datenintegrität und Produktqualität betrieben werden. Als Teil eines Risikomanagementsystems sollten Entscheidungen über den Umfang der Validierung und die Sicherstellung der Datenintegrität auf einer begründeten und dokumentierten Risikobewertung des computergestützten Systems basieren.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Ein Risikomanagementsystem soll bezüglich CS etabliert und auch für diesen Bereich in das Qualitätsmanagementsystem des Unternehmens eingebunden sein, um GMP-Compliance zu gewährleisten. Beim Risikomanagement sind alle Aspekte des GMP-Umfeldes zu berücksichtigen wie Patientensicherheit, Datenintegrität, Datenqualität und Produktqualität. Risikomanagement soll über den gesamten Lebenszyklus des CS betrieben werden.					
	Die Ergebnisse der Risikobewertung dienen ihrerseits als Grundlage für die Entscheidungen über den Umfang der Validierung und die Sicherstellung der Datenintegrität/-qualität.					

	Insbesondere bei Änderungen von CS ist auch bereits in der Projektphase eine erneute Risikobewertung durchzuführen, jedoch sollte diese auch in regelmäßigen Abständen durchgeführt werden. Der Umfang einer erneuten Risikobewertung sollte von der Art der Änderung sowie von der Kritikalität des CS abhängen.					
2.51	Inwieweit berühren computergestützte Systeme oder Prozesse die Patientensicherheit, Produktsicherheit oder die Qualität und Integrität der elektronischen Daten?	Mit dieser Fragestellung können kritische Systeme identifiziert werden. Diese sollten bei einer Inspektion vorrangig berücksichtigt werden.				
2.52	Welche Maßnahmen zur Risikominimierung wurden im Rahmen des Risikomanagements festgelegt?	Bei bestehenden Systemen können in manchen Fällen nicht alle GMP-Anforderungen erfüllt werden, weil dies technisch nicht möglich ist. Im Rahmen der Risikosteuerung sind daher möglicherweise zusätzliche Maßnahmen festgelegt oder der Einsatzzweck des Systems ist eingeschränkt worden. Ein Ersatz dieser Systeme ist anzustreben. (siehe Abschnitt Validierung)				
2.53	Welche Aussagen machen übergeordnete QS-Dokumente zu Identifizierung und Bewertung von Risiken?	Der Umgang mit CS muss in die relevanten Qualitätssysteme eingebunden sein.				
2.54	Welche akuten und prospektiven Risikoabwehrmaßnahmen lassen sich daraus ableiten?	Der grundsätzliche Umgang zur Risikobeseitigung und -prävention sollte im QS-System beschrieben sein.				

2.55	Inwieweit wurden Art und Umfang der Validierungsaktivitäten GMP-relevanter Prozesse durch eine Risikobewertung ermittelt?	Bei der Risikobewertung sollten die direkten und indirekten Auswirkungen des CS auf GMP untersucht werden. Kritische Prozesse oder Funktionalitäten, welche im Rahmen der Risikobewertung identifiziert wurden, könnten Gegenstand von Teilinspektionen sein. (siehe Abschnitt Validierung)				
2.56	Wurde eine Risikobewertung im Rahmen einer retrospektiven Validierung durchgeführt?	Folgende Aktivitäten bezüglich der Risikobewertung werden im Rahmen einer retrospektiven Validierung mindestens erwartet: -Durchführung einer Risikoanalyse zur Ermittlung GMP-relevanter Systemteile und zur Festlegung der erforderlichen zusätzlichen Maßnahmen, -Auswertung und Bewertung historischer Daten, -Testen der als kritisch eingestuften GMP-relevanten Teile des CS. (siehe Abschnitt Validierung)				
2.57	Wie ist die Risikobewertung in das Änderungsmanagementsystem für CS eingebunden?	Änderungen sollten einer Bewertung hinsichtlich der Risiken unterzogen werden.				

2.58	In welchem Umfang wird Risikomanagement in den jeweiligen Phasen des Systemlebenszyklus betrieben?	Risikomanagement sollte während des gesamten Systemlebenszyklus durchgeführt werden. Bei der ersten Bewertung sollte die GMP-Kritikalität analysiert werden. Insbesondere sollte bewertet werden, ob das System einen Einfluss auf die Patientensicherheit, die Produktqualität, die Datenqualität oder die Datenintegrität besitzt. Die Anforderungsspezifikationen sollten unter Berücksichtigung potentieller Risiken entwickelt werden. Diese legen die Basis für eine erste formale Risikobewertung. Komplexe Systeme sollten einer detaillierteren Risikobewertung unterzogen werden, um kritische Funktionen zu bestimmen. Dies hilft, bei der Validierung alle kritischen Funktionen zu berücksichtigen. Risikomanagement beinhaltet die Implementierung von Kontrollen und deren Verifikation.				
2.59	Hat die Erkennbarkeit von Risiken Einfluss auf das Gesamtrisiko?	Nur Risiken die vor ihrem Eintreten erkennbar sind, können dazu führen, dass das Gesamtrisiko geringer eingestuft wird.				

3 PROJEKTPHASE

3.1 Validierung

Werden Dritte (z. B. Lieferanten, Dienstleister) herangezogen, um z. B. ein computergestütztes System bereitzustellen, zu installieren, zu konfigurieren, zu integrieren, zu validieren, zu warten (z. B. Fernwartung), zu modifizieren oder zu erhalten, Daten zu verarbeiten oder im Zusammenhang stehende Serviceleistungen zu erbringen, müssen formale Vereinbarungen abgeschlossen sein, in denen die Verantwortlichkeiten des Dritten eindeutig beschrieben sind. [2]IT-Abteilungen sollten analog zu Dritten behandelt werden.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	„Die Anwendung soll validiert, die IT Infrastruktur soll qualifiziert werden." (Anhang 11 - Grundsätze)					
	Die Qualifizierung von IT-Infrastruktur ist nun eine klar formulierte Anforderung des Anhangs 11. Mit der Wahrnehmung sind die Systemeigner (in der Regel IT-Abteilungen) befasst.					
3.1	Gibt es Vorgaben, die die Qualifizierungsanforderungen von IT-Infrastruktur beschreiben?	Z. B. Spezifikationen für Server, Scanner, Switche, Drucker, Verfahrensanweisungen und Protokolle über die Qualifizierung.				
	Die Validierungsdokumentation und -berichte sollten die maßgeblichen Phasen des Lebenszyklus abbilden. [2]Hersteller sollten in der Lage sein, ihre Standards, Pläne, Akzeptanzkriterien, Vorgehensweisen und Aufzeichnungen basierend auf ihrer Risikobewertung zu begründen.					
	Lebenszyklusphasen sind Planung, Realisierung, Validierung, Betrieb und Stilllegung des Systems. Es wird erwartet, dass die GMP-Kritikalität zunächst auf Systemebene anhand einer SOP oder Checkliste ermittelt wird. Es gibt unterschiedliche Methoden der Softwareentwicklung (z. B. V-Modell, "rapid prototyping") und davon abgeleitete Vorgehensweisen für die Validierung. Die angewendeten Methoden sind darzustellen und zu					

	begründen.					
3.2	Auf die Frage nach der Validierung der Applikation / Software verweist die Einrichtung auf den Erwerb und die Installation validierter Software. Was kann man entgegnen?	Software lässt sich nur in der spezifischen Anwendungsumgebung validieren. Grundfunktionalitäten kann der Hersteller testen und prüfen. In diesen Fällen sollte die entsprechende Dokumentation vorliegen und bewertet sein.				
3.3	Welche Methodik wurde der Validierung des Systems zu Grunde gelegt? Was waren die maßgeblichen Phasen der Validierung? Welche Dokumente wurden im Rahmen der Validierung erstellt?	Weit verbreitet ist ein Validierungsansatz nach dem V-Modell. Dabei werden folgende Dokumente erwartet: • Erstellung eines Validierungsplans, • Formulierung von Nutzeranforderungen / Lastenheft, • Auswahl eines Lieferanten auf Basis der Nutzeranforderungen, • Erstellung eines Pflichtenheftes / einer Funktionsspezifikation auf Basis der Nutzeranforderungen (dieses erfolgt i. d. R. durch den Lieferanten), • Risikoanalysen, • Installation, • Installationsqualifizierung (IQ), • operationelle Qualifizierung (OQ), • Testen des Systems und ggf. Bewertung von Testdokumentationen des Lieferanten, • Leistungsqualifizierung (Testen in der Be-				

		triebsumgebung unter Betriebsbedingungen), • Vorgabedokumente (Spezifikationen) und korrespondierende Berichte zu den maßgeblichen Phasen (s. o.). Bei der Verwendung alternativer Modelle sollte deren Eignung belegt sein.				
3.4	Wie wirkt sich das Ergebnis der Risikobewertung auf den Umfang der Validierung aus? Inwieweit wurde der Umfang der Validierung entsprechend dem Ergebnis der Risikobewertung angepasst?	Validierungsumfang bei einem kritischen und einem unkritischen Prozess / Funktionalität vergleichen.				
	Die Validierungsdokumentation sollte, sofern zutreffend, Aufzeichnungen im Rahmender Änderungskontrolle und Berichte über alle während der Validierung beobachteten Abweichungen beinhalten.					
3.5	Wie wurden die Änderungen, die im Rahmen der Entwicklung und Validierung durchgeführt wurden, nachvollziehbar dokumentiert?	An dieser Stelle wird ein weniger formales Änderungsmanagement als in der Betriebsphase erwartet. Wichtig ist, dass auch Änderungen vor der Inbetriebnahme nachvollziehbar sind. Das Genehmigungsprozedere kann gegenüber Änderungen nach der Inbetriebnahme deutlich reduziert sein.				
3.6	Wie werden Abweichungen, die im Rahmen der Validierung festgestellt wurden (z. B. nicht spezifikationskonforme Testergebnisse), dokumentiert?	Es wird erwartet, dass Abweichungen dokumentiert und durch die Verantwortlichen (Prozesseigner, Systemeigner) bewertet werden, GMP-kritische Abweichungen vor Inbetriebnahme des				

		Systems beseitigt werden. Werden Abweichungen nicht beseitigt, ist eine Bewertung vorzunehmen und der Grund dafür zu dokumentieren.				
	Eine aktuelle Liste aller maßgeblichen Systeme und ihrer GMP-Funktionen (Inventar) sollte zur Verfügung stehen. [2]Für kritische Systeme sollte eine aktuelle Systembeschreibung vorliegen, welche die technische und logische Anordnung, den Datenfluss sowie Schnittstellen zu anderen Systemen oder Prozessen, sämtliche Hard-und Softwarevoraussetzungen und die Sicherheitsmaßnahmen detailliert wiedergibt.					
3.7	Welche computergestützten Systeme werden betrieben? Welchen Zweck / welche Funktionalität haben diese Systeme? Welche Systeme haben Sie als GMP-kritisch eingestuft?	Erwartet wird eine aktuelle, ggfs. modulare Aufstellung, die ein gelenktes Dokument darstellt. Für GMP-kritische Systeme sollte eine Systembeschreibung vorliegen.				
3.8	Auf Grund welcher Kriterien stufen Sie ein System als GMP-kritisch ein?	Erwartet wird eine SOP oder Checkliste und eine schriftliche Bewertung auf Basis der SOP oder Checkliste für jedes System.				
	Die Benutzeranforderungen sollten die erforderlichen Funktionen des computergestützten Systems beschreiben und auf einer dokumentierten Risikobewertung sowie einer Betrachtung der möglichen Auswirkungen auf das GMP System basieren. [2]Die Benutzeranforderungen sollten über den Lebenszyklus des Systems verfolgbar sein.					
	Benutzeranforderungen sind die Basis für Validierungsaktivitäten. Sie sind auch im Rahmen einer retrospektiven Validierung zu erstellen. Die Validierung hat das Ziel nachzuweisen, ob das System geeignet ist, die Anforderungen zu erfüllen. Der Umfang der Benutzeranforderungen hängt von der Komplexität des Systems ab.					
3.9	Wer hat die Benutzeranforderungen erstellt?	Die Benutzeranforderungen sollten durch den Betreiber des Systems erstellt werden. Es ist auch				

		möglich, die funktionale Spezifikation des Lieferanten zu bewerten.				
3.10	Wie werden Benutzeranforderungen formuliert?	Benutzeranforderungen sollten so formuliert werden, dass sie nachprüfbar bzw. verifizierbar sind.				
3.11	Wie kann gezeigt werden, dass das System geeignet ist und im Besonderen kritische Benutzeranforderungen erfüllt werden?	Es wird erwartet, dass kritische Anforderungen identifiziert werden und über den Validierungsprozess nachverfolgbar und erfüllt sind. Hier sollte man im Rahmen der Inspektion beispielhaft an kritischen Anforderungen prüfen, ob diesen Anforderungen verschiedene Lebenszyklusdokumente zugeordnet werden können wie z. B. eine funktionale Spezifikation, eine Risikobewertung, Testberichte u. a.				
3.12	Wurde auf Basis der Benutzeranforderungen eine Risikobewertung durchgeführt? Welche Anforderungen wurden als kritisch bewertet und warum?					
	Der Nutzer im regulierten Umfeld sollte alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass das System in Übereinstimmung mit einem geeigneten Qualitätsmanagementsystem entwickelt wurde. [2]Der Lieferant sollte angemessen bewertet werden.					
3.13	Software wird in der Regel eingekauft und dann spezifisch auf die eigenen Anforderungen hin konfiguriert (Softwarekategorie 4; siehe Anlage). Da damit der Prozess der					

	Softwareentwicklung von einem Dritten durchgeführt wird und nicht im Detail kontrollierbar ist, kommt der Lieferantenbewertung und der Überprüfung, ob die Software qualitätsgesichert entwickelt wurde, eine besondere Bedeutung zu.					
3.14	Wurde der Software-Lieferant bewertet?	Für produktionsnahe kritische Systeme wird ein Vor-Ort-Audit erwartet. Lieferanten von weniger kritischen Systemen können durch ein postalisches Audit bewertet werden.				
3.15	Wurde für die Bewertung des Lieferanten auf eine Zertifizierung Bezug genommen ?	Wenn der Lieferant nach einem geeigneten Standard zertifiziert wurde und dies in der Lieferantenbewertung berücksichtigt wurde, sollte erfragt werden, ob das betreffende System durch Anwendung des (zertifizierten) QM-Systems entwickelt wurde.				
	Für die Validierung maßgeschneiderter Systeme oder für den Kunden spezifisch angepasster computergestützter Systeme sollte ein Verfahren vorliegen, das die formelle Bewertung und Berichterstellung zu Qualitäts-und Leistungsmerkmalen während aller Abschnitte des Lebenszyklus des Systems gewährleistet.					
	Tabellenkalkulationsprogramme werden in pharmazeutischen Unternehmen vielfach genutzt. Sofern sogenannte VBA-Makros oder SQL-Abfragen in die Tabellenblätter integriert sind, sollten diese als maßgeschneiderte Systeme angesehen werden.					
3.16	Welche Dokumente sind bei maßgeschneiderten Systemen zusätzlich erstellt worden im Vergleich	Maßgeschneiderte Systeme werden speziell für eine Anwendung und einen Kunden entwickelt. Auf Anforderung müssten Aktivitäten zum Code				

	zu konfigurierbaren Standard-Software Paketen?	Review, Unit-Test, Integrationstest nachgewiesen werden. Die entsprechenden Berichte sollten mindestens beim Lieferanten vorliegen und dort im QM-System eingebunden sein. Diese Vorgehensweise sollte im Rahmen eines Lieferantenaudits überprüft worden sein. Bei Datenbanken handelt es sich vielfach um maßgeschneiderte oder individuell konfigurierte Systeme.				
3.17	Wie und wo werden die Konfigurationseinstellungen eines Systems dokumentiert? Lassen sich Änderungen der Konfiguration nachvollziehen? Lässt sich die jeweilige Konfiguration einem spezifischen Softwarestand/Release zuordnen? -	Spezifisch angepasste Systeme werden auf die Anforderungen des Betreibers hin konfiguriert. Die Konfiguration und die sich daraus ergebende Funktionalität sind zu dokumentieren und sollten durch Tests überprüft werden. Änderungen der Konfiguration sollen über das Änderungsmanagement erfolgen.				
	Die Eignung von Testmethoden und Testszenarien sollte nachgewiesen werden. [2]Insbesondere Grenzwerte für System-/ Prozessparameter, Datengrenzen und die Fehlerbehandlung sollten betrachtet werden. [3]Für automatisierte Testwerkzeuge und Testumgebungen sollte eine dokumentierte Bewertung ihrer Eignung vorliegen.					
3.18	Wie wurde die Eignung der Testfälle nachgewiesen?	Aus der Testbeschreibung kann man das erwartete Testergebnis und die Testdurchführung entnehmen.				
3.19	Wie werden kritische Datenfelder überprüft?	Insbesondere wenn kritische Daten Folgeaktionen auslösen, sollten Grenzwerte und andere Werte (z. B. Buchstaben statt Zahlen) für Testzwecke verwendet werden.				

3.20	Werden automatisierte Testwerkzeuge verwendet? Wie wurden diese hinsichtlich Ihrer Eignung überprüft?	Kritische Funktionalitäten der Testtools sollten geprüft werden. Die Eignung der Testdaten sollte belegt sein.				
	Werden Daten in ein anderes Datenformat oder System überführt, sollte im Rahmen der Validierung geprüft werden, dass der Wert und die Bedeutung der Daten im Rahmen dieses Migrationsprozesses nicht verändert werden.					
	Aufgrund von Software-Upgrades, eines Systemwechsels oder auch einer Stilllegung von Systemen kann es erforderlich sein, die bestehenden Daten aus den Altsystemen in andere Systeme oder Speichermedien zu migrieren bzw. zu überführen. Dieses ist ein kritischer Prozess, der Planung und Testen erfordert. Insbesondere unterschiedliche Datenformate können Einfluss auf die Datenintegrität haben. Die Archivierung von Daten ist eine Form der Migration.					
3.21	Wie wird die Größe der Stichprobe bestimmt, die im Rahmen eines Migrationsprozesses überprüft wird?	Das hängt ab von der Kritikalität der Daten (z. B. Blutbanksoftware, infektionsserologische Daten). In jedem Fall sollten alle unterschiedlichen Formate überprüft werden. Statistisch repräsentative Stichprobengrößen kann man z. B. der DIN ISO 2859 Teil1 entnehmen.				
3.22	Welche Strategie wird bei der Datenmigration verfolgt? Welche Vorgehensweise ist im Migrationsplan beschrieben?	Es sollte ein Datenmigrationsplan bestehen. Tests zur Datenmigration sollten in einer Testumgebung erfolgen. Es ist wichtig, dass die zu migrierenden Daten vorher auf die im Migrationsplan genannten Kriterien überprüft werden. Es sollte berücksichtigt werden, dass Daten über unterschiedliche Schnittstellen und mit verschiedenen Ausgangsformaten migriert werden können.				

3.23	Wie ist sichergestellt, dass die Bedeutung und Einheiten korrekt übertragen werden?	Bei der Migration dürfen Größeneinheiten (z. B. g, kg) und Bedeutung der Werte (z. B. Infektionsserologie) nicht verändert werden oder müssen im Falle einer Änderung korrekt transformiert werden.				
	Datenarchivierung kann auch Migration auf ein anderes Speichermedium sein. Will man kein Museum von Altgeräten vorhalten, ist es oftmals erforderlich, Daten und Metadaten (das sind die Informationen, die zur Interpretation der Daten erforderlich sind, z.B. Integrationsparameter) zu migrieren.					

3.2 Testpläne und -Standards

Nr.	Fragen und Bezug / Kommentierung	Ja	Nein	NZ	Antwort
3.24	Existieren Standards für die Testplanung, -durchführung und Testberichte?				
3.25	Werden für jedes Projekt Testpläne erstellt?				
3.26	Sind die Tests in unterschiedliche Phasen strukturiert, d.h. können sie hinreichend differenziert und zugeordnet werden (z.B. White-box testing, black-box testing/User Acceptance Tests)?				
3.27	Umfaßt ein Testplan folgende Punkte: • Systembezeichnung, inkl. Entwicklungsstand? • Testziele/Bezug zur Risikoanalyse? • Testfälle? • Testdaten, inkl. Akzeptanzkriterien? • Durchführung/Testumfang? • Ergebnisse der Tests, inkl. Beschreibung der Abweichungen? Bewertung der Ergebnisse, ggf. Änderungen in Abhängigkeit von der Entwicklungsstufe (SDLC) und erneutes Testen?				
3.28	Gibt es einen systematischen Ansatz zur Bestimmung des Testumfangs?				
3.29	Sind die Prüfer/Reviewer andere Personen als die Entwickler?				
3.30	Werden Test-Tools eingesetzt?				
3.31	Werden diese auf Validierung durch den Hersteller geprüft oder retro-validiert?				

3.32	Sind die Testberichte Bestandteil der Validierungsdokumentation?				
3.33	Werden Test-Audits, einschl. Dokumenten-Reviews in den verschiedenen Entwicklungsphasen (IQ, OQ, PQ) durchgeführt?				
3.34	Wird in solchen Audits auch nachgewiesen, dass die Teststandards eingehalten werden?				

4 BETRIEBSPHASE

4.1 Daten

Um Risiken zu minimieren sollten computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, geeignete Kontrollmechanismen für die korrekte und sichere Eingabe und Verarbeitung der Daten enthalten

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Während früher überwiegend einzelne Systeme vorzufinden waren, sind die verschiedenen Systeme inzwischen immer stärker vernetzt. Durch Übertragung von Daten von einem System zu einem anderen entfallen manuelle Eingaben als mögliche Fehlerquelle, aber diese so genannten Schnittstellen sollten bei der Validierung näher betrachtet werden. Da die Schnittstellen gewissermaßen zu beiden Systemen gehören, ist darauf zu achten, dass bei Änderungen in einem System mögliche Einflüsse auf die Schnittstelle und sich dadurch ergebende Folgeänderungen in dem über diese Schnittstelle angebundenen System betrachtet werden.					
	Man unterscheidet zwischen unidirektionalen und bidirektionalen Schnittstellen. Bei der ersten werden Daten immer in einer Richtung übertragen, während bidirektionale Daten in beide Richtungen transferieren.					
4.1	Zwischen welchen Systemen werden Daten übertragen? Welche Systeme tauschen Daten untereinander aus? Welche Protokolle werden verwendet?	Anhand der Kritikalität der Systeme kann bei der Inspektion entschieden werden, ob eine nähere Prüfung erfolgen soll.				

4.2	Welche technischen Protokolle für die Datenübertragung werden verwendet?	Sofern lediglich ein „Transport“ von Daten über eine Leitung erfolgt und Standardprotokolle für die Datenübertragung (z. B. TCP/IP) zum Einsatz kommen, ist dies in der Regel unkritisch. Wenn allerdings die Daten in den einzelnen Systemen in unterschiedlichen Formaten vorliegen, wird eine Veränderung der Daten an der Schnittstelle erfolgen. Beispiel für unterschiedliche Formate: Datumsangaben TTMMJJJJ -MMTTJJ.				
4.3	An welchen Schnittstellen erfolgt eine Umwandlung von Daten?	Neben Veränderungen der Einheiten (z. B. g stattzuvor kg) sind auch Änderungen im Datenformat (z. B. Komma oder Punkt als Dezimaltrenner) denkbar. Dies sollte spezifiziert und getestet sein.				

4.2 Prüfung auf Richtigkeit

Werden kritische Daten manuell eingegeben, sollte die Richtigkeit dieser Dateneingabe durch eine zusätzliche Prüfung abgesichert werden. Diese zusätzliche Prüfung kann durch einen zweiten Anwender oder mit Hilfe einer validierten elektronischen Methode erfolgen. Die Kritikalität und möglichen Folgen fehlerhafter oder inkorrekt eingegebener Daten für das System sollten im Risikomanagement berücksichtigt sein.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
4.4	Welche Daten wurden im Rahmen der Risikoanalyse als kritisch definiert?	Welche Daten als kritisch anzusehen sind, soll im Voraus festgelegt sein. Prinzipiell steht es dem Unternehmen frei, welche Daten als kritisch definiert werden. Werte (Daten), die jedoch für die Entscheidung über Freigabe oder Zurückweisung der Charge, eines Aus-				

		gangsstoffes, eines Zwischenproduktes oder eines Fertigarzneimittels herangezogen werden, sollten bei Inspektionen als kritische Daten angesehen werden. Welche Daten als kritisch anzusehen sind, soll im Voraus festgelegt sein.				
4.5	Wo werden Daten manuell eingegeben?	Die manuelle Eingabe von Daten ist fehleranfällig. Im Rahmen von Inspektionen sollte darauf geachtet werden, wo Daten von Hand eingegeben werden. Als Beispiel seien die Eingabe der Chargennummer oder des Verfalldatums bei der Verpackung oder auch die Eingabe der Grenzwerte für eine Bandwaage genannt.				
4.6	Wie und durch wen erfolgt eine zusätzliche Prüfung?	Die Prüfung kann nach Anhang 11 durch einen zweiten Bediener – das sollte dann zeitnah erfolgen – oder durch eine validierte elektronische Methode erfolgen. Denkbar für elektronische Methoden sind z. B. Prüfziffern bei nummerischen Werten (gibt es u. a. bei der Pharmazentralnummer und bei vielen Barcodes), die Ausgabe von Warnmeldungen, wenn Grenzwerte überschritten sind, oder auch Plausibilitätsprüfungen, bei denen der Bediener mehrere Werte (z. B. Artikelnummer, Charge, Menge) eingeben muss und das System deren „Zusammengehörigkeit“ mit Werten in der Datenbank vergleichen kann.				

4.7	Welche Folgen/ Konsequenzen hat eine fehlerhafte Dateneingabe?	Die Auswirkung einer fehlerhaften manuellen Dateneingabe sollte bewertet sein. Je nach Auswirkung sollten geeignete Kontrollmaßnahmen vorhanden sein.				
4.8	Welche zusätzlichen Tests, mit denen Fehleingaben erkannt werden können, sind vorhanden?	Am Beispiel einer Bandwaage in der Verpackung kann man verdeutlichen, dass falsch eingegebene Grenzen möglicherweise dazu führen, dass fehlende Blister nicht mehr erkannt werden. Wenn vor Produktionsbeginn eine Prüfung mit Musterpackungen erfolgt, wird die Fehleingabe quasi sofort erkannt und als Konsequenz ergibt sich eine Korrektur der fehlerhaft eingegebenen Daten. Es ist jedoch auch denkbar, dass eine fehlerhafte Dateneingabe (z. B. Korrekturfaktor) zu einer Abweichung im Gehalt oder der Stabilität führen. Bei kritischen Daten ist in jedem Fall eine zusätzliche Prüfung erforderlich.				
4.9	Welche Kontrollen zur Prüfung auf Richtigkeit werden bei „Excel“-Tabellen verwendet?	Wenn Tabellenkalkulationen zur Berechnung oder Auswertung verwendet werden, ist zunächst darauf zu achten, dass so genannte Vorlagen verwendet werden. Diese sind an der Dateiendung „.xlt“ bzw. „.xltx“ zu erkennen. Die „Wiederverwendung“ von Tabellenblättern, die zuvor schon für Berechnungen verwendet wurden und noch Werte enthalten, sollte bei Inspektionen beanstandet werden, da hier die Gefahr besteht, Werte der vorhergehenden Analyse zu				

		berücksichtigen. Solche Vorlagen sollten ähnlich wie eine Herstellungsanweisung als kontrolliertes Dokument behandelt werden, also einer Versionierung und dem Änderungsmanagement unterliegen.				

4.3 Datenspeicherung

Es sollten regelmäßige Sicherungskopien aller maßgeblichen Daten erstellt werden. Die Integrität und Richtigkeit der gesicherten Daten sowie die Möglichkeit der Datenwiederherstellung sollten während der Validierung geprüft und regelmäßig überwacht werden

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Wichtig ist zwischen Datensicherung und Archivierung zu unterscheiden. Bei Datensicherungen unterscheidet man inkrementelle und vollständige Sicherungen. Bei einer vollständigen Sicherung wird eine Kopie des gesamten der Datensicherung unterliegenden Datenbestandes erstellt. Bei einer inkrementellen Sicherung werden nach einer initialen vollständigen Sicherung in der Folge nur noch Daten kopiert, die seit der letzten Sicherung verändert wurden. Der Vorteil besteht darin, dass weniger Speicherplatz benötigt wird und das Backup schneller abläuft; als Nachteil ergibt sich dann allerdings, dass bei einer Wiederherstellung der Daten zunächst die letzte vollständige Sicherung und dann nacheinander alle inkrementellen Sicherungen zurückgespielt werden müssen.					
	Als Generationen bezeichnet man die Anzahl der aufbewahrten Datensicherungen bis man beginnt, die Datenträger zu überschreiben. Oft findet man auch mehrere überlappende Generationen. So wird z. B. von den Datensicherungen von Montag bis Donnerstag als tägliche Sicherung immer nur ein Datenträger aufbewahrt. Von der Datensicherung von Freitag werden hingegen als Wochensicherung z. B. vier Wochen aufbewahrt und von					

	denjenigen am Monatsanfang als Monatssicherung die letzten sechs.					
	RAID ist ein Akronym für engl. „Redundant Array of Independent Disks“, also „redundante Anordnung unabhängiger Festplatten“. Gängig im Pharma-Umfeld sind RAID 1 und RAID 5: RAID 1 (Mirroring) – Daten werden parallel auf zwei unabhängige Datenträger geschrieben (gespiegelt) – ist als Ersatz für eine Datensicherung nicht geeignet, da Fehler wie z. B. Löschungen mit gespiegelt werden. RAID 5 (Block-Level Striping mit verteilter Paritätsinformation) -Daten werden auf mindestens 3 Festplatten verteilt geschrieben. Durch Paritätsinformationen, die auf einer anderen Platte als die Daten abgelegt werden, können bei Ausfall einer Festplatte die Daten aus den auf den anderen Platten vorhandenen Informationen wiederhergestellt werden. RAID-Systeme sind ein Beitrag zur Verfügbarkeit von Daten, also zum Schutz vor Datenverlust durch Festplattendefekte. RAIDs sind jedoch nicht zur Datensicherung geeignet, da Löschungen oder unbeabsichtigte Veränderungen sich stets auch auf die redundant gespeicherten Daten auswirken.					
4.10	Welches Verfahren wird zur Datensicherung eingesetzt? Wie oft erfolgt eine Sicherung der Daten?	Datensicherungen sind in jedem Fall erforderlich. Die Frequenz der Datensicherung kann sehr unterschiedlich sein. Als Anhaltspunkt für die Notwendigkeit eines Backups kann man die Häufigkeit, mit der Daten ergänzt oder verändert werden, nehmen. Z. B. ein System zur Aufzeichnung kritischer Umgebungsbedingungen wird möglicherweise stündlich gesichert, während das Verzeichnis der SOPs nur wöchentlich gesichert wird.				
4.11	Wie viele Generationen von Datensicherungen werden aufbewahrt?	Üblicherweise bewahrt man mehr als eine Datensicherung auf. Gängig ist es z. B. für jeden Wochentag ein getrenntes Medium zu verwenden				

		die nach einer Woche überschrieben werden. Oft werden zusätzlich auch wöchentliche und/ oder monatliche Sicherungen erstellt. Es gibt aber auch Systeme die eine Historie über längere Zeiträume ermöglichen (z.B. stündlich für die letzten 24 h, täglich für den letzten Monat und wöchentliche Backups für die vorherigen Monate).				
4.12	Ist die Datenwiederherstellung validiert?	Das Zurückspielen einer Datensicherung sollte in jedem Fall getestet sein. Bei komplexen Systemen wird man die Wiederherstellung nicht in das so genannte Produktivsystem durchführen. Bei diesen komplexen Systemen findet man oft eine so genannte 3-System-Landschaft aus Entwicklungssystem, Testsystem und Produktivsystem. Hier kann es akzeptiert werden, wenn das zurückspielen einer Datensicherung im Testsystem überprüft wurde.				
4.13	Wo erfolgt die Aufbewahrung der Sicherungsmedien?	Sicherungsmedien sollten zumindest in einem getrennten Brandabschnitt aufbewahrt werden.				

4.4 Ausdrucke

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Nach Kapitel 4 sollen Nutzer im regulierten Umfeld für elektronische Dokumente festlegen, welche Daten als Rohdaten genutzt werden sollen. Dabei sind mindestens alle Daten, auf					

	denen Qualitätsentscheidungen basieren, als Rohdaten zu definieren.					
4.14	Welche Daten sind druckbar?	Alle als Rohdaten definierten Daten und alle zur Interpretation der Daten notwendigen Informationen sollten ausgedruckt werden können.				
4.15	Sind nachträgliche Änderungen erkennbar a) am Bildschirm? b) in Ausdrucken?	Grundlage dieser Forderung sind § 10 Absatz 1 AMWHV und Anhang 11 Nr. 8.2. Änderungen kritischer Daten sind im Audit Trail zu protokollieren. Vor Freigabe einer Charge ist zu überprüfen, ob bei Qualitätsdaten nachträgliche Änderungen erfolgten. Gerade bei elektronischer Dokumentation sind Veränderungen nicht automatisch auch nachträglich erkennbar. Es ist als ausreichend anzusehen, wenn z. B. durch eine Unterstreichung o. ä. erkennbar ist, dass es sich um einen geänderten Wert handelt und man zur Feststellung des ursprünglichen Wertes in die Protokolldatei Einsicht nehmen muss. Sofern Änderungen am Bildschirm erkennbar sind, kann man bei der Inspektion nach einem Ausdruck fragen und prüfen, ob die Änderungen auch erkennbar sind.				
4.16	Welche Verfahren sind für die Systeme etabliert, bei denen eine solche Funktionalität noch nicht vorhanden ist?	Sofern das System vor Inkrafttreten des Anhangs 11 im Juli 2011 installiert wurde und keine Funktionalität bietet, bei der nachträgliche Änderungen am Bildschirm und in Ausdrucken erkennbar sind,				

		kann es ausnahmsweise akzeptiert werden, wenn in einer entsprechenden SOP geregelt ist, dass vor Freigabe einer Charge eine Auswertung des Audit Trails erfolgt und das Ergebnis dieser Auswertung zusätzlich dokumentiert wird.				

4.5 Audit Trails

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Basierend auf einer Risikobewertung sollte erwogen werden, die Aufzeichnung aller GMP-relevanten Änderungen und Löschungen in das System zu integrieren (ein systemgenerierter „Audit Trail").					
4.17	Welche Prozesse sind GMP-relevant?	Die GMP-relevanten Prozesse werden i. d. R. bereits an anderer Stelle beschrieben, nämlich im Lastenheft. Die Risikobewertung zur Abgrenzung GMP-relevanter und nicht GMP-relevanter Prozesse sollte methodisch geeignet sein.				
4.18	Welche Eingabefelder enthalten kritische Daten?	Es besteht nicht die Notwendigkeit, in einem GMP-relevanten Prozess alle Datenfelder einem Audit Trail zu unterwerfen. Auch hier sollte im Detail eine Risikobewertung zur Festlegung der tatsächlich kritischen und prozessrelevanten Daten erfolgen. Kritische Variablen/ Werte müssen durch das Audit Trail erfasst werden.				
4.19	Wann werden Audit Trails gelöscht?	Audit Trails dürfen nicht verändert und prinzipiell nicht gelöscht werden. Sofern Firmen Daten, deren Aufbewahrungsfrist abgelaufen ist, lö-				

		schen, wäre die Löschung der zugehörigen Daten im Audit Trail zulässig. Hier ist zu hinterfragen, wie sichergestellt wird, dass nur die zugehörigen Einträge im Audit Trail gelöscht werden.				
	Bei der Änderung oder Löschung GMP-relevanter Daten sollte der Grund dokumentiert werden.					
	Diese Anforderung ist neu und soll sicherstellen, dass das Ändern und/ oder Löschen von Daten nachvollziehbar wird.					
4.20	Wer darf Daten ändern oder löschen?	Die Berechtigung zur Änderung/Löschung von Daten sollte im Benutzer- bzw. Rollenkonzept hinterlegt sein. Eindeutige Identifizierung des Nutzers, ein Datum und ein Zeitstempel sind erforderlich.				
4.21	Wie wird bei einer Änderung bzw. Löschung die Begründung dokumentiert?	Die Begründung kann in Form eines Freitextes erfolgen. Drop-/Pull-down-Menüs sind auch akzeptabel. In jedem Fall muss die Begründung inhaltlich nachvollziehbar sein. Die Eingabe einer Begründung sollte vom System erzwungen werden.				
	Audit Trails müssen verfügbar sein, in eine allgemein lesbare Form überführt werden können und regelmäßig überprüft werden					
4.22	Welche Informationen werden bei Änderungen oder Löschungen aufgezeichnet?	Es sollten mindestens folgende Informationen vorliegen: -„wer“, „was“, „wann“ und „wie“ geändert hat, -Anzeige des ursprünglichen und des geänderten Wertes, -Grund der Änderung/ Löschung				

4.23	Wie oft erfolgt die regelmäßige Überprüfung des Audit Trails?	Dabei sind zum einen die Funktionalität und zum anderen die Daten des Audit Trails zu prüfen. Das Intervall sollte nachvollziehbar unter Berücksichtigung des Prozessrisikos festgelegt werden.				

4.6 Änderungs-und Konfigurationsmanagement

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Jede Änderung an einem computergestützten System einschließlich der Systemkonfigurationen sollte kontrolliert und nach einem festgelegten Verfahren erfolgen.					
4.24	Ab wann werden Änderungen kontrolliert erfasst und umgesetzt?	Bereits im Rahmen der Entwicklung sollten Änderungen erfasst und bewertet werden, was i. d. R. zu einer Änderung der Benutzeranforderung („user requirement specification“) und/oder der Funktionsspezifikation führt. Der Übergang von der Entwicklungsphase in den laufenden Betrieb sollte klar abgegrenzt sein. Es bietet sich ggf. an, zwei verschiedene Verfahrensweisen zu etablieren.				
4.25	Welche Elemente weist das Änderungsmanagement auf?	Üblich sind: -Festlegung der Rollen (z. B. Antrag, Bewertung, Maßnahmen, Durchführung, Abschluss), -Art und Weise der Dokumentation, -Antrag inkl. Begründung, -Bewertung der GMP-Relevanz und des Prozessrisikos, -Festlegung der Maßnahmen und Tests, -Genehmigung, -Durchführung, -Abschluss und Rückmeldung an				

		Antragsteller. Art und Kritikalität der Änderung kann Einfluss auf die notwendigen Schritte (Ablauf, Dokumentation) haben. Reparaturen durch Austausch gleichartiger Komponenten können als vorab generell genehmigte Änderungen beschrieben sein.				
4.26	Welche Elemente weist das Konfigurationsmanagement auf?	Üblich sind: -Art und Weise der Dokumentation, -Kodierung/ Parametrierung.				
4.27	Wie werden Änderungen klassifiziert?	Eine Klassifizierung ist mindestens in die zwei Kategorien „GMP-relevant“ und „nicht GMP-relevant“ vorzunehmen. Darüber hinaus wird empfohlen, eine Einstufung „kritisch“ und „unkritisch“ vorzunehmen. Nur auf dieser Basis ist eine Reduzierung von Maßnahmen (Validierung ja/nein und Umfang der Validierung) zur Umsetzung einer Änderung möglich.				
4.28	Welche Kontrollen erfolgen bei Änderungen der Konfiguration?	Die Kontrollen sind systemspezifisch zu definieren, die Maßnahmen basierend auf einer Risikobewertung festzulegen.				
4.29	Existiert ein dokumentiertes Verfahren für kontrollierte Änderungen (change control procedure) bei • dem SDLC? • dem Quellcode? • der H/W Spezifikation und OQ? • den Konfigurationsdaten?					
4.30	Existiert eine eindeutige Definition, ab welcher Änderung eine Re-Validierung, ganz oder					

	teilweise, notwendig ist (Risikomanagement)?				
4.31	Sind die Verantwortlichkeiten beim Änderungsmanagement geregelt (release of change, implementor, reviewer etc.)?				
4.32	Sind Verfahren vorhanden, die es verhindern, dass ein Update oder eine Änderung eines S/W-Moduls oder eines wichtigen Dokuments unbemerkt oder von mehreren Personen gleichzeitig erfolgen kann?				
4.33	Ist sichergestellt, dass nach Änderung am System erneut Tests, möglichst die gleichen (Regression-Tests) durchgeführt werden müssen?				
4.34	Ist es möglich, Änderungen vom Antrag bis zur Implementierung zurückzuverfolgen?				
4.35	Kann jede Version eines jeden Konfigurationselementes eindeutig und einheitlich identifiziert werden?				
4.36	Werden ausgelieferte Versionen von H/W und S/W Systemen sowie die dazugehörigen Dokumentationen archiviert?				

4.7 Periodische Evaluierung

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Computergestützte Systeme sollten periodisch evaluiert werden, um zu bestätigen, dass sie sich noch im validen Zustand befinden und die GMP-Anforderungen erfüllen.					
4.37	Wie häufig erfolgen die periodischen Überprüfungen?	Anhang 11 gibt kein Intervall vor. Die Häufigkeit ist vom Unternehmen festzulegen. Für unterschiedliche Systeme können verschiedene Intervalle festgelegt sein. Die Überprüfungen sollten mindestens jährlich erfolgen. Andere Intervalle sollten nachvollziehbar begründet wer-				

		den. Umfang sowie Art und Weise der periodischen Prüfung sollten schriftlich festgelegt werden. Auch hier kann in Abhängigkeit von GMP-Relevanz und Kritikalität eine entsprechende Abstufung vorgenommen werden.				
	Solche Evaluierungen sollten, sofern sachgerecht, den derzeitigen Funktionsumfang, Abweichungsaufzeichnungen, Vorfälle, Probleme, Aktualisierungen, Leistung, Zuverlässigkeit, Sicherheit und Berichte zum Validierungsstatus umfassen.					
4.38	In wessen Verantwortung liegt die Durchführung der periodischen Evaluierung?	Hierzu gibt es keine Vorgaben. Es sollte klar geregelt sein, wer die Verantwortung trägt und an wen die Durchführung ggf. delegiert wird. Die Evaluierung sollte unter Mitwirkung der beteiligten Abteilungen/ Bereiche erfolgen (QA, IT, Fachabteilung usw.).				
4.39	Ist die Evaluierung an einen Dienstleister delegiert?	Die Aufgabe/ Arbeit selbst kann delegiert werden, die Verantwortung dafür aber nicht. Mögliche Verantwortlichkeiten: QA oder der Systemeigner Produktion/ Qualitätskontrolle oder eine Validierungseinheit -verantwortlich ist letztendlich das pharmazeutische Unternehmen bzw. dessen Sachkundige Person.				

4.8 Dokumenten-Review und -Genehmigung

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort

4.40	Existiert eine eindeutige Definition, welche Dokumente einem Review unterliegen?				
4.41	Ist die Organisation des Review-Prozesses festgelegt und beschrieben?				
4.42	Gibt es Review-Checklisten?				
4.43	Sind Verfahren bei Abweichungen festgelegt und beschrieben?				
4.44	Sind Verantwortlichkeiten definiert für: • Review-Verfahren? • Genehmigungsverfahren? • Verfahren bei Abweichungen?				

4.9 Sicherheit

Es sollten physikalische und/ oder logische Maßnahmen implementiert sein, um den Zugang zu computergestützten Systemen auf autorisierte Personen zu beschränken. Geeignete Maßnahmen zur Vermeidung unerlaubten Systemzugangs können die Verwendung von Schlüsseln, Kennkarten, persönlichen Codes mit Kennworten, biometrische Verfahren sowie den eingeschränkten Zugang zu Computern mit zugehöriger Ausrüstung und Datenspeicherungsbereichen einschließen.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Zur Erhöhung der Sicherheit von CS kommen verschiedene Maßnahmen in Betracht, z. B. Datenspeicherung, geregelter Datenzugriff, Datenverschlüsselung, Virenschutz, Verwendung von Firewalls. Die Auswahl der Maßnahmen richtet sich nach der Kritikalität des Systems und der Daten.					
	Die Vergabe von Zugangsberechtigungen soll gewährleisten, dass das im Betrieb beschäftigte Personal Zugriff auf die Daten und Programme erhält, die zur Erfüllung der übertragenen Aufgaben erforderlich sind.					
	Je nach Betriebssystem bestehen unterschiedliche Möglichkeiten. Sofern mehrere Personen Zugriff zum System haben, dürfen Zugriffe auf Dateien und Programme nur mit					

	entsprechender Autorisierung möglich sein. Dabei ist zu beachten, dass zur Vergabe solcher Rechte vielfach mehrere Ebenen bestehen. So ist es möglich, eine Datei oder ein Programm nur für einen einzigen Benutzer zugänglich zu machen. Es ist jedoch ebenso möglich, diese Rechte für eine bestimmte Gruppe (z. B. alle Meister) oder eben für alle Nutzer mit Zugangsberechtigung zum System zu vergeben.				
	Sofern Zugriffsrechte für Gruppen vergeben wurden, kann im Rahmen einer Inspektion z. B. geprüft werden, welche Gruppen bestehen und welche Personen welchen Gruppen zugeordnet sind. Die Vergabe von Zugriffsrechten für Gruppen ist nur in Ausnahmefällen zulässig, z. B. bei Leserechten.				
	Wenn man sich dann noch erläutern lässt, welche Rechte die einzelnen Gruppen haben, kann überprüft werden, ob die einzelnen Personen nur die zur Erfüllung ihrer Aufgabe notwendigen Rechte haben.				
	In der Berechtigungsverwaltung stellen Benutzerrollen (kurz: Rollen) eine konzeptionelle Weiterentwicklung von Benutzergruppen dar. Eine Rolle definiert Aufgaben, Eigenschaften und vor allem Rechte eines Benutzers (oder Administrators) in einer Software bzw. in einem Betriebssystem. Statt Benutzern oder Gruppen Rechte direkt zuzuweisen, wird eine Rolle definiert, die dann vielen Benutzern zugeordnet werden kann. Einem Benutzer können eine oder auch mehrere Rollen zugewiesen werden. Dies führt zu einer Vereinfachung der Berechtigungsverwaltung.				
4.10 Infrastruktursicherheit					
4.45	Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?				
4.46	Der Zutritt zu wichtigen IT-Systemen und Raumen ist geregelt. Besucher, Handwerker, Servicekräfte etc. werden begleitet und beaufsichtigt.				

4.47	Der Zugang zu den Serverräumen wird protokolliert.				
4.48	Es besteht ein ausreichender Schutz vor Einbrechern				
4.49	Es gibt es einen Netzplan. Der Netzplan wird regelmäßig aktualisiert.				
4.50	Der Bestand an Hard- und Software ist in Inventarlisten erfasst.				
4.11 Informationssicherheitsmanagement					
4.51	Die Unternehmens- bzw. Behördenleitung hat die Informationssicherheitsziele festgelegt und bekennt sich zu ihrer Verantwortung für die Informationssicherheit. Alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte sind berücksichtigt worden.				
4.52	Es gibt einen IT-Sicherheitsbeauftragten und ein Organigramm der Verantwortlichkeiten.				
4.53	Die bestehenden Richtlinien und Zuständigkeiten sind allen Zielpersonen bekannt.				
4.54	Es gibt Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.).				
4.55	Die Wirksamkeit von Sicherheitsmaßnahmen wird regelmäßig überprüft.				
4.56	Es gibt es ein dokumentiertes Sicherheitskonzept.				
4.12 Infrastruktursicherheit					
4.57	Vorhandene Schutzmechanismen in Anwendungen und Programmen werden genutzt.				
4.58	Es werden flächendeckend Viren-Schutzprogramme eingesetzt.				

4.59	Allen Systembenutzern sind Rollen und Profile zugeordnet.				
4.60	Es Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf. Sinnvolle Beschränkungen sind definiert.				
4.61	Es gibt verschiedene Rollen und Profile für die Administratoren.				
4.62	Es ist bekannt und geregelt, welche Privilegien und Rechte Programme haben.				
4.63	Sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen werden geeignet angepasst. Der Auslieferungszustand wird prinzipiell nicht beibehalten.				
4.64	Handbücher und Produktdokumentationen werden vor Einsatz gelesen.				
4.65	Nicht benötigte sicherheitsrelevante Programme und Funktionen werden konsequent deinstalliert bzw. deaktiviert.				
4.66	Es werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert.				
4.13 Vernetzung und Internetanbindung					
4.67	Es gibt ein geeignetes Firewall-Konzept mit zwei hintereinander geschalteten Firewalls.				
4.68	Konfiguration und Funktionsfähigkeit der Firewall-Systeme werden regelmäßig überprüft und kontrolliert.				
4.69	Es gibt ein Intrusion-Detection Konzept mit täglichen Intervallen. Internet-Verbindungen werden kontinuierlich überprüft. Die Überprüfung wird protokolliert.				
4.70	Gefährliche Zusatzprogramme (Plug-Ins) und aktive Inhalte sind prinzipiell nicht zugelassen.				
4.71	Alle unnötigen Dienste und Programmfunktionen werden konsequent deaktiviert.				

4.72	Alle verwendeten Web-Browser sind sicher konfiguriert.				
4.73	Alle Mitarbeiter sind ausführlich geschult.				
4.14 Beachtung von Sicherheitserfordernissen					
4.74	Vertrauliche Informationen und Datenträger werden sorgfältig aufbewahrt.				
4.75	Vertrauliche Informationen werden vor Wartungs-/Reparaturarbeiten von Datenträgern/IT-Systemen gelöscht.				
4.76	Die Mitarbeiter werden regelmäßig in sicherheitsrelevanten Themen geschult.				
4.77	Es gibt Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter.				
4.78	Bestehende Sicherheitsvorgaben werden kontrolliert.				
4.15 Wartung von IT-Systemen – Umgang mit Updates					
4.79	Sicherheits-Updates werden regelmäßig eingespielt.				
4.80	Es gibt Verantwortliche, die sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informieren und ihre Kollegen schulen.				
4.81	Es gibt ein Testkonzept für Softwareänderungen mit der Möglichkeit zum Fallback.				
4.16 Passwörter und Verschlüsselung					
4.82	Alle Programme und Anwendungen bieten Sicherheitsmechanismen wie Verschlüsselung oder Passwortschutz. Die Sicherheitsmechanismen sind aktiviert.				

4.83	Voreingestellte oder leere Passwörter werden prinzipiell geändert.				
4.84	Alle Mitarbeiter sind in der Wahl sicherer Passwörter geschult.				
4.85	Alle Administratorkonsolen sind durch Passworte geschützt.				
4.86	Alle Arbeitsplatzrechner mit Zugang zu sicherheitsrelevanten Informationen werden beim Verlassen des Arbeitsplatzes gesperrt. Die Sperren sind mit Kennwort gesichert.				
4.87	Besonders gefährdete Systeme wie Notebooks und Remote-Systeme sind ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt.				
4.17 Notfallvorsorge					
4.88	Es gibt einen Notfallplan mit Anweisungen und Kontaktadressen.				
4.89	Der Notfallplan behandelt alle systemkritischen Notfallsituationen.				
4.90	Der Notfallplan ist gut zugänglich und allen Mitarbeitern der Systemadministration bekannt.				
4.91	Für Notfälle sind die wichtigsten Passwörter sicher hinterlegt.				
4.18 Datensicherung					
4.92	Es gibt es eine klar definierte Backupstrategie.				
4.93	Die vorgesehene Backupstrategie wird strikt eingehalten.				
4.94	Es ist festgelegt, welche Daten wie lange gesichert werden.				

4.95	Die Sicherung bezieht auch tragbare Computer mit ein.					
4.96	Die Sicherungsbänder werden regelmäßig kontrolliert.					
4.97	Sicherungs- und Rücksicherungsverfahren sind dokumentiert.					
4.98	Zugang zu dem Stahlschrank, in dem die Bandsicherungen aufbewahrt werden, haben nur wenige, klar definierte Personen.					
4.19 Datenschutz						
4.99	Alle Mitarbeiter sind zur Einhaltung des Datenschutzes (bei der Verarbeitung personenbezogener Daten) unterrichtet und schriftlich verpflichtet.					
4.100	Es gibt es datenschutzkonforme Richtlinien für die Einhaltung des Datenschutzes für FTP-Zugänge und den Remote-Betrieb.					
4.101	Die datenschutzgerechte Löschung/Vernichtung von Sicherungsbändern und Datenträgern wird durch geeignete Maßnahmen garantiert.					
4.20 Zugriffsschutz						
4.102	Wie werden erfolglose Zugriffsversuche dokumentiert?	Diese Dokumentation kann im Rahmen der Inspektion eingesehen werden. In der Dokumentation sollte festgehalten sein, mit welcher Benutzerkennung wann und von wo der Zugriffsversuch erfolgte. Hier kann man dann z. B. bei einer Häufung nach den ergriffenen Maßnahmen fragen. Nach mehreren erfolglosen Versuchen, Zugriff auf das Computersystem zu erlangen (z. B.					

		falsches Passwort), sollte der betreffende Zugang gesperrt sein. Das Verfahren zur Entsperrung sollte festgelegt sein.				
4.103	Welche Maßnahmen sind zum Schutz vor äußeren Einflüssen, z. B. Viren, vorhanden?	Werden externe Daten aus dem Netz oder von Datenträgern heruntergeladen und geöffnet, ist der Einsatz von Antiviren-Software zwingend. Systeme, die mit dem Internet verbunden sind, sollten durch eine geeignete Firewall geschützt werden. Darüber hinaus kann auch bei mehreren internen Netzen der Einsatz von Firewalls zum Schutz vor benachbarten Netzen erforderlich sein. Die Antiviren-bzw. Firewall-Software sollte regelmäßig aktualisiert werden.				
4.104	Wer vergibt den jeweiligen Status der Zugriffsrechte und wie ist das Prozedere?	Die Rollen und Befugnisse von Administratoren sollten klar definiert sein. Die Administratoren sollten zur Wahrnehmung ihrer Aufgaben entsprechend geschult sein.				
4.105	Welche Festlegungen wurden getroffen, um den Einsatz sicherer Passwörter zu gewährleisten?	Es sollten Vorgaben für Passwörter festgelegt sein, z. B. für Länge, zu verwendende Zeichen, Häufigkeit der Änderungen, erneute Verwendung. Ein gängiger Standard findet sich im BSI IT-Grundschutz, demnach sollten Passwörter länger als sieben Zeichen sein, nicht in Wörterbüchern vorkommen, nicht aus Namen bestehen und auch Sonderzeichen oder Ziffern enthalten.				

4.106	Wie werden erfolglose Zugriffsversuche dokumentiert?	Diese Dokumentation kann im Rahmen der Inspektion eingesehen werden. In der Dokumentation sollte festgehalten sein, mit welcher Benutzerkennung wann und von wo der Zugriffsversuch erfolgte. Hier kann man dann z. B. bei einer Häufung nach den ergriffenen Maßnahmen fragen. Nach mehreren erfolglosen Versuchen, Zugriff auf das Computersystem zu erlangen (z. B. falsches Passwort), sollte der betreffende Zugang gesperrt sein. Das Verfahren zur Entsperrung sollte festgelegt sein.				
4.107	Wer darf (wann) welche Daten ändern?	Die Erlaubnis sollte auf namentlich festgelegte Personen beschränkt sein. Dies sollte jedoch nur für "bestätigte Daten" gelten. Wenn sich jemand bei der Eingabe von Daten vertippt und dies sogleich korrigiert, ist dies nicht als Änderung im Sinne des Anhangs 11 anzusehen. Erst nach der Bestätigung (vielfach mit der Enter-/Return-Taste) und Speicherung der Daten kann man von Änderungen im Sinne des Anhangs 11 ausgehen.				
4.108	Wie ist diese Ermächtigung, Eingaben und Änderungen vornehmen zu dürfen, dokumentiert?	Die Berechtigungen sind so zu dokumentieren, dass nachvollziehbar ist, welcher Benutzer wann welche Berechtigung erhalten bzw. verloren hat (üblich in Datenbank oder Tabellenform). Wichtig ist zu überprüfen, wer Änderungen vornehmen darf und ob dabei die Voraussetzungen der AMWHV (nachträgliche Erkennbarkeit) einge-				

		halten werden.				
4.109	Welche Methoden werden eingesetzt, um den Zugang zum System durch Nichtberechtigte zu verhindern?	Grundsätzlich muss unterschieden werden zwischen -physischer Zutrittskontrolle (Räumlichkeiten) und -logischer Zugriffskontrolle (Software). Beides sollte bei der Inspektion berücksichtigt werden. Das System sollte in der Lage sein, die für den jeweiligen Anwender freigegebenen Aufgaben zu identifizieren (z. B. durch Verknüpfung von User-ID und Passwort zu einer eindeutigen Kombination, mit der die Autorisierung des Anwenders für eine spezielle Anwendung einhergeht).				
4.110	Welche Personen sind zur Eingabe oder Änderung von Daten ermächtigt?	Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die dazu ermächtigt und geschult sind: -Eingabe: nur durch Personen, die laut Arbeitsplatzbeschreibung am jeweiligen System arbeiten. -Änderung: durch den jeweiligen Funktionsträger im Sinne AMG/AMWHV oder von ihm autorisierte Personen.				
4.111	Welche Regelungen gibt es zur Festlegung der Zugriffsrechte?	Die Vergabe von Zugriffsrechten sollte in einer SOP geregelt sein. Bei der Verteilung der Rechte in einem Netzwerk bzw. bei Unterschriften sind in der Regel verschiedene Rollen zu unterscheiden.				

4.112	Wie prüft das System die Identität des Benutzers, der kritische Daten eingibt, ändert oder bestätigt?	Die Identifizierung eines Benutzers kann erfolgen über a) Wissen, z. B. Benutzerkennung und Passwort, b) Besitz, z. B. Chipkarte, Schlüssel, c) ein biometrisches Merkmal, z. B. Fingerabdruck, Stimme, Form des Gesichtes. Gängig ist Variante a). Für sicherheitsrelevante Bereiche ist auch b) im Einsatz. Biometrische Systeme sind derzeit noch unüblich. Die Validierung dieser Systeme sollte kritisch hinterfragt werden.				
	Erteilung, Änderung und Entzug von Zugriffsberechtigungen sollten aufgezeichnet werden.					
4.113	Welches Verfahren besteht für die Ausgabe, Annullierung und Veränderung der Ermächtigung zur Eingabe und Änderung von Daten?	Die Vergabe der entsprechenden Zugriffsberechtigungen sollte so erfolgen, dass die betreffenden Personen nur die Berechtigung für die von ihnen durchgeführten Arbeiten erhalten. Beim Ausscheiden oder Wechsel eines Mitarbeiters sollte die (alte) Zugriffsberechtigung deaktiviert werden. Es sollte geprüft werden, ob die Berechtigungen im System mit den Aufgaben der Mitarbeiter/innen übereinstimmen. Es sollte ein Register über autorisierte Personen gepflegt werden.				
4.114	Wie ist das Verfahren zur Eingabe und Änderung von Daten beschrieben?	Hier kann durch das Inspektionsteam u. a. überprüft werden, ob tatsächlich nur befugte Personen Eingaben und Änderungen vornehmen können.				

4.21 Vorfallmanagement

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
	Alle Vorfälle, nicht nur Systemausfälle und Datenfehler, sollten berichtet und bewertet werden.					
4.115	Wie sind Vorfälle definiert?	Ein Unternehmen kann definieren, was ein Vorfall und was bestimmungsgemäßer Gebrauch ist. Z. B. kann das Zurücksetzen eines Passwortes regelmäßige Aufgabe der Administration und daher kein Vorfall sein, da auch das System dies über Logfiles dokumentiert.				
	Die Ursache eines kritischen Vorfalls sollte ermittelt werden und die Basis für Korrektur-und Vorbeugemaßnahmen sein.					
4.116	Wie werden Vorfälle klassifiziert?	Es sollte zumindest eine Definition von kritischen und nicht kritischen Vorfällen vorliegen. Die Ursache sollte dokumentiert, Korrektur-und Vorbeugemaßnahme sollten festgelegt sein. In Abhängigkeit der Einstufung können unterschiedlich detaillierte Abläufe zur Bearbeitung von Vorfällen vorliegen.				
4.117	Wer ist bei dem Vorfallmanagement beteiligt?	In einer Verfahrensanweisung sollte festgelegt werden, wer wie Vorfälle erfasst und bearbeitet. Die Erfassung, die Bewertung, das Festlegen von Maßnahmen, der Abschluss und das Follow-up sollten Rollen und Funktionalitäten zugeordnet sein. In Abhängigkeit der Kritikalität müssen der				

		Prozesseigner und ggf. SP/ QA eingebunden werden.				

4.22 Elektronische Unterschrift

Elektronische Aufzeichnungen können elektronisch signiert werden. Von elektronischen Unterschriften wird erwartet, dass sie a) im Innenverhältnis eines Unternehmens die gleiche Bedeutung haben wie handschriftliche Signaturen, b) dauerhaft mit dem zugehörigen Dokument verbunden sind, c) die Angabe des Datums und der Uhrzeit der Signatur beinhalten.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
4.118	Die Nutzung elektronischer anstelle handschriftlicher Unterschriften sowie die Art der elektronischen Unterschrift liegen grundsätzlich im Verantwortungsbereich des regulierten Unternehmens. GMP-Vorgaben zur Art bzw. Qualität der elektronischen Unterschrift gibt es nicht. Das Signaturgesetz ist nicht anwendbar. Im Rahmen der Inspektion elektronischer Unterschriften ist es daher zunächst wichtig, die firmeninternen Festlegungen zur Genehmigung von Dokumenten im Allgemeinen, insbesondere im Hinblick auf die Berechtigungen und Zugriffskonzepte zu kennen.					
4.119	Die Bedeutung elektronischer Unterschriften ist wie bei handschriftlichen Unterschriften gemäß allgemeiner GMP-Vorgaben in der jeweiligen Firma festzulegen, ohne dass dies im Anhang 11 gesonderter Erwähnung bedarf.					
4.120	Welche Dokumente werden elektronisch unterschrieben?	Hier kann ein Überblick gewonnen werden, auch im Hinblick auf die Kritikalität der elektronischen Unterschriften.				
4.121	Welche Arten von elektronischen Unterschriften finden Verwendung?	Die Art der elektronischen Unterschrift ist (s. o.) nicht vorgegeben. Im Falle der elektronischen Unterschrift unter Herstellungsprotokoll, Prüfprotokoll oder zur Dokumentation der Freigabeentscheidung wird die Verwendung einer				

		fortgeschrittenen elektronischen Signatur empfohlen. Sofern einfache elektronische Unterschriften verwendet werden, gewinnt der Nachweis der Unabstreitbarkeit der Unterschrift besondere Bedeutung. Die Minimalanforderung an die Ausführung einer elektronischen Unterschrift ist mindestens die erneute Eingabe eines Passwortes. Durch einfache Funktionstasten oder Befehle generierte Namenswiedergaben stellen keine elektronische Signatur dar.				
4.122	Existieren auch Genehmigungen in elektronischen Dokumenten, die nicht mit einer elektronischen Unterschrift erfolgen?	Möglicherweise gibt es auch Dokumente, die durch einfache Funktionstasten oder Befehle (z. B. in einem elektronischen Workflow) genehmigt oder geprüft werden. In diesem Fall handelt es sich nicht um Unterschriften und es ist zu prüfen, ob in der Papierwelt ein Visum ausreichend wäre. In jedem Falle sollte das System die Identität des Nutzers, der die Dokumente geprüft, bearbeitet, genehmigt oder freigegeben hat, aufzeichnen.				
4.123	Liegt eine schriftliche Einverständniserklärung der elektronische Unterschriften nutzenden Personen vor, die elektronischen Unterschriften als im Innenverhältnis rechtsverbindliches Äquivalent zu einer handgeschriebenen Unterschrift anzuerkennen?	Da Anhang 11 nur auf das Innenverhältnis abzielt, sollte -sofern nicht ausschließlich qualifizierte elektronische Unterschriften im Sinne des Signaturgesetzes Verwendung finden -eine derartige Erklärung vorliegen, um die Authentizität der Unterschrift unabstreitbar zu machen.				

4.124	Ist eine nachträgliche Änderung eines unterschriebenen Dokumentes möglich? Falls ja, ist die Änderung erkennbar? Bleibt die Unterschrift gültig?	Es muss sichergestellt sein, dass nachträgliche Änderungen von bereits unterzeichneten Dokumenten erkennbar sind und bei einer Änderung die Unterschrift ungültig wird.				
4.125	Wie wird die Identität des Bedieners überprüft?	In der Regel wird die Identität durch Benutzerkennung und Passwort sichergestellt. Dies erfordert entsprechende Zugriffskonzepte (vgl. Ziffer 12 Anhang 11). Alternativen wie Chipkarten oder Schlüssel sind ebenfalls akzeptabel. Im Falle der Verwendung von Systemen zur Erkennung biometrischer Merkmale sollte die Validierung des Systems kritisch hinterfragt werden.				
4.126	Wie wurde das Verfahren der elektronischen Unterschrift inkl. der unlöschbaren Verknüpfung mit dem unterschriebenen Dokument validiert?	Hier gelten die gleichen Bedingungen wie bei der Validierung anderer Systeme.				
4.127	Werden elektronisch unterschriebene Dokumente über Schnittstellen in andere Systeme übertragen oder werden durch elektronische Unterschriften weitere Workflows angestoßen?	Die Schnittstellen zu anderen Systemen und weitere Abläufe sollten zumindest erfragt werden, um entscheiden zu können, ob eine Weiterverfolgung anderer Systeme im Rahmen der Inspektion erforderlich ist.				
4.128	Wie lange werden elektronisch unterschriebene Dokumente aufbewahrt? Werden elektronisch unterschriebene Dokumente in andere Systeme, ggf. auch in Archivsysteme, migriert?	Die Aufbewahrungsfristen elektronisch unterschriebener Dokumente unterscheiden sich nicht von handschriftlich unterschriebenen Dokumenten. Sofern elektronisch unterschriebene Dokumente archiviert oder migriert werden siehe Angaben unter Ziffer 4.8 Anhang 11 sowie unter				

		Ziffer 17 Anhang 11.				

4.23 Kontinuität des Geschäftsbetriebs

Wenn computergestützte Systeme kritische Prozesse unterstützen, sollten Vorkehrungen getroffen sein, um die fortlaufende Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. durch ein manuelles oder ein alternatives System). Der erforderliche Zeitaufwand zur Inbetriebnahme dieser alternativen Verfahren sollte jeweils für ein bestimmtes System und die unterstützten Prozesse risikoabhängig festgelegt werden. Diese Verfahren sollten angemessen dokumentiert und getestet werden.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
4.129	Kritische Prozesse sind zu identifizieren und aufzulisten.					
4.130	Beispiele für mögliche Ausfallszenarien (Abhilfemöglichkeiten in Klammern angegeben) sind -Ausfall von Komponenten, z. B. Drucker oder Waage (Bereithalten von Ersatzgeräten), -Schwankungen in der Stromspannung bzw. Stromausfall (Ausgleichssysteme bzw. Notstrom), -Schäden an der Hardware durch äußere Einflüsse (Vorhalten von Ersatzsystemen), -Systemabsturz (lokale Datenpuffer), -Eindringen von Viren u. a. (laufende Aktualisierung der Antivirensoftware).					
4.131	Punkt 16 des Anhangs 11 betrifft nicht nur sich in der Produktion befindliche Arzneimittelchargen, sondern auch Chargen, die bereits im Verkehr sind (z. B. bei Rückrufen). Daher ist bei Prozessen, in denen der Zeitfaktor kritisch ist, festzulegen, innerhalb welcher Frist alternative Maßnahmen greifen müssen.					
4.132	Gibt es einen Maßnahmenplan und wie ist er aufgebaut?	Der Maßnahmenplan sollte Folgendes enthalten: -eine Beschreibung möglicher Fehler und Ausfallsituationen mit Angabe der Häufigkeit bzw. der Wahrscheinlichkeit des Auftretens, -Erläuterung evtl. mitlaufender Alternativsysteme, -Beschreibung der Vorgehensweise bei Fehlern				

		und Ausfallsituationen, -Erfordernis der Dokumentation und ggf. das Nachpflegen alternativ aufgezeichneter Daten in das CS sollten festgelegt werden, -Beschreibung des Wiederhochfahrens des CS nach Fehlerbeseitigung, -Auflistung der zur Wiederinbetriebnahme autorisierten Personen. Der Maßnahmenplan sollte regelmäßig überprüft werden; die hierfür verantwortlichen Personen sind festzulegen.				
4.133	Gibt es ein Meldeverfahren und was beinhaltet es?	Das Meldeverfahren sollte beinhalten: -die Klassifizierung des Fehlers oder der Ausfallsituation mit der Auswirkung auf den betroffenen Prozess, -die Festlegung von Verantwortlichkeiten für die zu treffenden Maßnahmen, -die Fehlersuche, -Präventionsmaßnahmen.				
4.134	Wie sind die alternativen Verfahren beschaffen?	Die Geschwindigkeit, mit der die alternativen Verfahren die ausgefallenen Verfahren ersetzen, muss der Dringlichkeit der Maßnahmen angemessen sein. Die alternativen Verfahren müssen schriftlich festgelegt und validiert sein sowie regelmäßigen Tests bezüglich ihres Funktionierens und der zeitnahen Implementierung unterzogen werden. Werden Daten des alternativen Verfahrens wieder ins System eingegeben, sollten diese verifiziert				

		werden.				
4.135	Wie erfolgt der Umgang mit Daten, die nach Systemausfall oder anderen Fehlern wiedergewonnen werden konnten?	Die Daten sollten auf mögliche Fehler und Integrität überprüft werden.				

4.24 Archivierung

Daten können archiviert werden. Diese Daten sollten auf Verfügbarkeit, Lesbarkeit und Integrität geprüft werden. Sind maßgebliche Änderungen am System erforderlich (z. B. Computer und zugehörige Ausrüstung oder Programme), sollte sichergestellt und getestet werden, ob die Daten weiterhin abrufbar sind.

Nr.	Fragen und Bezug	Kommentierung	Ja	Nein	NZ	Antwort
4.136	Wichtig ist der Unterschied zwischen Datensicherung und Archivierung**.**					
4.137	Welche Tests werden durchgeführt, um die Verfügbarkeit der Daten sicherzustellen?	Datenträger sind nur begrenzt haltbar. Leider gibt es keine verbindlichen Daten über die Haltbarkeit elektronische Datenträger. Das Unternehmen sollte allerdings intern eine Festlegung getroffen haben, nach welcher Zeit die Lesbarkeit archivierter Daten geprüft werden soll. Insbesondere bei Aufbewahrungszeiträumen von mehr als sechs Jahren ist damit zu rechnen, dass die Daten umkopiert werden müssen. Auch ist bei längeren Zeiträumen davon auszugehen, dass Hardware, Betriebssysteme und Programme zur Archivierung sich ändern. In solchen Fällen ist vor Abschaltung des bisherigen Systems zu testen, ob die Daten unverändert im neuen System lesbar				

		gemacht werden können und unverändert bleiben.				
4.138	Werden die Datenträger an geeigneter Stelle aufbewahrt?	Die Haltbarkeit der Datenträger hängt auch von Umweltbedingungen ab. Im Rahmen der Inspektion kann z. B. geprüft werden, ob die vom Hersteller des Datenträgers gegebenen Empfehlungen zur Lagerung eingehalten werden und ob die Einhaltung der Parameter (z. B. Temperatur) auch überwacht wird.				
4.139	Welche Tests werden durchgeführt, wenn Datenträger umkopiert werden?	Als Mindestanforderung ist ein so genanntes „verify“ durchzuführen, bei dem durch die jeweilige Applikation die beiden Datenträger verglichen werden. Sofern nicht auf ein identisches Medium umkopiert wird, ist zu hinterfragen, ob die Daten auf das neue Medium tatsächlich nur 1:1 kopiert werden oder ob eine Veränderung der Daten und ihrer Bezüge erfolgt.				

5 ZUSÄTZLICHE FRAGEN

Nr	Frage/Bemerkungen	Antwort/Kommentar

6 UNTERSCHRIFT

_____	_____	_____
Datum	Name des Auditors	Unterschrift

7 DEFINITIONEN UND ABKÜRZUNGEN

Die unterstrichenen Begriffe sind dem Glossar von Anhang 11 entnommen.

Akzeptanzkriterien
Die Kriterien, die ein System/ eine Komponente erfüllen müssen, um von einem Anwender, Kunden oder einer anderen autorisierten Stelle akzeptiert zu werden.

Akzeptanztest
Tests, die durchgeführt werden, um festzustellen, ob ein System die Akzeptanzkriterien erfüllt oder nicht und um den Kunden in die Lage zu versetzen das System zu akzeptieren oder abzulehnen. Siehe auch Fabrik-Akzeptanztest (FAT) und Standort-Akzeptanztest (SAT).

Anforderung
Eine Anforderung ist eine Aussage über die Beschaffenheit oder Fähigkeit, die generell zu gewährleisten oder obligatorisch ist.

Anwendung
Software, die auf einer definierten Plattform/ Hardware installiert ist und spezifische Funktionen bietet.

Archivierung
Erstellen von Kopien von Daten, um diese langfristig verfügbar zu halten, in der Regel mit dem zusätzlichen Ziel, Speicherplatz frei zu machen.

Audit Trail
Systemseitiger Kontrollmechanismus, der es ermöglicht, Veränderungen und Löschungen zu dokumentieren.

Backup
Siehe Datensicherung.

Code Review
Mit dem Review werden Arbeitsergebnisse der Softwareentwicklung manuell geprüft. Das Review ist ein mehr oder weniger formal geplanter und strukturierter Analyse-und Bewertungsprozess der Software. Beim Code Review wird ein Programmabschnitt nach oder während der Entwicklung von einem/ mehreren Gutachter/n Korrektur gelesen, um mögliche Fehler, Vereinfachungen oder Testfälle zu finden.

CS
Computergestütztes System.

Datensicherung/ Backup
Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

Dritter
Nicht direkt vom Inhaber der Herstellungs-oder Einfuhrerlaubnis geführte Einrichtung.

Fabrik-Akzeptanztest (FAT)
Ein Akzeptanztest im Werk des Lieferanten, üblicherweise unter Einbeziehung des Kunden. Siehe auch Akzeptanztest, Gegensatz zu Standort-Akzeptanztest. (Factory Acceptance Test)

Firewall

Eine Firewall ist ein Hard-oder Softwaresystem, das die Verbindung zwischen Netzen kontrolliert und insbesondere Angriffe aus dem Internet auf das eigene Netz abwehrt.

GAMP

Good Automated Manufacturing Practice, Leitfaden zur Validierung automatisierter Systeme in der pharmazeutischen Herstellung.

Integrität

Schutz vor unbefugter Änderung von Information.

ITIL

Abkürzung für IT Infrastructure Library. Eine Sammlung von Gute-Praxis-Leitfäden zum IT Service Management. Diese umfassen Dienstleistungen/ Services rund um IT. Der Service Lebenszyklus beinhaltet Strategie, Design, Übergang und Durchführung der Services sowie deren kontinuierliche Verbesserung.

IT-Infrastruktur

Hardware und Software wie Netzwerksoftware und Betriebssysteme, die für die Funktionsfähigkeit der Anwendung erforderlich sind.

Kommerziell erhältliche Standardsoftware

Software, die auf Grund eines Marktbedarfs entwickelt wurde, kommerziell verfügbar ist, und deren Einsatzfähigkeit durch ein breites Spektrum kommerzieller Kunden nachgewiesen wurde. Wird im Englischen auch mit COTS (Commercial-Off-the-Shelf Software) abgekürzt.

Konfiguration

Mit einer Konfiguration wird eine bestimmte Anpassung/ Einstellung von Programmen oder Hardwarebestandteilen eines Computers an Benutzeranforderungen bezeichnet. Neben der Installation (Ersteinstellung) umfasst der Begriff auch die wählbaren Voreinstellungen (auch Optionen) der Betriebsparameter.

Kundenspezifische (bespoke)/ für den Kunden spezifisch angepasste (customized) computergestützte Systeme

Ein computergestütztes System angepasst an einen spezifischen Geschäftsprozess.

LAN

Local Area Network, lokales, räumlich begrenztes Netzwerk.

Lebenszyklus

Alle Phasen der Systemlebensdauer von den initialen Anforderungen bis zur Stilllegung einschließlich Design, Spezifikation, Programmierung, Testung, Installation, Betrieb und Wartung.

Lebenszyklusmodell

Vorgehensweise, um während des Entwurfs, der Entwicklung der Erstellung und dem Betrieb von computergestützten Systemen eine durchgängige Qualitätssicherung über alle Ebenen zu erreichen.

MES

Manufacturing Execution System (Fertigungsmanagementsystem).

Migration

Vollständige Übertragung von Daten in ein anderes Computersystem mit dem Ziel, die Daten zukünftig im neuen System zu nutzen.

PPS

Production Planning System – Fertigungsplanungssystem.

Prozesseigner

Die für den Geschäftsprozess verantwortliche Person.

Rapid Prototyping

Methode der Softwareentwicklung, bei der schnell ein einsatzbereites System vorliegt, dass dann in einer Reihe von Iterationen verbessert und erweitert wird, bis die Anforderungen erfüllt sind. Die Spezifikation entsteht dabei parallel zur Entwicklung der Software.

Quellcode

(1) Computerinstruktionen und Datendefinitionen, die in einer für den Assembler, Compiler oder für andere Programmcode-Übersetzer geeigneten Form dargestellt sind.
(2) Die menschenlesbare Version einer Instruktionsliste eines Programms, das einen Computer veranlasst, eine Aufgabe auszuführen.

Review

Vollständige Überprüfung einer Systemkomponente oder eines Dokumentes hinsichtlich Form und Inhalt durch eine weitere Person mit entsprechender Sachkenntnis.

Schnittstelle

Eine Schnittstelle ist ein definierter Übergang zwischen Datenübertragungseinrichtungen, Hardwarekomponenten oder logischen Softwareeinheiten.

Sicherheit

Unter Sicherheit des Systems und der Daten werden alle technischen und organisatorischen Maßnahmen zum Schutz vor Verlust, Beschädigung und unzulässiger Änderung verstanden und damit die Vertraulichkeit, die Integrität und die Verfügbarkeit sicherstellen.

SOP

Standard Operating Procedure, Standardarbeitsanweisung.

Spezifikation (IT)

Ein Dokument, das die Anforderungen, den Entwurf, das Verhalten oder andere Charakteristika eines Systems oder einer Komponente -und öfters -die Vorgehensweisen zur Feststellung, ob diese Vorschriften eingehalten wurden, vollständig, exakt und nachprüfbar beschreibt.

Standort-Akzeptanztest (SAT)

Ein Akzeptanztest am Kunden-Standort, üblicherweise unter Einbeziehung des Lieferanten. (Site Acceptance Test) Siehe auch Akzeptanztest, Gegensatz zu Fabrik-Akzeptanztest.

Systemeigner

Die für die Verfügbarkeit und Wartung eines computergestützten Systems und die Sicherheit der auf dem System gespeicherten Daten verantwortliche Person.

TCP/ IP

Transmission Control Protocol/ Internet Protocol. Standardprotokolle für die Übertragung von Daten zwischen Rechnern. Beinhaltet eine Verifizierung einer korrekten Übertragung.

Test, funktionell

(1) Tests, die die internen Mechanismen oder Strukturen eines Systems oder einer Komponente ignorieren und ausschließlich auf die Resultate (Ausgaben) als Antwort auf selektierte Vorgaben (Eingaben) und Ausführungsbedingungen fokussiert.
(2) Test, durchgeführt zur Beurteilung der Konformität eines System oder einer Komponente mit spezifischen funktionalen Anforderungen und korrespondierenden vorhergesagten Ergebnissen. Synonym: Black-Box-Test, eingangs-/ ausgangsbezogener Test. Im Gegensatz dazu: struktureller Test.

Test, strukturell

(1) Test, der alle internen Mechanismen (Strukturen) eines Systems oder einer Komponente mit einbezieht. Typen können sein: Zweigtest, Pfadtest, Statement-Test.
(2) Test, der sicherstellt, dass jedes Programm-Statement zur Ausführung gebracht wird und dass jedes Programm-Statement die vorgesehene Funktion ausführt. Synonym: White-Box-Test, Glass-Box-Test, logisch-getriebener Test, Unit Test.

Testfall
Ein Satz von Test-Eingaben, Betriebsbedingungen und erwarteten Ergebnissen, entwickelt für ein bestimmtes Ziel wie die beispielhafte Ausführung eines bestimmten Programmzweigs oder die Verifikation der Einhaltung einer spezifischen Anforderung.

Testplan
Ein Dokument, das den Umfang, den Ansatz, die Ressourcen und den Zeitplan der beabsichtigten Testaktivitäten beschreibt. Es legt die Testgegenstände, die zu testenden Funktionen und die Testaufgaben fest sowie wer diese Tests im Einzelnen ausführen wird und alle Risiken, die eine Planung für unvorhergesehene Ereignisse erfordern.

Verifizierung
Bestätigung durch Bereitstellen eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind. Wird teilweise an Stelle von IQ, OQ, PQ verwendet.

WAN
Ein Wide Area Network (WAN, dt., Weitverkehrsnetz) ist ein Rechnernetz, das sich im Unterschied zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt.
Die Anzahl der angeschlossenen Rechner ist unbegrenzt. WANs erstrecken sich über Länder oder sogar Kontinente. WANs werden benutzt, um verschiedene LANs, aber auch einzelne Rechner miteinander zu vernetzen. WANs können bestimmten Organisationen gehören und ausschließlich von diesen genutzt werden oder sie werden z. B. durch Internetdienstanbieter errichtet oder erweitert, um einen Zugang zum Internet anbieten zu können.

8 QUELLEN

- AiM 07121202 Überwachung computergestützter Systeme, https://www.zlg.de/index.php?eID=tx_nawsecuredl&u=0&file=fileadmin/downloads/AM/QS/07121202.pdf&hash=e48d9bf7fa19237b8c3b035ae8126005401f6cc4
- EU-GMP Leitfaden, https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Statistiken/GKV/Bekanntmachungen/GMP-Leitfaden/GMP-Leitfaden-1.pdf , 2011
- Anhang 11 des EU GMP-Leitfadens, http://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Statistiken/GKV/Bekanntmachungen/GMP-Leitfaden/Anlage_2_zur_Bekanntmachung_-_Annex_11.pdf, 2011
- IT Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- GAMP5, http://www.ispe.org/gamp-5

9 ANLAGEN UND FORMULARE

- Anlage 1 – Softwarekategorien nach GAMP5
- Anlage 2 – Anhang 11 „Computergestützte Systeme“ zum EU-Leitfaden der Guten Herstellungspraxis in der Fassung der vom Bundesministerium für Gesundheit bekanntgemachten Übersetzung ergänzt um Satznummern.

9.1 Anlage 1 -Softwarekategorien nach GAMP5®

Kategorie 1 – Infrastruktur-Software

Infrastrukturelemente sind untereinander verbunden, um eine integrierte Umgebung für den Betrieb und die Unterstützung von Applikationen und Dienstleistungen zu bilden.

In dieser Kategorie werden zwei Softwaretypen unterschieden: Bewährte oder kommerziell-verfügbare unterlagerte Software: Applikationen werden zur Ausführung auf dieser Softwareplattform entwickelt. Zur Plattform gehören Betriebssysteme, Datenbankmanager, Programmiersprachen, Systemdienste, Steuerungssprachen-Interpreter (IEC 61131), statistische Programmierwerkzeuge und Tabellenkalkulationspakete (aber nicht die Applikationen für diese Pakete, siehe Anhang S3).

Infrastruktur-Software-Werkzeuge: Dieses umfasst Hilfsprogramme wie Netzüberwachungssoftware, Stapelverarbeitungswerkzeuge, Sicherheitssoftware, Antivirensoftware und Konfigurations-Management-Werkzeuge. Eine Risikobewertung sollte für Werkzeuge mit potentiell hoher Auswirkung durchgeführt werden, z. B. für die Kennwortverwaltung oder das Sicherheitsmanagement, um zu ermitteln, ob zusätzliche Kontrollen angemessen sind.

Kategorie 2 – Diese Kategorie wird in GAMP5® nicht weiter verwendet.

Kategorie 3 – Nicht-konfigurierte Produkte

Diese Kategorie umfasst Serienprodukte für Geschäftszwecke. Sie umfasst sowohl Systeme, die nicht für die Geschäftsprozesse konfiguriert werden können, als auch Systeme, die zwar konfigurierbar sind, aber bei denen die Standardkonfiguration verwendet wird. In beiden Fällen ist eine Konfiguration zur Anpassung an die Betriebsumgebung möglich und wahrscheinlich (z.

B. Druckerkonfiguration). Eine Einschätzung basierend auf dem Risiko und der Komplexität sollte ergeben, ob die nur mit der Standardkonfiguration verwendeten Systeme als Kategorie 3 oder als Kategorie 4 zu behandeln sind.

Kategorie 4 – Konfigurierte Produkte

Konfigurierbare Software-Produkte liefern Standard-Schnittstellen und Funktionen, die die Konfigurierung von anwenderspezifischen Geschäftsprozessen ermöglichen. Dazu werden normalerweise vorkonfektionierte Softwaremodule konfiguriert.

Viele mit der Software verbundene Risiken hängen davon ab, wie gut das System konfiguriert wurde, um die Anforderungen des Geschäftsprozesses zu erfüllen. Bei neuer Software und bei aktuellen größeren Aktualisierungen kann es erhöhte Risiken geben.

Kundenspezifische Softwarekomponenten, z B. mit interner Skript-Sprache entwickelte Makros, die geschrieben oder modifiziert wurden, um spezifische geschäftliche Anforderungen des Anwenders zu erfüllen, sollten als Kategorie 5 behandelt werden.

Kategorie 5 – Kundenspezifische Applikationen

Diese Systeme oder Untersysteme werden entwickelt, um einen spezifischen Bedarf des regulierten Unternehmens abzudecken. Das mit kundenspezifischer Software einhergehende Risiko ist hoch. Im Lebenszyklusansatz und bei den Anpassungsentscheidungen sollte dieses erhöhte Risiko beachtet werden, da weder Erfahrungen aus der Anwendung noch Informationen zur Systemzuverlässigkeit vorliegen.

9.2 Anlage 2 – Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis

Anhang 11 zum EG-Leitfaden der Guten Herstellungspraxis

Computergestützte Systeme[2]

Rechtsgrundlage zur Veröffentlichung dieses Leitfadens:
Artikel 47 der Richtlinie 2001/83/EG zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel und Artikel 51 der Richtlinie 2001/82/EG zur Schaffung eines Gemeinschaftskodexes für Tierarzneimittel. Dieses Dokument bietet eine Anleitung für die Auslegung der Grundsätze und Leitlinien der Guten Herstellungspraxis (GMP) für Arzneimittel entsprechend der Richtlinie 2003/94/EG für Humanarzneimittel und der Richtlinie 91/412/EWG für Tierarzneimittel.

Status des Dokuments:
Revision 1

Grund der Änderung:
Der Anhang wurde als Reaktion auf den verstärkten Einsatz computergestützter Systeme und die zunehmende Komplexität dieser Systeme überarbeitet. In der Folge wurden auch für Kapitel 4 des GMP-Leitfadens Änderungen vorgeschlagen.

Termin des Inkrafttretens:
30. Juni 2011

[2] In der Fassung der Bekanntmachung vom 08. August 2011 (BAnz Nr. 125 v. 19.08.2011) Im Text sind jeweils als hochgestellte Ziffern zusätzlich die Satznummern angegeben.

Dokument Typ Checkliste	Dokument Titel Checkliste Audit	Dokument Nr. 2-040
Gültig ab:		Version 1.0

Grundsätze

Der vorliegende Anhang gilt für alle Arten computergestützter Systeme, die als Bestandteil von GMP-pflichtigen Vorgängen eingesetzt werden. Ein computergestütztes System ist eine Kombination aus Software-und Hardwarekomponenten, die zusammen bestimmte Funktionen erfüllen. Die Anwendung sollte validiert, die IT Infrastruktur sollte qualifiziert sein. Wird eine manuelle Tätigkeit durch ein computergestütztes System ersetzt, darf es in der Folge nicht zu einer Beeinträchtigung der Produktqualität, der Prozesskontrolle oder der Qualitätssicherung kommen. Dabei darf sich das Gesamtrisiko des Prozesses nicht erhöhen.

Allgemeines

1. Risikomanagement

Risikomanagement sollte über den gesamten Lebenszyklus des computergestützten Systems unter Berücksichtigung von Patientensicherheit, Datenintegrität und Produktqualität betrieben werden. Als Teil eines Risikomanagementsystems sollten Entscheidungen über den Umfang der Validierung und die Sicherstellung der Datenintegrität auf einer begründeten und dokumentierten Risikobewertung des computergestützten Systems basieren.

2. Personal

Es sollte eine enge Zusammenarbeit zwischen maßgeblichen Personen, wie z. B. Prozesseignern, Systemeignern und Sachkundigen Personen, sowie der IT stattfinden. Alle Personen sollten über eine geeignete Ausbildung und Zugriffsrechte sowie festgelegte Verantwortlichkeiten zur Wahrnehmung der ihnen übertragenen Aufgaben verfügen.

3. Lieferanten und Dienstleister

3.1 Werden Dritte (z. B. Lieferanten, Dienstleister) herangezogen, um z. B. ein computergestütztes System bereitzustellen, zu installieren, konfigurieren, integrieren, validieren, warten (z. B. Fernwartung), modifizieren oder zu erhalten, Daten zu verarbeiten oder im Zusammenhang stehende Serviceleistungen zu erbringen, müssen formale Vereinbarungen abgeschlossen sein, in denen die Verantwortlichkeiten des Dritten eindeutig beschrieben sind. IT-Abteilungen sollten analog zu Dritten behandelt werden.

3.2 Kompetenz und Zuverlässigkeit des Lieferanten sind Schlüsselfaktoren bei der Auswahl eines

Produktes oder eines Dienstleisters. Die Notwendigkeit eines Audits sollte auf einer Risikobewertung basieren.

3.3 Die bei kommerziell erhältlichen Standardprodukten bereitgestellte Dokumentation sollte durch Nutzer im regulierten Umfeld dahingehend überprüft werden, ob die Benutzeranforderungen erfüllt sind.

3.4 Die Informationen zum Qualitätssystem und zu Audits, die Lieferanten oder Entwickler von Software und verwendeten Systemen betreffen, sollten Inspektoren auf Nachfrage zur Verfügung gestellt werden.

Projektphase

4. Validierung

4.1 Die Validierungsdokumentation und -berichte sollten die maßgeblichen Phasen des Lebenszyklus abbilden. Hersteller sollten in der Lage sein, ihre Standards, Pläne, Akzeptanzkriterien, Vorgehensweisen und Aufzeichnungen basierend auf ihrer Risikobewertung zu begründen.

4.2 Die Validierungsdokumentation sollte, sofern zutreffend, Aufzeichnungen im Rahmen der Änderungskontrolle und Berichte über alle während der Validierung beobachteten Abweichungen beinhalten.

4.3 Eine aktuelle Liste aller maßgeblichen Systeme und ihrer GMP-Funktionen (Inventar) sollte zur Verfügung stehen. Für kritische Systeme sollte eine aktuelle Systembeschreibung vorliegen, welche die technische und logische Anordnung, den Datenfluss sowie Schnittstellen zu anderen Systemen oder Prozessen, sämtliche Hard-und Softwarevoraussetzungen und die Sicherheitsmaßnahmen detailliert wiedergibt.

4.4 Die Benutzeranforderungen sollten die erforderlichen Funktionen des computergestützten Systems beschreiben und auf einer dokumentierten Risikobewertung sowie einer Betrachtung der möglichen Auswirkungen auf das GMP System basieren. Die Benutzeranforderungen sollten über den Lebenszyklus verfolgbar sein.

4.5 Der Nutzer im regulierten Umfeld sollte alle erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass das System in Übereinstimmung mit einem geeigneten Qualitätsmanagementsystem entwickelt wurde. Der Lieferant sollte angemessen bewertet werden.

4.6 Für die Validierung maßgeschneiderter Systeme oder für den Kunden spezifisch angepasster computergestützter Systeme sollte ein Verfahren vorliegen, das die formelle Bewertung und Berichterstellung zu Qualitäts-und Leistungsmerkmalen während aller Abschnitte des Lebenszyklus des Systems gewährleistet.

4.7 Die Eignung von Testmethoden und Testszenarien sollte nachgewiesen werden. Insbesondere Grenzwerte für System-/Prozessparameter, Datengrenzen und die Fehlerbehandlung sollten betrachtet werden. Für automatisierte Testwerkzeuge und Testumgebungen sollte eine dokumentierte Bewertung ihrer Eignung vorliegen.

4.8 Werden Daten in ein anderes Datenformat oder System überführt, sollte im Rahmen der Validierung geprüft werden, dass der Wert und /der die Bedeutung der Daten im Rahmen dieses Migrationsprozesses nicht verändert werden.

Betriebsphase

5. *Daten*

Um Risiken zu minimieren sollten Computergestützte Systeme, die Daten elektronisch mit anderen Systemen austauschen, geeignete Kontrollmechanismen für die korrekte und sichere Eingabe und Verarbeitung der Daten enthalten.

6. *Prüfung auf Richtigkeit*

Werden kritische Daten manuell eingegeben, sollte die Richtigkeit dieser Dateneingabe durch eine zusätzliche Prüfung abgesichert werden. Diese zusätzliche Prüfung kann durch einen zweiten Anwender oder mit Hilfe einer validierten elektronischen Methode erfolgen. Die Kritikalität und möglichen Folgen fehlerhafter oder inkorrekt eingegebener Daten für das System sollten im Risikomanagement berücksichtigt sein.

7. *Datenspeicherung*

7.1 Daten sollten durch physikalische und elektronische Maßnahmen vor Beschädigung geschützt werden. Die Verfügbarkeit, Lesbarkeit und Richtigkeit gespeicherter Daten sollten geprüft werden. Der Zugriff auf Daten sollte während des gesamten Aufbewahrungszeitraums gewährleistet sein.

7.2 Es sollten regelmäßige Sicherungskopien aller maßgeblichen Daten erstellt werden. Die Integrität und Richtigkeit der gesicherten Daten sowie die Möglichkeit der Datenwiederherstellung sollten

während der Validierung geprüft und regelmäßig überwacht werden.

8. Ausdrucke

8.1 Es sollte möglich sein, klar verständliche Kopien von elektronisch gespeicherten Daten zu erhalten.

8.2 Von Protokollen, die zur Chargenfreigabe herangezogen werden, sollten Ausdrucke generiert werden können, die eine Veränderung der Daten nach ihrer Ersteingabe erkennen lassen.

9. Audit Trails

Basierend auf einer Risikobewertung sollte erwogen werden, die Aufzeichnung aller GMP-relevanten Änderungen und Löschungen in das System zu integrieren (ein systemgenerierter „Audit Trail“). Bei der Änderung oder Löschung GMP-relevanter Daten sollte der Grund dokumentiert werden. Audit Trails müssen verfügbar sein, in eine allgemein lesbare Form überführt werden können und regelmäßig überprüft werden.

10. Änderungs-und Konfigurationsmanagement

11. Periodische Evaluierung

Jede Änderung an einem computergestützten System einschließlich der Systemkonfigurationen sollte kontrolliert und nach einem festgelegten Verfahren erfolgen.

Computergestützte Systeme sollten periodisch evaluiert werden, um zu bestätigen, dass sie sich noch im validen Zustand befinden und die GMP-Anforderungen erfüllen. Solche Evaluierungen sollten, sofern sachgerecht, den derzeitigen Funktionsumfang, Abweichungsaufzeichnungen, Vorfälle, Probleme, Aktualisierungen, Leistung, Zuverlässigkeit, Sicherheit und Berichte zum Validierungsstatus umfassen.

12. *Sicherheit*

12.1 Es sollten physikalische und / oder logische Maßnahmen implementiert sein, um den Zugang zu computergestützten Systemen auf autorisierte Personen zu beschränken. Geeignete Maßnahmen zur Vermeidung unerlaubten Systemzugangs können die Verwendung von Schlüsseln, Kennkarten, persönlichen Codes mit Kennworten, biometrische Verfahren sowie den eingeschränkten Zugang zu Computern mit zugehöriger Ausrüstung und Datenspeicherungsbereichen einschließen.

12.2 Der Umfang der Sicherheitsmaßnahmen ist von der Kritikalität des computergestützten Systems abhängig.

12.3 Erteilung, Änderung und Entzug von Zugriffsberechtigungen sollten aufgezeichnet werden.

12.4 Systeme zur Verwaltung von Daten und Dokumenten sollten die Identität des Anwenders, der Daten eingibt, ändert, bestätigt oder löscht, mit Datum und Uhrzeit aufzeichnen.

13. Vorfallmanagement

Alle Vorfälle, nicht nur Systemausfälle und Datenfehler, sollten berichtet und bewertet werden. Die Ursache eines kritischen Vorfalls sollte ermittelt werden und die Basis für Korrektur-und Vorbeugemaßnahmen sein.

14. *Elektronische Unterschrift*

Elektronische Aufzeichnungen können elektronisch signiert werden. Von elektronischen Unterschriften wird erwartet, dass sie

a) im Innenverhältnis eines Unternehmens die gleiche Bedeutung haben wie handschriftliche Signaturen,

b) dauerhaft mit dem zugehörigen Dokument verbunden sind,

c) die Angabe des Datums und der Uhrzeit der Signatur beinhalten.

15. *Chargenfreigabe*

Wird ein computergestütztes System zur Aufzeichnung der Chargenzertifizierung und -freigabe eingesetzt, sollte durch das System sichergestellt werden, dass nur Sachkundige Personen die Chargenfreigabe zertifizieren können. Das System sollte diese Personen eindeutig identifizieren und die Identität der zertifizierenden oder freigebenden Person dokumentieren. Eine elektronische Chargenzertifizierung oder -freigabe sollte mittels elektronischer Unterschrift erfolgen.

16. *Kontinuität des Geschäftsbetriebes*

Wenn computergestützte Systeme kritische Prozesse unterstützen, sollten Vorkehrungen getroffen sein, um die fortlaufende Unterstützung dieser Prozesse im Falle eines Systemausfalls sicherzustellen (z. B. durch ein manuelles oder ein alternatives System). Der erforderliche Zeitaufwand zur Inbetriebnahme dieser alternativen Verfahren sollte jeweils für ein bestimmtes System und die

unterstützten Prozesse risikoabhängig festgelegt werden. Diese Verfahren sollten angemessen dokumentiert und getestet werden.

17. *Archivierung*

Daten können archiviert werden. Diese Daten sollten auf Verfügbarkeit, Lesbarkeit und Integrität geprüft werden. Sind maßgebliche Änderungen am System erforderlich (z. B. Computer und zugehörige Ausrüstung oder Programme), sollte sichergestellt und getestet werden, ob die Daten weiterhin abrufbar sind.