Geltungsbereich	Inspektorat	
Schlüsselwörter	Inspektion, Computer	
Querverweise	AiM 071211, AiM 071218, Votum V11002, Votum V11003	
erstellt	EFG 11	
fachlich geprüft	Dr. Arno Terhechte (EFG 11)	31.08.2022
formell geprüft	Dr. Katrin Reder-Christ (ZLG)	31.08.2022
Beschlussfassung durch:	☒ erstellende EFG ☐ Länderreferentengremien	
beschlossen	EFG 11	29.08.2022
	Humanarzneimittelbereich Carolyn Hoops, Vorsitzende AG AATB	- entfällt -
	Tierarzneimittelbereich Dr. Dagmar Duda-Spiegel, Vorsitzende AG TAM	- entfällt -
	Tierimpfstoffbereich Dr. Barbara Stetter, Vorsitzende AG TT	- entfällt -
in Kraft gesetzt		
	gültig ab	

Inhaltsverzeichnis

1 Vorbemerkung 3
2 Inspektion eines computergestützten Systems gemäß Anhang 11 4
Grundsatz (Principle) 4
Allgemeines (General) 5
1. Risikomanagement (Risk Management) 5
2. Personal (Personnel) 8
3. Lieferanten und Dienstleister (Suppliers and Service Providers) 10
Projektphase (Project Phase) 13
4. Validierung (Validation) 13
Betriebsphase (Operational Phase) 20
5. Daten (Data) 20
6. Prüfung auf Richtigkeit (Accuracy Checks) 22
7. Datenspeicherung (Data Storage) 24
8. Ausdrucke (Printouts) 28
9. Audit Trails (Audit Trails) 29
10. Änderungs- und Konfigurationsmanagement (Change and Configuration Management) 33
11. Periodische Evaluierung (Periodic evaluation) 35
12. Sicherheit (Security) 36
13. Vorfallmanagement (Incident Management) 42
14. Elektronische Unterschrift (Electronic Signature) 44
15. Chargenfreigabe (Batch release) 47
16. Kontinuität des Geschäftsbetriebes (Business Continuity) 48
17. Archivierung (Archiving) 51
3 Definitionen und Abkürzungen 54
4 Anlagen und Formulare 60
5 Änderungsgrund 60
6 Literaturhinweise 60

1 Vorbemerkung

Das vorliegende AiM befasst sich mit der Inspektion computergestützter Systeme (CS).

Der Prozess der digitalen Transformation in der pharmazeutischen Industrie geht einher mit der Einführung neuer Technologien (agile Softwareentwicklung, künstliche Intelligenz u. a.) und Servicemodellen (Cloud Computing). Ebenso hat sich das regulatorische Umfeld im Besonderen durch Regelungen zum Thema Datenintegrität (u. a. PIC/S PI 041-1) seit 2015 gravierend geändert. Obwohl die aktuelle Revision des Anhang 11 ‚Computergestützte Systeme' des EU-GMP-Leitfadens noch nicht abgeschlossen ist, wurde das AiM aktualisiert, um die Veränderungen im Rahmen von Inspektionen zu adressieren und den Einstieg in die Inspektion computergestützter Systeme zu erleichtern.

Die Gliederung des Fragen- und Kommentierungsteiles (→ Kap. 2) folgt dem Aufbau des Anhangs 11[1]. Dessen Text sowie die amtliche deutsche Übersetzung[2] werden den einzelnen Abschnitten in kursiver Schrift vorangestellt. Nachfolgend sind jeweils Anmerkungen zum Text aufgeführt.

Zu jedem Abschnitt enthält dieses AiM Fragen, die bei einer Inspektion gestellt werden können. Entsprechende Kommentare dazu sollen als Grundlage für die Bewertung der erhaltenen Antworten dienen. Wo erforderlich, sind Verweise auf andere Kapitel und Anhänge des EU-GMP-Leitfadens aufgeführt.

Das AiM enthält ferner einen Abschnitt Definitionen und Abkürzungen, in dem auch das Glossar aus dem Anhang 11 enthalten ist (→ Kap. 3). Die Terminologie kann in einzelnen Unternehmen von den hier verwendeten Begriffen abweichen. So werden z. B. 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 diesem AiM nicht immer aktuell abgebildet werden. In Zweifelsfällen wird empfohlen, konkrete Fragen an die EFG 11 (Computergestützte Systeme) zu richten oder deren Mitglieder hinzuzuziehen.

Weitere Informationen sind im Frage- und Antwort-Papier der EMA zum Anhang 11[3] sowie in Voten der EFG 11 zu finden.

[1] https://ec.europa.eu/health/document/download/8d305550-dd22-4dad-8463-2ddb4a1345f1_en?filename=annex11_01-2011_en.pdf

[2] https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Statistiken/GKV/Bekanntmachungen/GMP-Leitfaden/Anlage_2_zur_Bekanntmachung_-_Annex_11.pdf

[3] https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-manufacturing-practice/guidance-good-manufacturing-practice-good-distribution-practice-questions-answers

2 Inspektion eines computergestützten Systems gemäß Anhang 11

Grundsatz (Principle)	
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.*	
This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities. *The application should be validated; IT infrastructure should be qualified.* *Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.*	
Nr.	**Anmerkungen**
G-1	Im Fokus des Anhangs 11 stehen GMP-kritische Prozesse, bei denen CS eingesetzt werden. Für den Bereich Forschung und Entwicklung ist die Umsetzung dieser Anforderungen empfehlenswert, aber nicht obligat. Für GDP-Prozesse kann dieser Anhang zur Spezifizierung der Angaben der GDP-Richtlinie dienen. Für die Anwendbarkeit des Anhangs 11 ist es nicht entscheidend, wo das CS betrieben wird (‚on-premise' oder bei einem Dienstleister/‚cloud service provider'). GMP-kritische Prozesse sind solche, die im EU-GMP-Leitfaden genannt sind. Diese können steuernder, datenverarbeitender oder dokumentierender Art sein.
G-2	Ein CS besteht nicht nur aus Software und Hardware. Wichtig sind ebenso die Infrastruktur/Umgebung, in die es integriert ist, und die Personen, die das System bedienen. Mit Anforderung der Inventarliste im Rahmen der Inspektionsvorbereitung kann sich die Inspektorin/der Inspektor einen ersten Eindruck von der Systemlandschaft verschaffen. Anhand einer Checkliste/Verfahrensanweisung sollte der ‚regulated user' (RU) die Einteilung in GxP-kritische und -unkritische Systeme durchgeführt haben. (→ Anhang 11 Nr. 4.3).
G-3	Die Terminologie der Validierung von Applikationen und der Qualifizierung der Infrastruktur ist mit der Definition von Validierung (von Prozessen) und Qualifizierung (von Anlagen) in der AMWHV konsistent. Informationen über den Stand der Validierungs- und Qualifizierungsaktivitäten sind Bestandteil des VMP (und dessen Anlagen). Der VMP liefert einen Überblick über

	den Qualifizierungs- und Validierungsstatus computergestützter Systeme und kann im Rahmen der Inspektionsvorbereitung gesichtet werden.
G-4	Die Maßgabe, hinsichtlich Produktrisiko, Risiko für die Patientinnen/Patienten sowie dem Ausmaß der Qualitätssicherung und Datenintegrität die gleiche Sicherheit wie bei manuellen Prozessen zu erzielen, bleibt im Anhang 11 (Rev. 1) unverändert. Dieses gilt ebenfalls für den Fall, dass computergestützte Prozesse/Systeme und Daten ausgelagert werden.

Allgemeines (General)

1. Risikomanagement (Risk Management)

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.

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

Nr.	Anmerkungen
1-1	Ein Risikomanagementsystem soll bezüglich CS etabliert und auch für diesen Bereich in das Qualitätsmanagementsystem des Unternehmens eingebunden sein, um die GMP-Compliance zu gewährleisten. Beim Risikomanagement sind alle Aspekte des GMP-Umfeldes zu berücksichtigen, wie Sicherheit der Patientinnen/Patienten, Datenintegrität, Datenqualität und Produktqualität. Risikomanagement soll über den gesamten Lebenszyklus des CS betrieben werden. Viele Risikoanalysen beschränken sich auf Risiken im Zusammenhang mit einer Funktionalität. Zu betrachten sind ebenfalls die Risiken in Bezug auf die Vollständigkeit, Unveränderbarkeit, Lesbarkeit und Verfügbarkeit von GMP-kritischen Daten.
1-2	Grundlage für den Einsatz von CS im GMP-Umfeld ist deren fundierte und dokumentierte Risikobewertung (‚risk assessment') anhand festgelegter, begründeter und nachvollziehbarer Kriterien. Mittels methodischer Vorgehensweise werden CS in einem ausreichend hohen Detaillierungsgrad analysiert und hinsichtlich ihrer Ergebnisse und Auswirkungen auf ein (pharmazeutisches) Produkt, die Sicherheit für die Patientinnen/Patienten, die Datenqualität und Datenintegrität untersucht. Ein von den RU vielfach zur Risikobewertung genutztes Instrument ist die FMEA. Bei der Berechnung der Risikoprioritätszahl (RPZ) wird häufig die Auftretenswahrscheinlichkeit miteinbezogen, was nur sinnvoll ist, wenn die Werte empirisch zu untermauern sind. Hinsichtlich der Risiken bezogen auf die Datenintegrität sollte unterschieden werden zwischen dem Risiko für die Daten selbst (Veränderung, Löschung) und dem Risiko, welches sich aus nicht korrekten Daten für den Prozess, die Produktqualität und die Patientinnen/Patienten ergeben würde.

1-3	Die Ergebnisse der Risikobewertung dienen ihrerseits als Grundlage für die Entscheidungen über den Umfang der Validierung, Qualifizierung und der notwendigen Maßnahmen zur Sicherstellung der Datenintegrität/-qualität.	
1-4	Insbesondere bei Änderungen von CS ist bereits in der Projektphase eine erneute Risikobewertung durchzuführen. In regelmäßigen Abständen ist diese im Rahmen der periodischen Evaluierung zu wiederholen. Der Umfang einer erneuten Risikobewertung sollte von der Art der Änderung sowie von der Kritikalität des CS und des davon unterstützten Prozesses abhängen.	
Nr.	**Fragen und Bezug**	**Kommentierung**
1-5	Inwieweit beeinflussen CS oder Prozesse die Sicherheit für Patientinnen/Patienten, die Produktsicherheit oder die Qualität und Integrität der elektronischen Daten? Inwieweit sind CS involviert in Prozesse, die mittelbar oder unmittelbar die Qualität eines Arzneimittels beeinflussen oder Daten prozessieren, die erforderlich sind, um den Werdegang einer Charge nachzuvollziehen?	Mit dieser Fragestellung können kritische Systeme identifiziert werden. Diese sollten bei einer Inspektion vorrangig berücksichtigt werden. Dieses sind beispielsweise Systeme, • die Produktionsprozesse auf der Feldebene steuern (z. B. Reaktorsteuerung, Abfüllanlage, Mischer) oder • die übergeordnete Prozesse steuern (PLS, MES) oder • die im näheren Produktionsumfeld (z. B. RLT-Anlagen, CIP-/SIP-Prozesse, Anlagen zur Produktion und Verteilung von WFI oder Aqua purificata) oder im Bereich der IPC und Qualitätskontrolle (Multifunktionstester, HPLC-Systeme, CDS, LIMS, ELN) eingesetzt werden.
1-6	Welche Maßnahmen zur Risikominimierung wurden im Rahmen des Risikomanagements festgelegt?	Bei bestehenden Systemen können in manchen Fällen nicht alle Anforderungen nach GMP und ALCOA+ erfüllt werden. Technisch-funktionale Maßnahmen (Bedienerkonzepte, Audit Trail-Funktionalität, Automatisierung, Schnittstellen, gehärtete Konfiguration) sind immer organisatorischen Maßnahmen (SOP, zusätzliche Dokumentation, 4-Augenprinzip bei manuellen Eingaben etc.) vorzuziehen, da sie dem Konzept der integrierten Sicherheit folgen. Ein automatisierter validierter Prozess ist einem manuellen Prozess – auch wenn er kontrolliert wird – vorzuziehen. Organisatorische Maßnahmen können interimsweise den Zeitraum bis zur Anschaffung geeigneter Systeme absichern. Der Umfang der risikominimierenden technischen und/oder organisatorischen Maßnahmen steigt mit dem Risiko.

1-7	Welche Aussagen machen übergeordnete QS-Dokumente zur Identifizierung und Bewertung von Risiken?	Der Umgang mit CS muss in die relevanten Qualitätssysteme eingebunden sein. Das Verfahren zur Durchführung einer Risikobewertung, die zu beteiligenden Personen, die Anforderungen an die Dokumentation und das Follow-up sind in einer Verfahrensanweisung zu beschreiben. Eine Nachverfolgbarkeit (‚tracebility') von Risiken und risikominimierenden Maßnahmen muss möglich sein.
1-8	Welche akuten und prospektiven Risikoabwehrmaßnahmen lassen sich daraus ableiten?	Der grundsätzliche Umgang zur Risikobeseitigung und -prävention sollte im QS-System beschrieben sein.
1-9	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 Sicherheit der Patientinnen/Patienten, Produktqualität sowie Integrität und Qualität der Daten untersucht werden.
1-10	Grundsätzlich ist es erforderlich, prospektiv zu validieren. In Einzelfällen kann eine retrospektive Validierung durchgeführt worden sein. Wurde eine Risikobewertung im Rahmen einer retrospektiven Validierung durchgeführt?	Folgende Aktivitäten bezüglich der Risikobewertung werden im Rahmen einer retrospektiven Validierung mindestens erwartet (→ Abschnitt Validierung): • 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.
1-11	Wie ist die Risikobewertung in das Änderungsmanagementsystem für CS eingebunden?	Änderungen sollten einer Bewertung hinsichtlich der Risiken unterzogen werden.
1-12	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 Sicherheit der Patientinnen/Patienten, 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. Diese sollte sowohl kritische Funktionen als auch Risiken für die Datenintegrität identifizieren. Das Ergebnis der Risikobewertung beeinflusst das Ausmaß der Validierungsaktivitäten und der Maßnahmen zur Sicherstellung der Datenintegrität. Risikomanagement beinhaltet die Implementierung von risikominimierenden Maßnahmen und die Überprüfung ihrer Wirksamkeit.
1-13	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.

2. Personal (Personnel)

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.

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Nr.	Anmerkungen
2-1	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), welches 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.
2-2	Zur Wahrnehmung der Aufgaben sollten alle Mitarbeitenden über festgelegte Verantwortlichkeiten und angemessene Zugriffsrechte verfügen.
2-3	Zugriffsrechte sollten nur an Mitarbeitende vergeben werden, die ausreichend geschult sind.
2-4	Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die diesbezüglich ausreichend geschult sind.

Nr.	Fragen und Bezug	Kommentierung
2-5	Welche Qualifikation besitzt das IT-Personal?	Der Grundsatz von GMP, dass Personal nur entsprechend seiner Kenntnisse und Fähigkeiten eingesetzt werden soll, gilt auch für IT-Personal. Die Einarbeitung neuer Mitarbeiterinnen/Mitarbeiter im IT-Bereich sollte die Schulung in den wesentlichen GMP-Schwerpunkten berücksichtigen.
2-6	Wie ist das Personal geschult? In welcher Art und Weise umfasst der Schulungsplan die Anforderungen an den Umgang mit CS?	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 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. Die regelmäßige Schulung des IT-Personals in wesentlichen GMP-Schwerpunkten sollte sich im Schulungsplan widerspiegeln.
2-7	In welchem Umfang wird das IT-Personal in GMP-Themen geschult?	Das IT-Personal sollte insbesondere zur Dokumentation und zum Änderungs-/Konfigurations- und Abweichungsmanagement geschult sein. Die Anforderung an Datenintegrität sollten bekannt sein.
2-8	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.
2-9	Wie sind die Verantwortlichkeiten bei den involvierten Personen festgelegt?	Es kann kritisch hinterfragt werden, ob die verantwortlichen Personen auch mit den nötigen Kompetenzen ausgestattet sind.
2-10	Welche Personen sind zur Eingabe oder Änderung von Daten ermächtigt?	Die Eingabe oder Änderung von Daten sollte nur von solchen Personen vorgenommen werden, die fachlich kompetent, geschult und dazu ermächtigt 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.
2-11	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.

3. Lieferanten und Dienstleister (Suppliers and Service Providers)

3.1 *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. IT-Abteilungen sollten analog zu Dritten behandelt werden.*

3.1 *When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.*

Nr.	Fragen und Bezug	Kommentierung
3-1	Welche Leistungen und Pflichten sind vertraglich vereinbart worden?	Die Vertragsgestaltung soll eindeutig sein, die Aufgaben/Verantwortlichkeiten sollen detailliert beschrieben sein (‚service level agreement', Verantwortungsabgrenzungsvertrag). Reaktionszeiten sollen definiert sein.
3-2	Welche Personen wurden einbezogen?	Mindestens Prozesseigner und Systemeigner sollten in die Vertragsgestaltung eingebunden sein.
3-3	Wie werden im Unternehmen Dienstleister definiert?	Dienstleister sind alle diejenigen, die Serviceleistungen erbringen, unabhängig davon, ob diese zum Firmenverbund/Konzern gehören oder nicht.
3-4	Welche Vorgaben und Regelungen existieren bei Fernwartung/-zugriff?	Der Fernzugriff sollte mit Anmeldung und Freigabe durch den Kunden erfolgen. Fehlerbehebungen, Korrekturen und/oder Änderungen müssen erfasst und bewertet werden. Es muss sichergestellt sein, dass keine nicht autorisierten Änderungen am System erfolgen.

3-5	Wird für die Speicherung von GxP-Daten oder für die Installation oder den Betrieb einer Applikation (DMS, LIMS, MES, ERP etc.) ein externer Dienstleister im Sinne eines Cloud-Service genutzt?	Zunächst ist zu klären, welches Bereitstellungsmodell (‚public cloud', ‚community cloud' oder ‚private cloud' genutzt wird) und welches Servicemodell (IAAS, PAAS, SAAS) genutzt wird. Ebenfalls sollte eine Risikobewertung des RU vorhanden sein, die die Applikation und die Daten hinsichtlich ihrer Kritikalität bezogen auf Verfügbarkeit, Vertraulichkeit und Unveränderbarkeit bewertet und einstuft. Daraus resultiert die Entscheidung, ob ein Cloud-Service geeignet ist und welches Service- und Bereitstellungsmodell zu wählen ist. Für Details zu den Anforderungen wird auf das Votum zur externen Speicherung von Daten verwiesen.
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.*		
3.2 *The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.*		
Nr.	**Fragen und Bezug**	**Kommentierung**
3-6	Wie und von wem wurde die Bewertung des Lieferanten bzw. des Dienstleisters vorgenommen?	Eine Verfahrensanweisung, die den Prozess und die Kriterien für die Lieferanten- und Dienstleisterqualifizierung beschreibt, sollte vorhanden sein. Im Rahmen der Qualifizierung können Kenntnisse über den Lieferanten, Erfahrungen mit dem Lieferanten, Referenzen, Zertifizierungen des Lieferanten bzw. des Dienstleisters mit einbezogen werden. Zertifizierungen sind auf den zu Grunde gelegten Standard/die zu Grunde gelegte Norm, den Umfang, die Aktualität und die Gültigkeit zu prüfen. Öffentlich zugängliche Datenbanken ermöglichen eine Echtheitsprüfung. Eine rein kaufmännische Bewertung ist nicht akzeptabel.
3-7	Wurde ein Audit durchgeführt? Von wem wurde das Audit durchgeführt und wer stellt sicher, dass festgestellte Mängel beseitigt werden?	Es sollte interne Festlegungen geben, in welchen Fällen ein Audit erforderlich ist und von wem das Audit durchgeführt wird. Zu berücksichtigen ist ebenfalls ein adäquates Follow-up. Das Auditteam sollte über entsprechenden IT-Sachverstand, Prozess- und QS-Kenntnisse

		verfügen (z. B. IT/‚subject matter expert', Prozesseigner, QS). Es gibt unterschiedliche Formen eines Audits: ein Fragebogen (‚questionnaire') oder ein vor-Ort-Audit. Ein vor-Ort-Audit kann durch mehrere RU durchgeführt werden (Joint Audit) oder durch einen Dienstleister.
3-8	Welche Kriterien bestimmen das Risiko eines CS?	Folgende Kriterien bestimmen das Risiko: • direkter (SPS, PLS, MES, CDS, LIMS) oder indirekter Einfluss (DMS, CAPA, DEVOPs, Training) auf die Produktqualität. • Softwarekategorie (COTS Klasse 4 oder Klasse 5) • Art der Bereitstellung (intern oder extern)
3.3 *Die bei kommerziell erhältlichen Standardprodukten bereitgestellte Dokumentation sollte durch Nutzer im regulierten Umfeld dahingehend überprüft werden, ob die Benutzeranforderungen erfüllt sind.*		
3.3 *Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.*		
Nr.	**Fragen und Bezug**	**Kommentierung**
3-9	Wie wurde überprüft, ob das Standardprodukt die Benutzeranforderungen erfüllt?	Es soll ein dokumentierter Abgleich der Benutzeranforderungen gegen die vom Lieferanten zur Verfügung gestellte Dokumentation durchgeführt werden. Abweichungen sollen einer Risikobetrachtung unterzogen werden.
3-10	Welche Prüfungen sollte der RU in der Betriebsumgebung durchführen?	Der ‚User Acceptance Test' (UAT) ist in der Betriebsumgebung des RU durchzuführen. Bei COTS Produkten können funktionale Tests des Softwareherstellers (Grundfunktionalität) den Validierungsumfang des RU reduzieren. Die RU-spezifische Konfiguration muss dokumentiert und verifiziert sein. Wenn auf die Dokumentation des Softwareherstellers Bezug genommen wird, muss diese verfügbar und durch den RU bewertet sein.
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.*		
3.4 *Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.*		

Nr.	Anmerkungen
3-11	Die Lieferantenbewertung, das Pflichtenheft sowie weitere Qualifizierungsdokumente sollen chronologisch und plausibel vorliegen. Inspektoren haben die Möglichkeit, Auditberichte einzusehen.
Projektphase (Project Phase)	
4. Validierung (Validation)	
Nr.	**Anmerkungen**
4-1	Die Anwendung soll validiert, die IT-Infrastruktur soll qualifiziert werden. (Anhang 11 – Grundsätze)
4-2	Die Qualifizierung von IT-Infrastruktur ist eine klar formulierte Anforderung des Anhangs 11. Mit der Wahrnehmung sind die Systemeigner (in der Regel IT-Abteilungen) befasst. Sofern ‚Cloud Service Provider' (CSP) oder andere Dienstleister die Infrastruktur bereitstellen, hat das keinen Einfluss auf die Anforderung selbst. Ob der CSP seine Infrastruktur qualifiziert hat und der Prozess der Qualifizierung in seinem Qualitätssicherungssystems beschrieben ist, ist im Rahmen der Qualifizierung des Dienstleisters und dem fortwährendem Monitoring durch den RU zu prüfen.
4-3	Vorgaben, die die Qualifizierungsanforderungen von IT-Infrastruktur beschreiben, finden sich z. B. in Form von Spezifikationen für Server, Scanner, Switche, Drucker, Verfahrensanweisungen und Protokollen über die Qualifizierung. Hardware-Infrastruktur wird immer mehr durch Software ersetzt. Damit ändert sich auch die Methodik der Qualifizierung. Bei Software stehen eher die Konfiguration und der Prozess im Vordergrund. Die automatisierte Bereitstellung von Infrastruktur und die Prozesskontrolle der Bereitstellung und Installation über Monitoringtools haben Einfluss darauf, wie die spezifikationskonforme Installation und Funktion von Infrastruktur im Sinne einer Qualifizierung nachgewiesen werden.
***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.*	
***4.1** The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.*	
Nr.	**Anmerkungen**
4-4	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. Computergestützte Systeme, die künstliche Intelligenz nutzen, d. h. Entscheidungen nicht auf Basis definierter Algorithmen, sondern auf Basis von Trainingsdaten durch komplexe, sich verändernde Algorithmen treffen, sind mit diesem klassischen Ansatz nicht zu validieren. Ein europäisch einheitlicher Standard zu den Anforderungen an die Validierung ist bis dato nicht verfügbar. Das Hauptaugenmerk sollte auf der Relevanz, Angemessenheit und Integrität der Daten liegen, die zum Testen dieser Modelle verwendet werden, sowie auf den Ergebnissen dieser Tests und soweit verfügbar im Vergleich zu bereits akzeptierten Standards.	
Nr.	**Fragen und Bezug**	**Kommentierung**
4-5	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 für einen definierten Zweck validieren. Im Falle von konfigurierbarer Software kann der Hersteller Grundfunktionalitäten testen und prüfen, so dass sich der RU auf die Verifizierung der spezifischen Konfiguration beschränkt. In diesen Fällen sollte die entsprechende Dokumentation des Softwareherstellers vorliegen und bewertet sein. Auf dieser Basis kann der Umfang der spezifischen Validierung in der Anwendungsumgebung festgelegt werden.
4-6	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 Betriebsumgebung unter Betriebsbedingungen) • Vorgabedokumente (Spezifikationen) und korrespondierende Berichte zu den maßgeblichen Phasen (s. o.) Bei der Verwendung alternativer Modelle sollte deren Eignung belegt sein.
4-7	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?	Im Rahmen der Inspektion kann der Validierungsumfang bei einem kritischen mit einem unkritischen Prozess/Funktionalität verglichen werden. Bei einem unkritischen Prozess kann ggf. eine ausschließliche Funktionsprüfung ausreichen. Bei einem kritischen Prozess könnte man Spezifikationsgrenzen abprüfen oder auch Falscheingaben wie z. B. Buchstaben statt Zahlen.
4-8	Inwieweit wurde das V-Modell bei der agilen Softwarenentwicklung beachtet?	Die Zeitersparnis bei agilen Methoden wird dadurch erreicht, dass Funktionalitäten von verschiedenen Entwickler(gruppen) parallel in kurzen Zeiträumen entwickelt werden. Interessant ist, wie dabei Grundanforderungen des V-Modells (‚user requirement', Umsetzung, Verifizierung und insbesondere die Integration der Funktionalität) nachvollziehbar dokumentiert sind. Dabei ist es nicht erforderlich, dieses in papiergestützter Form zu realisieren. Die Traceability, das Konfigurationsmanagement und die Testdokumentationen lassen sich besser über elektronische Systeme gewährleisten.
4.2 *Die Validierungsdokumentation sollte, sofern zutreffend, Aufzeichnungen im Rahmen der Änderungskontrolle und Berichte über alle während der Validierung beobachteten Abweichungen beinhalten.*		
4.2 *Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.*		
Nr.	**Fragen und Bezug**	**Kommentierung**
4-9	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.

4-10	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 sowie GMP-kritische Abweichungen vor Inbetriebnahme des Systems beseitigt werden. Werden Abweichungen nicht beseitigt, ist eine Bewertung vorzunehmen und der Grund dafür zu dokumentieren.

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.*

4.3 *An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.*

Nr.	Fragen und Bezug	Kommentierung
4-11	Welche computergestützten Systeme werden betrieben? Welchen Zweck/welche Funktionalität haben diese Systeme? Welche Systeme wurden als GMP-kritisch eingestuft?	Erwartet wird eine aktuelle, ggf. modulare Aufstellung, die ein gelenktes Dokument darstellt. Für GMP-kritische Systeme sollte eine Systembeschreibung vorliegen.
4-12	Auf Grund welcher Kriterien wurde ein System als GMP-kritisch eingestuft?	Erwartet wird eine SOP oder Checkliste und eine schriftliche Bewertung auf Basis der SOP oder Checkliste für jedes System.

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 des Systems verfolgbar sein.*

4.4 *User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.*

Nr.	Anmerkungen
4-13	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.

Nr.	Fragen und Bezug	Kommentierung
4-14	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.
4-15	Wie werden Benutzeranforderungen formuliert?	Benutzeranforderungen sollten so formuliert werden, dass sie nachprüfbar bzw. verifizierbar sind.
4-16	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.
4-17	Wurden die Ergebnisse der Risikobewertung bei der Erstellung der Benutzeranforderungen berücksichtigt? Welche Anforderungen wurden als kritisch bewertet und warum?	Bsp.: Wenn die Verfügbarkeit von GMP-Daten als kritisch eingestuft wurde, muss sich dieses in den Benutzeranforderungen wiederfinden. Notwendige risikominimierende Maßnahmen könnten z. B. die Forderung nach redundanten Systemen oder einer USV 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.*		
4.5 *The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.*		

Nr.	Anmerkungen
4-18	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.

Nr.	Fragen und Bezug	Kommentierungen
4-19	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 oder in anderer Weise bewertet werden.

4-20	Wurde für die Bewertung des Lieferanten auf eine Zertifizierung Bezug genommen?	Wenn der Lieferant nach einem geeigneten Standard zertifiziert und dies in der Lieferantenbewertung berücksichtigt wurde, sollte erfragt werden, ob das betreffende System durch Anwendung des (zertifizierten) QM-Systems entwickelt wurde. Umfang und Aktualität des Zertifikats sollten geprüft 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.*		
***4.6** For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.*		
Nr.	**Anmerkungen**	
4-21	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. Bei Datenbanken handelt es sich vielfach um maßgeschneiderte oder individuell konfigurierte Systeme.	
Nr.	**Fragen und Bezug**	**Kommentierungen**
4-22	Welche Dokumente sind bei maßgeschneiderten Systemen zusätzlich erstellt worden im Vergleich zu konfigurierbaren Standard-Software Paketen?	Maßgeschneiderte Systeme werden speziell für eine Anwendung und einen Kunden entwickelt. Auf Anforderung müssten Aktivitäten zum ‚code 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. Konfigurierbare Softwarepakete werden ggf. durch spezifisch programmierte ‚add-ons' an die Kundenwünsche angepasst. Diese ‚add-ons' sind dann ebenfalls maßgeschneidert (GAMP Klasse 5).
4-23	Wie und wo werden die Konfigurationseinstellungen eines Systems dokumentiert? Lassen sich Änderungen der Konfiguration nachvollziehen? Lässt sich die je-	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.

	weilige Konfiguration einem spezifischen Softwarestand/Release zuordnen?	Zur jeweiligen Konfiguration soll auch die jeweilige Version (‚release') der Software dokumentiert sein.
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.*		
4.7 *Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.*		
Nr.	**Fragen und Bezug**	**Kommentierungen**
4-24	Wie wurde die Eignung der Testfälle nachgewiesen?	Aus der Testbeschreibung kann man das erwartete Testergebnis und die Testdurchführung entnehmen.
4-25	Wie werden kritische Datenfelder überprüft?	Insbesondere wenn kritische Daten Folgeaktionen auslösen, sollten Grenzwerte und andere Werte oder Datenformate (z. B. Buchstaben statt Zahlen) für Testzwecke verwendet werden.
4-26	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. Automatisiertes Testen wird z. B. für das Regressionstesten nach Änderungen der Applikationssoftware, aber auch nach Änderungen der Plattform/des Betriebssystems eingesetzt.
4.8 *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.*		
4.8 *If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.*		
Nr.	**Anmerkungen**	
4-27	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.	
4-28	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.	

Nr.	Fragen und Bezug	Kommentierung
4-29	Wie wird die Größe der Stichprobe bestimmt, die im Rahmen eines Migrationsprozesses überprüft wird?	Das hängt ab von der Kritikalität der Daten (z. B. Verfahrensanweisungen, Schulungs- und Chargendokumentationen, Vertriebsdaten, Herstell- oder Prüfmethoden). In jedem Fall sollten alle unterschiedlichen Ausgangsformate überprüft werden. Bei der Migration muss sichergestellt sein, dass Daten und Metadaten vollständig migriert werden. Statistisch repräsentative Stichprobengrößen kann man z. B. der DIN ISO 2859 Teil 1 entnehmen.
4-30	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.
4-31	Wie ist sichergestellt, dass die Bedeutung der Werte und die 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.

Betriebsphase (Operational Phase)

5. Daten (Data)

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.

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

Nr.	Anmerkungen
5-1	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. Diese so genannten Schnittstellen sollten initial bei der Validierung und nachfolgend bei der periodischen Evaluierung 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.	
5-2	Ergänzend sind geeignete Kontrollmaßnahmen im Sinne integrierter technischer Kontrollen zu etablieren, um die Integrität der Daten für die einzelnen Prozesse zu gewährleisten. Bei netzwerkbasiertem Datentransfer sind spezifische Protokolle (z. B. https) zu verwenden. Interne Datenübertragungen sind durch Checksummen oder Hashwerte abzusichern.	
5-3	Man unterscheidet zwischen unidirektionalen und bidirektionalen Schnittstellen. Bei ersteren werden Daten immer in eine Richtung übertragen, während bidirektionale Daten in beide Richtungen transferieren.	
Nr.	**Fragen und Bezug**	**Kommentierung**
5-4	Zwischen welchen Systemen werden Daten übertragen? Welche Systeme tauschen Daten untereinander aus?	Anhand der Kritikalität der Systeme kann bei der Inspektion entschieden werden, ob eine nähere Prüfung erfolgen soll. Beispiele für Schnittstellen mit wahrscheinlich hoher Kritikalität wären CDS und LIMS, MES und PLS, ERP und MES, LIMS und ERP.
5-5	Welche technischen Protokolle für die Datenübertragung werden verwendet?	Grundsätzlich sind technische Maßnahmen, welche bei Datenübertragungen die Vollständigkeit und Unveränderbarkeit der Daten sicherstellen/unterstützen, zu empfehlen. Sobald der Datentransfer über das firmeneigene, interne Netzwerk hinausgeht (z. B. Datenaustausch mit Laboren, Lohnherstellern oder externen Dienstleistern), sollten diese Maßnahmen geübte Praxis sein.
5-6	Wurde die Schnittstelle, an der eine Umwandlung von Daten erfolgt, spezifiziert?	Bei der Umwandlung von Daten an Schnittstellen kann es zu Veränderungen der Einheiten (z. B. g statt zuvor kg) oder auch Änderungen im Datenformat (z. B. Komma oder Punkt als Dezimaltrenner) kommen. Die Schnittstellen sind entsprechend zu spezifizieren.
5-7	Auf welche Weise erfolgt die Übertragung von Datensätzen getrennter Systeme (‚stand-alone'-Systeme), die keine automatische/direkte Schnittstelle haben?	Daten sollen keinesfalls auf nicht integren Medien zwischengespeichert, sondern direkt auf sicheren Systemen gespeichert werden. Beispiele für möglicherweise nicht sichere Zwischenspeicherung, sofern diese nicht angemessenen Verfahren zur Sicherstellung der Datenintegrität unterliegen: • Lokale Festplatten

		• temporäre Speicherung • USB-Hard-Drives/-Sticks
6. Prüfung auf Richtigkeit (Accuracy Checks)		
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.		
For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.		
Nr.	**Fragen und Bezug**	**Kommentierung**
6-1	Welche Daten wurden im Rahmen einer Bewertung als kritisch definiert?	Welche Daten als kritisch anzusehen sind, soll im Voraus festgelegt sein. Grundsätzlich sind Daten und die dazugehörigen Metadaten GMP-kritisch, wenn man sie benötigt, um eine GxP-Aktivität nachzuvollziehen oder zu beurteilen. PIC/S PI 041-1 unterscheidet bei der Beurteilung der Kritikalität zwischen dem Risiko für den Prozess und damit der Produktqualität und Patientensicherheit sowie dem Risiko, dass Daten verändert, gelöscht oder verloren gehen.
6-2	Welche Daten werden wann manuell in welche Systeme eingegeben?	Die manuelle Eingabe von Daten ist fehleranfällig. Im Rahmen von Inspektionen sollte darauf geachtet werden, welche Daten wann manuell in welche Systeme eingegeben werden. Als Beispiel seien die Eingabe der Chargennummer oder des Verfallsdatums bei der Verpackung oder auch die Eingabe der Grenzwerte für eine Bandwaage genannt.
6-3	Wie und durch wen erfolgt eine zusätzliche Prüfung?	Die Prüfung kann nach Anhang 11 durch eine zweite bedienende Person oder durch eine validierte elektronische Methode erfolgen. Sofern Daten z. B. von einem Messgerät abgelesen werden, die nicht dauerhaft verfügbar sind, muss die Verifizierung und Erstdokumentation im Rahmen eines gleichzeitigen 4-Augen-Prinzips erfolgen. Werden Daten z. B. von einem dauerhaften Medium (Papierdokument,

		anderes CS) manuell übertragen, kann die Verifizierung in Abhängigkeit vom Prozess auch später erfolgen. Denkbar für elektronische Methoden sind z. B. Prüfziffern bei numerischen 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 die bedienende Person mehrere Werte (z. B. Artikelnummer, Charge, Menge) eingeben muss und das System deren „Zusammengehörigkeit“ mit Werten in der Datenbank vergleichen kann.
6-4	Welche Folgen/Konsequenzen hat eine fehlerhafte Dateneingabe?	Die Auswirkung einer fehlerhaften manuellen Dateneingabe im Besonderen auf die Produktqualität und das Risiko für die Patientinnen/Patienten sollte bewertet sein. Je nach Auswirkung sollten geeignete Kontrollmaßnahmen vorhanden sein. Werden Daten unerkannt verändert, gelöscht oder gehen verloren, ist der Nachweis der GxP-Konformität nicht möglich.
6-5	Welche zusätzlichen Tests, mit denen Fehleingaben erkannt werden können, sind vorhanden?	Mögliche integrierte Kontrollen, um eine Fehlereingabe zu vermeiden, sind z. B.: • automatisierte Plausibilitätsprüfungen gegen Spezifikationsgrenzen und/oder Vergleich mit bereits eingegebenen Werten • vom System geforderte zweifache Eingabe mit Abgleich der eingegebenen Werte • vorgegebene Feldformatierung und Einheiten Je geringer die Entdeckungswahrscheinlichkeit einer Fehleingabe im Folgeprozess ist und je kritischer die Daten für einen Prozess sind, desto umfänglicher müssen die Kontrollmechanismen sein. Bei kritischen Daten ist in jedem Fall eine zusätzliche Prüfung erforderlich.
6-6	Welche Kontrollen zur Prüfung auf Richtigkeit werden bei Excel-Tabellen und/oder vergleichbaren Tabellenkalkulationsprogrammen verwendet?	Excel wird für Berechnungen, Auswertungen oder auch zur Verwaltung von Geräten, Standards etc. genutzt. Excel in seiner Standardfunktionalität erfüllt nicht die Anforderungen zur

		Sicherstellung der Datenintegrität, wie z. B. Audit Trail, ‚logfiles', Schutz vor Veränderungen etc. Ebenso werden zahlreiche Fehler bei der Formatierung der Excel-Sheets beobachtet. 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. Diese Vorlagen sollten so geschützt sein, dass nur in den vorgesehenen Feldern Daten im korrekten Format eingegeben werden können. Formeln sollten geprüft und gesichert sein. Die „Wiederverwendung" von Tabellenblättern, die zuvor schon für Berechnungen verwendet wurden und noch Werte enthalten, ist zu verhindern, da hier die Gefahr besteht, Werte der vorhergehenden Analyse zu berücksichtigen. Solche Vorlagen sind wie z. B. eine Prüfanweisung als gelenktes Dokument zu behandeln, unterliegen also einer Versionierung und dem Änderungsmanagement. Excel-Sheets und vergleichbare Tabellenkalkulationsprogramme sollten ihrer Kritikalität entsprechend validiert werden (→ Kap. 4 Nr. 4-20).

7. Datenspeicherung (Data Storage)

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.*

7.1 *Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.*

7.2 *Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.*

Nr.	Anmerkungen	
7-1	Wichtig ist, zwischen Datensicherung und Archivierung (→ Kapitel 17) zu unterscheiden. Datensicherung erzeugt ein aktuelles Abbild (‚true copy') der auf dem CS vorhandenen Daten. 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 Back-up schneller abläuft. Als Nachteil ergibt sich allerdings, dass bei einer Wiederherstellung der Daten zunächst die letzte vollständige Sicherung und dann nacheinander alle inkrementellen Sicherungen zurückgespielt werden müssen. Stand der Technik ist, dass beide Formen sich ergänzen und in unterschiedlichen Intervallen durchgeführt werden, z. B. täglich eine inkrementelle Sicherung und wöchentlich eine Vollsicherung.	
7-2	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 Datenträger aufbewahrt und von denjenigen am Monatsanfang als Monatssicherung die letzten sechs.	
7-3	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 (‚lock-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. Sie sind jedoch nicht zur Datensicherung geeignet, da Löschungen oder unbeabsichtigte Veränderungen sich stets auch auf die redundant gespeicherten Daten auswirken.	
Nr.	**Fragen**	**Kommentare**
7-4	Welches Verfahren wird zur Datensicherung eingesetzt?	Datensicherungen sind in jedem Fall erforderlich. Die Frequenz der Datensicherung kann sehr unterschiedlich sein. Als Anhaltspunkt für

	Wie oft erfolgt eine Sicherung der Daten? Ist das Verfahren detailliert in einer SOP beschrieben und liegt diese dem Durchführenden – i. d. R. dem Systemeigner – vor?	das Intervall zur Durchführung eines Back-Ups kann man die Häufigkeit nehmen, mit der Daten ergänzt oder verändert werden, z. B.: Ein System zur Aufzeichnung kritischer Herstellungsdaten (MES), welches fortlaufend oder stündlich gesichert wird, gegenüber einem Trainings- oder Dokumentenmanagement-System, welches über Nacht oder wöchentlich gesichert wird.
7-5	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, das jeweils nach einer Woche überschrieben wird. 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 Back-Ups für die vorherigen Monate).
7-6	Wie ist sichergestellt, dass das Back-up vollständig und unverändert ist?	Im Idealfall sollte der Prozess des Back-ups durch eine Monitoring-Software überwacht werden, die beim Auftreten von Fehlern oder bei einem unvollständigen Prozess entsprechende Fehlermeldungen generiert. Ein geeignetes Verfahren zur Sicherstellung von Vollständigkeit und Unveränderlichkeit des Back-Ups ist die Verschlüsselung. Diese Methode kann bei externen, physikalischen Speichermedien (Bänder, DVD, NAS) und der externen Speicherung bei einem Dienstleister (z. B. Cloudspeicherung) eingesetzt werden. Bei der Speicherung durch einen externen Dienstleister sollte der Datentransfer bereits verschlüsselt erfolgen. Den Stand der Technik beschreiben z. B. Technische Richtlinien des BSI (BSI TR-02102, . Kryptographische Verfahren: Empfehlungen und Schlüssellängen)
7-7	Ist die Datenwiederherstellung/Restore aus allen Back-up-Medien und -Systemen validiert?	Das Rückspielen einer Datensicherung sollte für alle Varianten getestet sein. Für einen ‚Restore'-Test sollte die Testumgebung genutzt werden. Das Produktivsystem sollte durch die Durchführung des ‚Restore' nicht gefährdet werden.

		Grundsätzlich ist eine 3-System-Landschaft (Entwicklungsumgebung, Testumgebung, Produktivumgebung) zu empfehlen.
7-8	Wie und wo erfolgt die Aufbewahrung der Sicherungsmedien?	Sicherungsmedien sollten zugriffskontrolliert in einem getrennten Brandabschnitt physisch aufbewahrt werden. Es sollte sichergestellt sein, dass die klimatischen Verhältnisse den Anforderungen der jeweiligen Sicherungsmedien angepasst sind. Hierunter können z. B. die Umgebungstemperatur, Luftfeuchtigkeit, Lichteinfall/-intensität und Staubbildung fallen. Sofern keine feuer- und wasserfesten sowie luftdichten Schränke/Tresore verwendet werden, sollte auf Wasser-, Schaum- und Pulver- oder ähnliche Löschanlagen, die schädlichen Einfluss auf die Sicherungsmedien haben könnten, verzichtet werden. Es können z. B. Gaslöschanlagen Verwendung finden. Weitere Hilfestellung kann der IT-Grundsatz-Baustein ‚INF.6: Datenträgerarchiv' des BSI geben.
7-9	Wie ist sichergestellt, dass Daten, die in Ihrem proprietären Format gespeichert werden, über den gesamten erforderlichen Zeitraum lesbar sind?	Das Problem bei der Speicherung von Daten in ihrem proprietären dynamischen Format ist, dass für die Lesbarkeit und Reprozessierung der Daten die Applikation und/oder das Gerät vorhanden sein muss, mit dem sie erzeugt wurden. Für den Fall, dass sich die Applikation nicht virtualisieren lässt, kann es erforderlich sein, das Gerät in einem betriebsfähigen Zustand zu erhalten. Gem. PIC/S PI 041-1 kann risikobasiert festgelegt werden, ob und wie lange eine Speicherung in dem proprietären Format erforderlich ist.
7-10	Wie ist sichergestellt, dass im Besonderen bei der Archivierung von Daten in einem nichtproprietären Format (z. B. PDF) neben den Daten die vollständigen Metadaten gespeichert werden?	Metadaten sind Daten, die die zum Verständnis der Daten erforderlichen Kontextinformationen liefern. Es sind Daten, die benötigt werden, um die GxP-Aktivität vollständig zu rekonstruieren (Einheit, Zeit- oder Datumsstempel, Bedieneridentifikation (ID), Geräte-ID, Verarbeitungsparameter, Sequenzdateien, Prüfpfade etc.).
7-11	Was ist bei einer Datenspeicherung außerhalb der Betriebsstätte zu beachten?	Verweis auf das Votum V11002 „Anforderungen an die Aufbewahrung elektronischer Daten" der EFG 11.

8. Ausdrucke (Printouts)

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.*

8.1 *It should be possible to obtain clear printed copies of electronically stored data.*

8.2 *For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.*

Nr.	Anmerkungen
8-1	Gemäß Stand von Wissenschaft und Technik ist es schwierig, eine ‚true copy' in Papierform zu erzeugen, die alle Daten und Metadaten enthält. Es ist aus heutiger Sicht auch nicht erforderlich, dass alle Daten und Metadaten vollständig als Papierausdruck vorhanden sein müssen. Sofern ein Papierausdruck erzeugt wird, muss er entweder eine vollständige Kopie der elektronischen Daten sein oder es muss definiert sein, welche Daten ausgedruckt werden und welche nur elektronisch verfügbar sind.

Nr.	Fragen und Bezug	Kommentierung
8-2	Werden elektronische Daten in Form von Papierausdrucken oder statischen Dateiformaten gespeichert oder archiviert?	Bei dieser Vorgehensweise ist es schwierig, die Gesamtheit der Daten und Metadaten zu erfassen. Insbesondere die Metadaten werden häufig nicht vollständig ausgedruckt oder nicht im erzeugten PDF gespeichert (wer, wann, an welchem Gerät, mit welcher Untersuchungsmethode, mit welcher Auswertemethode, wo abgelegt usw.). (→ Abschnitt 7, Nr. 7-10)
8-3	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. Einfache Log-Dateien enthalten keine Informationen zum Änderungsgrund und sind – abhängig von der Konfiguration – nicht vor Veränderungen geschützt. Vor Freigabe einer Charge ist zu überprüfen, ob bei Qualitätsdaten nachträgliche Änderungen oder Löschungen erfolgt sind. 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/kann. Sofern Änderungen am Bildschirm erkennbar sind, kann man bei der Inspektion nach einem Ausdruck fragen und prüfen, ob die Änderungen darin auch erkennbar sind.
8-4	Welche Verfahren sind für die Systeme etabliert, bei denen die Erkennbarkeit nachträglicher Änderungen 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. Für einfache analytische Geräte für unkritische Prozesse (z. B. Dichte, Viskosität im Rahmen einer Inprozesskontrolle) kann es akzeptabel sein, dass diese Funktionalität nicht vorhanden ist.
8-5	Sind dem Herstellungsprotokoll auch Ausdrucke der elektronischen Daten beigefügt und wurden diese bei der Beurteilung des Herstellungsschrittes berücksichtigt?	Zur Dokumentation von Herstellprozessen werden immer noch häufig papierbasierte Formblätter genutzt, in denen zu bestimmten Zeiten (kritische) Prozessparameter erfasst werden. Vielfach werden automatisierte Systeme in der Herstellung eingesetzt, welche kontinuierlich die Prozessparameter aufzeichnen und Alarme und Logdateien zu Änderungen der Maschineneinstellungen dokumentieren. Somit müssten diese elektronischen Daten bei einer ausschließlich papierbasierten Chargendokumentation ausgedruckt und berücksichtigt werden.
9. Audit Trails (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“).		
Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").		

Nr.	Fragen und Bezug	Kommentierung
9-1	Welche Daten sind GMP-relevant?	Die GMP-relevanten Daten sind solche, die den Werdegang einer Charge beschreiben und Informationen liefern zu Prozessen, die direkt oder indirekt die Qualität des Arzneimittels beeinflussen oder einen Einfluss auf das Risiko für die Patientinnen/Patienten haben. Diese Daten und Informationen, egal ob sie kritisch sind für die Produktqualität und/oder kritisch hinsichtlich des Risikos bezogen auf ihre Integrität, sollten im Rahmen eines Daten-Assessments bewertet worden sein.
9-2	Welche Eingabefelder enthalten GMP-relevante 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 den Audit Trail erfasst werden.
9-3	Wie ist sichergestellt, dass Änderungen oder Löschungen GMP-kritischer Daten durch einen Audit Trail nachvollziehbar sind?	Die Anforderungen an den Audit Trail sollten im Lastenheft festgelegt sein. Basierend auf dem Lastenheft ist der Audit Trail zu konfigurieren. Nach der Verifikation der Konfiguration sollte der Audit Trail nicht gelöscht werden können und mit den Daten, die geändert oder gelöscht werden, verbunden sein. Eine Löschung ist nur nach Ablauf der Archivierungsfrist zulässig.
9-4	Wie ist die Verfügbarkeit der Audit Trails sichergestellt?	Bei der Einführung eines Prozesses ist zu definieren, welche Änderungen und Löschungen über einen Audit Trail nachvollziehbar sein müssen. Diese Audit Trails sind entsprechend zu konfigurieren, so dass sie unmittelbar verfügbar und lesbar sind. Verfahren, die auf einer individuellen Datenbankabfrage beruhen oder ggf. auch nur anlassbezogen generiert werden, sind nicht akzeptabel.
9-5	Wie wird der Audit Trail Review durchgeführt?	Der Audit Trail Review sollte in einer SOP geregelt sein. Der Prozess kann durch ein Formblatt unterstützt werden. Die SOP sollte festlegen, wie z. B. die Funktionalität als solche nach der Erstvalidierung geprüft wird (Revalidierung, periodische Bewertung). Ebenso ist festzulegen:

		• welche Audit Trails im Rahmen der Freigabe einer Charge geprüft werden sollen. • in welchen Frequenzen die systemischen Audit Trails (Änderungen von Geräteeinstellungen) geprüft werden.
9-6	Wurde der Audit Trail entsprechend den Anforderungen zur Sicherstellung der Datenintegrität konfiguriert?	Bei komplexen CS (CDS, LIMS, MES) sind im Rahmen der Konfiguration (Klasse 4 Software) zahlreiche Konfigurationsitems zur Beschreibung dieser Funktionalität vorhanden. Im regulierten Umfeld besteht die Erwartung einer gehärteten Konfiguration, d. h. die maximal mögliche Einstellung zur Erfassung und die restriktivste Konfiguration in Bezug auf Änderungen dieser Einstellungen.
Bei der Änderung oder Löschung GMP-relevanter Daten sollte der Grund dokumentiert werden.		
For change or deletion of GMP-relevant data the reason should be documented.		
Nr.	**Anmerkungen**	
9-7	Diese Anforderung soll sicherstellen, dass das Ändern und/oder Löschen von Daten nachvollziehbar wird.	
Nr.	**Fragen und Bezug**	**Kommentierung**
9-8	Wer darf Daten ändern oder löschen? Darf der Systemadministrator Daten ändern?	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. Nur in einem kontrollierten, dokumentierten und autorisierten Prozess dürfen erforderlichenfalls Daten geändert werden. Die Änderung muss über ein Audit Trail nachvollziehbar sein. Auch auf Infrastruktur-Ebene sollte jegliche Änderung kontrolliert erfolgen.
9-9	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.		

Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

Nr.	Fragen und Bezug	Kommentierung
9-10	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
9-11	Wie oft erfolgt die regelmäßige Überprüfung des Audit Trails?	Die Funktionalität ist regelmäßig im Rahmen der periodischen Evaluierung zu bewerten und ggf. zu prüfen. Das Intervall sollte nachvollziehbar unter Berücksichtigung des Prozessrisikos festgelegt werden. Vor der Chargenfreigabe sollten Änderungen oder Löschungen kritischer Daten bewertet werden. Verfahrensparameteränderungen, die im Rahmen eines Change-Control-Verfahrens durchgeführt wurden, sind in diesem Zusammenhang nicht zu betrachten.
9-12	Welche Auswahlkriterien liegen dem Audit Trail Review zugrunde?	Bei der üblichen Datenabfrage zu Audit Trails werden nicht nur Audit Trails im Sinne der engen Definition des Anhang 11, sondern häufig auch Log-Dateien und automatische Systemänderungen ausgegeben. Daher ist es erforderlich, diese Daten anhand vorher definierter Auswahlkriterien filtern zu können, um einen zielgerichteten Review zu ermöglichen.
9-13	Was wird unter ‚allgemein lesbarer Form‘ verstanden?	‚Lesbare Form‘ bedeutet eine Aufzeichnung (Papierdokument, elektronische Aufzeichnung o. ä.), die die folgenden Mindestangaben enthält: • alter Wert • neuer Wert • Änderungszeitpunkt • durchführende Person • Änderungsgrund

9-14	Welche Maßnahmen sind bei „Altsystemen“ ohne Audit Trail-Funktionalität zu treffen, um Änderungen und Löschungen zu kontrollieren?	Altsysteme liegen nur vor, wenn sie vor Inkrafttreten des Anhangs 11 (1992) installiert waren. Zuerst ist zu klären, ob Daten überhaupt änderbar sind (z. B. elektronische Schreiber). Wenn nicht, ist kein Audit Trail erforderlich. Bei Systemen ohne Audit Trail-Funktionalität kann z. B. durch eine SOP geregelt werden, dass jede Änderung in einem Logbuch dokumentiert und von einer zweiten Person verifiziert wird.

10. Änderungs- und Konfigurationsmanagement (Change and Configuration Management)

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

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

Nr.	Fragen und Bezug	Kommentierung
10-1	Was sind Änderungen an computergestützten Systemen, die in Zusammenhang mit Anhang 11 Nr. 10 betrachtet werden sollten?	Änderung an der Applikation: • Software-Update z. B. aufgrund einer Abweichung/eines Fehlers oder „reguläres“ Update von Seiten des Anbieters • Konfigurationsänderungen: z. B. der Zugriffsberechtigungen • Änderungen an Prozessparametern, die elektronisch hinterlegt sind. Änderung der zugrundeliegenden Infrastruktur: • Änderungen können auch die der Applikation zu Grunde liegende Infrastruktur betreffen, z. B. Patch des Betriebssystems, Datenbankänderungen, Änderungen der Netzwerkprotokolle, Änderungen der Bereitstellung etc.
10-2	Welche Konsequenzen haben die unterschiedlichen Änderungen?	Änderung an der Applikation: • Prüfung des Einflusses auf den validierten Status und der Notwendigkeit zusätzlicher Validierungsaktivitäten und/oder Regressionstestungen Änderung von Prozessparametern: • Wurde die Änderung der Prozessparameter bewertet? Wurde der Prozess ggf. revalidiert?

		Wurde die Änderung im Rahmen des Konfigurationsmanagements/Rezeptverwaltung erfasst und dokumentiert? • Der Umfang der Änderungskontrolle ist abhängig vom CS und dessen Konfiguration und Auswertung im Rahmen der Herstellung/Prüfung. Änderung der zugrundeliegenden Infrastruktur: • Bewertung der release note und ggf. Regressionstestung
10-3	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 sollten Einfluss auf die Festlegung der notwendigen Schritte haben. Reparaturen durch Austausch gleichartiger Komponenten können als vorab generell genehmigte Änderungen beschrieben sein.
10-4	Ab wann werden Änderungen kontrolliert, erfasst und umgesetzt?	Änderungen sollten sowohl während der Entwicklung, als auch im laufenden Betrieb erfasst und bewertet werden. In der Entwicklung führt eine Änderung meist zu einer Änderung der Benutzeranforderung (‚user requirement specification') und/oder der Funktionsspezifikation. Im laufenden Betrieb kann eine Änderung ebenfalls zu einer nachträglichen Änderung der Benutzeranforderung/Funktionsspezifikation oder auch der Risikoanalyse führen. Diese Doku-

		mente müssen daher entsprechend weitergeführt/ergänzt werden. Außerdem ist die Auswirkung auf den validierten Status zu prüfen. Der Übergang von der Entwicklungsphase in den laufenden Betrieb sollte klar abgegrenzt sein. Es bietet sich ggf. an, zwei verschiedene Verfahrensweisen zu etablieren. Verschiedene Versionen der Software sollten nachvollzogen werden können.
10-5	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.
10-6	Wie werden externe Dienstleister mit einbezogen?	Der Softwareanbieter sollte ebenfalls über ein Änderungskontrollsystem verfügen. Die Interaktion zwischen den Änderungskontrollsystemen des Softwareanbieters und des Anwenders sollte vertraglich beschrieben sein. Der Anwender muss über etwaige Änderungen am computerisierten System vorab informiert werden (z. B. Software-Update). Die Änderung sollte erst vorgenommen werden, wenn der Anwender diese autorisiert hat.

11. Periodische Evaluierung (Periodic evaluation)

Computergestützte Systeme sollten periodisch evaluiert werden, um zu bestätigen, dass sie sich noch im validen Zustand befinden und die GMP-Anforderungen erfüllen.

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.

Nr.	Fragen und Bezug	Kommentierung
11-1	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 und risikobasiert begründet werden.

		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.		
Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.		
Nr.	**Fragen und Bezug**	**Kommentierung**
11-2	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 (QS, IT, Fachabteilung usw.).
11-3	Ist die Evaluierung an einen Dienstleister delegiert?	Die Aufgabe/Arbeit selbst kann delegiert werden, die Verantwortung dafür aber nicht. Mögliche Verantwortlichkeiten: QS oder der Systemeigner Produktion/Qualitätskontrolle oder eine Validierungseinheit – verantwortlich ist letztendlich das pharmazeutische Unternehmen bzw. dessen sachkundige Person.
12. Sicherheit (Security)		
Nr.	**Anmerkungen**	
12-1	GxP-relevante Systeme werden zunehmend auch über die Grenzen firmeninterner Netzwerke hinaus vernetzt (Remote-Zugriffe für Wartung, Cloud, IOT, Pharma 4.0). Daraus resultiert eine komplexere Bedrohungslage. Die letzten Jahre haben gezeigt, dass Hackerangriffe (in vielen Fällen Ransomware) dazu geführt haben, dass pharmazeutische Firmen temporär nicht produzieren und ausliefern konnten. Der Gesetzgeber hat mit der BSI-KritisV Anforderungen für die Betreiber kritischer Infrastruktur festgelegt. Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes sind gemäß BSIG und BSI-KritisV verpflichtet, IT-Sicherheit auf dem ‚Stand der Technik' umzusetzen. Diejenigen Unternehmen, die Schwellenwerte überschreiten, müssen ein zertifiziertes ISMS gem. EN ISO 27001 installieren. Der Anhang 11 fokussiert sich in seinen Anforderungen sehr stark auf den Zugang zu GxP-relevanten Systemen. PI041-1 beschreibt einen weiterreichenden Ansatz, um Daten in Transfer und in Ruhe (data in motion, data at rest) zu schützen.	

	Nr. 12.2. des Anhangs 11 führt mit der Aussage, dass der Umfang der Sicherheitsmaßnahmen von der Kritikalität des CS abhängig ist, eine grundsätzliche Maxime auf, die regulierte Firmen beachten sollen.
12-2	Um ein angemessenes Sicherheitsniveau zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der CS, der Daten und der Prozesse zu erreichen, sollte das Unternehmen ein Informationssicherheitsmanagementsystem installiert haben.
12-3	Die Sicherheitsmaßnahmen dienen dem Schutz der CS und Daten vor absichtlichen und unbeabsichtigten Verlust, Beschädigung und unberechtigten Änderungen.
12-4	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, wobei individuell erkennbar sein muss, wer eine Aktivität durchführt.
12-5	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.

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.

Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

Nr.	Fragen und Bezug	Kommentierung
12-6	Wie wurde das Personal bezüglich Sicherheit und Datenintegrität geschult?	Die Schulungen sollten auch Bedeutung und Zweck der Sicherheitsmaßnahmen umfassen und damit das Personal (Anwender und Administratoren) für die Informationssicherheit sensibilisieren.

12-7	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). Zu den physischen Maßnahmen gehören der Schutz der lokalen Hardware und der Server vor physischer Beschädigung, unbefugtem physischen Zugriff und Nichtverfügbarkeit. Der physische Zugang zur Hardware soll auf autorisiertes Personal beschränkt sein und die Datensicherung auf zwei örtlich unabhängigen Servern erfolgen. Logische Zugriffskontrollen umfassen u. a. die Vergabe der Zugriffsberechtigungen und die Auswahl einer sicheren Methode der Benutzeridentifizierung.
12-8	Welche Regelungen gibt es zur Festlegung der Zugriffsrechte?	Die Vergabe von Zugriffsrechten sollte in einer SOP geregelt sein. Die Zugriffsrechte sind entsprechend den Aufgaben und Verantwortlichkeiten festzulegen. Hierbei ist der Grundsatz ‚need to know, need to have' zu berücksichtigen, indem Systemnutzer nur die Rechte im System erhalten, die sie zur Arbeitsbewältigung benötigen. Bei der Verteilung der Rechte in einem Netzwerk bzw. bei Unterschriften sind in der Regel verschiedene Rollen zu unterscheiden. Bei der Verteilung der Rollen ist ein weiterer Grundsatz zu beachten, die ‚segregation of duties'. Hierzu ist idealerweise ein mindestens dreistufiges Modell etabliert, welches den ‚normalen Nutzer', den ‚super user' – also der Person, die auch Rezepte und Methoden erstellen und ändern kann – und dem Systemadministrator zu unterscheiden.
12-9	Werden Gruppenaccounts genutzt?	Aufgrund mangelnder technischer Möglichkeiten oder zum Teil auch beabsichtigt, sind Gruppenaccounts eingerichtet. Diese ermöglichen einer Mehrzahl von Nutzern (all denjenigen, die Kenntnis der Accountdaten haben) Zugriff, ohne das erkennbar ist, wer die Aktivität durchgeführt hat. Dieses ist nicht zulässig. Als Übergangsmaßnahme kann ein Log-Buch die fehlenden Informationen liefern.

12-10	Wer vergibt den jeweiligen Status der Zugriffsrechte und wie ist das Prozedere?	Die Vergabe, Änderung und der Entzug von Zugriffsrechten sollten auf GxP-Applikationsebene durch den Prozesseigner und in Verantwortung des LH bzw. LQ verwaltet werden. Ausführer sind dann die Systemeigner. Die Rollen und Befugnisse von Administratoren sollten klar definiert sein. Die Administratoren sollten zur Wahrnehmung ihrer Aufgaben entsprechend geschult sein. Der Administrator nimmt die Zuordnung zu den Rechten technisch vor. LH, LQ oder Geschäftsführung sind für die fachliche Zuordnung verantwortlich.
12-11	Wer hat Systemadministratorzugriff auf das System und die Daten?	Systemadministratoren sollten unabhängig von den Systemanwendern sein. Dies betrifft v. a. die Aufgaben Sicherheitseinstellungen (wie Konfigurationseinstellungen), Back-Up, Archivierung.
12-12	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.
12-13	Wer darf (wann) welche Daten eingeben oder ändern?	Die Erlaubnis sollte auf namentlich festgelegte Personen beschränkt sein. 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 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.
12-14	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) eingehalten werden.
12-15	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. Die Validierung von biometrischen Systemen sollte kritisch hinterfragt werden. Eine Remote-Identifizierung, z. B. zu Cloud-basierten Systemen, sollte als zwei-Faktor-Authentifizierung erfolgen, d. h. eine Kombination aus zwei der drei o. a. Faktoren a), b) und c). 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.
12-16	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 min-

		destens acht Zeichen lang sein, nicht in Wörterbüchern vorkommen, nicht aus Geburtstagen bzw. Namen bestehen und Groß- und Kleinbuchstaben, Sonderzeichen sowie Ziffern enthalten.
12.2 *Der Umfang der Sicherheitsmaßnahmen ist von der Kritikalität des computergestützten Systems abhängig.*		
12.2 *The extent of security controls depends on the criticality of the computerised system.*		
Nr.	**Anmerkungen**	
12-17	Die Auswahl der Maßnahmen richtet sich nach der Kritikalität des Systems und der Daten. Dabei ist auch das Ausmaß der Vernetzung des Systems zu berücksichtigen.	
Nr.	**Fragen und Bezug**	**Kommentierung**
12-18	Welche Maßnahmen sind zum Schutz vor äußeren Einflüssen, z. B. Viren, vorhanden?	Werden Daten aus externen Netzwerken oder von Datenträgern heruntergeladen und geöffnet, ist der Einsatz von aktuellen IT-Security-Schutzmaßnahmen (z. B. Malware-Schutz-Software, Antiviren-Software, Web-Schutz-Software, Firewall-Konfiguration, Patch-Management und Installation eines ‚Intrusion Detection System' (IDS) zu Erkennung von Angriffen) zwingend notwendig. Diese IT-Security-Schutzmaßnahmen sollten regelmäßig aktualisiert und auf ihre Wirksamkeit hin überprüft werden. Bei erkannten Sicherheitslücken sollten Korrekturmaßnahmen ergriffen werden. Ebenso wichtig ist die zeitnahe Installation von Sicherheits-Updates für die betreffende Software, um Sicherheitslücken bzw. Schwachstellen in der Software zu schließen. Die Etablierung angemessener IT-Sicherheitsmaßnahmen kann vom regulierten Nutzer durch Zertifizierung gemäß eines anerkannten Qualitätssicherungssystems (IT-Grundschutz, DIN EN ISO 27000er-Reihe oder Pharmastandard BS3) nachgewiesen werden.

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

12.3 *Creation, change, and cancellation of access authorisations should be recorded.*

Nr.	Fragen und Bezug	Kommentierung
12-19	Welches Verfahren besteht für die Ausgabe, Annullierung und Veränderung der Zugriffberechtigungen?	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 einer/eines Mitarbeitenden sollte die (alte) Zugriffsberechtigung deaktiviert werden. Es sollte geprüft werden, ob die Berechtigungen im System mit den Aufgaben der/des Mitarbeitenden übereinstimmen. Es sollte ein Register über autorisierte Personen gepflegt werden, welches bei der Inspektion überprüft werden kann.

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.*

12.4 *Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.*

Nr.	Fragen und Bezug	Kommentierung
12-20	Wie ist das Verfahren zur Eingabe und Änderung von Daten beschrieben? Gibt es zu jeder GxP-Aktivität einen Logfile, der dokumentiert, wann wer welche Aktion ausgeführt hat?	Hier kann durch das Inspektionsteam u. a. überprüft werden, ob tatsächlich nur befugte Personen Eingaben und Änderungen vornehmen können und ob diese mit Datum und Uhrzeit aufgezeichnet werden.

13. Vorfallmanagement (Incident Management)

Alle Vorfälle, nicht nur Systemausfälle und Datenfehler, sollten berichtet und bewertet werden.

All incidents, not only system failures and data errors, should be reported and assessed.

Nr.	Fragen und Bezug	Kommentierung
13-1	Wie sind Vorfälle definiert?	Ein Unternehmen kann definieren, was ein Vorfall und was bestimmungsgemäßer Gebrauch ist. Das Zurücksetzen eines Passwortes kann z. B. regelmäßige Aufgabe der Administration

		und daher kein Vorfall sein, da auch das System dies über Logfiles dokumentiert. Vorfälle können z. B. technisches Versagen, Fehlfunktion, mangelnde Performance, Angriff Dritter, Ausfall externer Dienste oder menschliches Versagen sein.
13-2	Hat ein Vorfall Auswirkungen auf GMP-relevante Prozesse?	Viele IT-Vorfälle werden nur aus IT-Sicht betrachtet. Es sollte jedoch auch immer geprüft werden, ob der Vorfall Auswirkungen auf GMP-relevante Prozesse haben kann. Prozess- und Systemeigner sollten daher bei der Beurteilung des Vorfalls zusammenwirken. Wenn ein Server kurzzeitig ausfällt, dann aber wieder hochgefahren werden kann, sollte geprüft werden, ob die GMP-relevanten Daten vollständig zur Verfügung stehen und gespeichert wurden. Das Personal, welches mit dem Vorfallmanagement betraut ist, sollte auch im Abweichungsmanagement von GMP-Prozessen geschult sein.
Die Ursache eines kritischen Vorfalls sollte ermittelt werden und die Basis für Korrektur- und Vorbeugemaßnahmen sein.		
The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.		
Nr.	**Fragen und Bezug**	**Kommentierung**
13-3	Wie werden Vorfälle erfasst und ausgewertet?	Vorfälle sollten systematisch erfasst und hinsichtlich Häufung und Schwere bewertet werden. Vorfälle werden durch die eigene IT oder – wenn sie im Zusammenhang mit Software stehen – von externen Dienstleistern/Softwareherstellern erfasst und bearbeitet. Häufig erfolgt die Meldung über ein Softwaretool oder einen Helpdesk. Analog der Bearbeitung von Abweichungen wird die systematische Erfassung durch eine Datenbank und durch in Verfahrensanweisungen definierten Workflows erleichtert. Sofern Vorfälle extern durch den Softwarehersteller erfasst werden (Helpdesk), ist der Informationsaustausch im Dienstleistungsvertrag (‚service level agreement') zu regeln.
13-4	Wie werden Vorfälle klassifiziert?	Es sollte zumindest eine Definition von kritischen und nicht kritischen Vorfällen vorliegen. Die Ursache sollte dokumentiert, Korrektur- und

		Vorbeugemaßnahmen sollten festgelegt sein. In Abhängigkeit der Einstufung können unterschiedlich detaillierte Abläufe zur Bearbeitung von Vorfällen vorliegen. Um die Bearbeitung von Vorfällen zu steuern/priorisieren und den Aufwand/Workflow dem Risiko des Vorfalls für die Produktqualität anzupassen, sind Vorfälle hinsichtlich ihrer Kritikalität einzustufen.
13-5	Wer ist am Vorfallmanagement beteiligt?	In einer Verfahrensanweisung sollte festgelegt werden, wer wie Vorfälle erfasst und bearbeitet. Der Erfassung, der Bewertung, dem Festlegen von Maßnahmen, dem Abschluss und dem Follow-up sollten Rollen und Funktionalitäten zugeordnet sein. In Abhängigkeit der Kritikalität müssen der Prozesseigner und ggf. die sachkundige Person/QS eingebunden werden.
13-6	Wie erfolgt der Nachweis der Erfolgskontrolle der Vorfallbehebung?	Die Eignung der korrektiven Maßnahmen ist zu prüfen. Hierzu sind Verantwortlichkeiten und Termine festzulegen. In Abhängigkeit von der Kritikalität und von der Tiefe des Eingriffs in das jeweilige System können Revalidierungen und Requalifizierungen erforderlich sein, z. B. nach Softwareänderungen aufgrund von Fehlern.

14. Elektronische Unterschrift (Electronic Signature)

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.

Electronic records may be signed electronically. Electronic signatures are expected to:

a. have the same impact as hand-written signatures within the boundaries of the company,

b. be permanently linked to their respective record,

c. include the time and date that they were applied.

Nr.	Anmerkungen
14-1	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.	
14-2	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.	
Nr.	**Fragen und Bezug**	**Kommentierung**
14-3	Welche Dokumente werden elektronisch unterschrieben?	Hier kann ein Überblick gewonnen werden, auch im Hinblick auf die Kritikalität der elektronischen Unterschriften.
14-4	Welche Arten von elektronischen Unterschriften finden Verwendung?	Die Art der elektronischen Unterschrift ist nicht vorgegeben (s. o.). Im Falle der elektronischen Unterschrift unter Herstellungsprotokoll, Prüfprotokoll oder zur Dokumentation der Freigabeentscheidung wird die Verwendung einer fortgeschrittenen elektronischen Signatur nach Artikel 26 der Verordnung (EU) 910/2014 empfohlen (vgl. auch Votum V11003). Sofern andere Verfahren eingesetzt werden, sollte im Rahmen der Validierung belegt werden, dass Authentizität und Unabstreitbarkeit der Signatur sowie Integrität der Daten gewährleistet sind. Zusätzlich zu der Anmeldung am System sollte die erneute Eingabe eines Passworts für die Unterschrift notwendig sein, um in geeigneter Weise sicherzustellen, dass elektronische Unterschriften eindeutig einer Person zugeordnet werden können. Durch einfache Funktionstasten oder Befehle generierte Namenswiedergaben stellen keine elektronische Signatur dar.
14-5	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 der nutzenden Person, die die Dokumente geprüft, bearbeitet, genehmigt oder freigegeben hat, aufzeichnen.

14-6	Haben die Personen, die elektronische Unterschriften leisten, schriftlich ihr Einverständnis erklärt, dass diese im Innenverhältnis rechtverbindlich äquivalent zu einer handgeschriebenen Unterschrift ist?	Die qualifizierte elektronische Unterschrift im Sinne der VO (EU) Nr. 910/2014 ersetzt die handgeschriebene Unterschrift. Diese Möglichkeit wird von der Pharmaindustrie bisher kaum angewandt. Für die einfache und fortgeschrittene Unterschrift im Sinne der Verordnung muss eine Erklärung vorliegen, um die Authentizität der Unterschrift unabstreitbar zu machen. Hintergrund ist, dass der Anhang 11 nur auf das Innenverhältnis abzielt und keine bestimmte Art der elektronischen Signatur vorgibt. Dies ist möglich, da die VO (EU) Nr. 910/2014 bzw. das eIDAS-Durchführungsgesetz im Innenverhältnis eines regulierten Nutzers nicht einschlägig ist, weil weder die RL 2001/83, noch die RL 2017/1572 sowie weder das AMG noch die AMWHV auf diese Vorgaben referenzieren. Da es aber bei einfachen oder fortgeschrittenen Unterschriften dazu kommen könnte, dass die unterzeichnende Person die Authentizität einer geleisteten Unterschrift abstreitet, sollte von den Nutzenden eine entsprechende Erklärung zur Zustimmung zur Nutzung und zur Unabstreitbarkeit der Echtheit der Unterschrift vorliegen. Dies schützt einerseits die Firma, gibt andererseits aber den Nutzenden elektronischer Unterschriften die Möglichkeit, auf ein angemessenes Sicherheitslevel vor Leistung der Erklärung hinzuwirken (vgl. hierzu auch Votum V11003).
14-7	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 die Unterschrift bei einer Änderung ungültig wird.
14-8	Wie wird die Identität der bedienenden Person überprüft?	In der Regel wird die Identität durch Benutzerkennung und Passwort sichergestellt. Dies erfordert entsprechende Zugriffskonzepte (vgl. Ziffer 3.4.8 bzw. 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.
14-9	Wie wurde das Verfahren der elektronischen Unterschrift inkl.	Hier gelten die gleichen Bedingungen wie bei der Validierung anderer Systeme.

	der unlöschbaren Verknüpfung mit dem unterschriebenen Dokument validiert?	
14-10	Wie ist sichergestellt, dass bei Datentransfer über Schnittstellen die Authentizität und Unabstreitbarkeit der Signatur erhalten bleibt?	Dieses sollte über die Konfiguration der Schnittstelle im Zusammenhang mit entsprechenden Testfällen im Rahmen der Validierung gewährleistet werden.
14-11	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. Es ist auch akzeptabel, wenn Daten nicht archiviert, sondern ausschließlich (in der Applikation) gesichert werden. Sofern sie archiviert werden, muss sichergestellt werden, dass die Daten (Dokumente) mit der Unterschrift vollständig migriert werden und auch nach einer Formatänderung alle Informationen (Daten und Metadaten) langfristig unverändert abrufbar bleiben.

15. Chargenfreigabe (Batch release)

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.

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

Nr.	Anmerkungen
15-1	Wenn die Zertifizierung der Chargenfreigabe elektronisch erfolgt, fordert Anhang 11 (als einzige Stelle) auch eine elektronische Unterschrift.
15-2	Die Zertifizierung der Chargenfreigabe ist inhaltlich zu unterscheiden von Folgeaktivitäten, wie z. B. die Durchführung von Statusänderungen der zertifizierten Arzneimittelcharge.
15-3	Im Kapitel „Allgemeine Grundsätze“ des Anhang 16 ist beschrieben, welche drei Schritte die Chargenfreigabe umfasst. Dabei ist die Zertifizierung der Chargenfreigabe als deren zweiter Schritt definiert: „ii. Die Zertifizierung der Fertigprodukt-

	charge durch eine sachkundige Person, die bestätigt, dass die Charge den Anforderungen der Guten Herstellungspraxis und der entsprechenden Genehmigung für das Inverkehrbringen entspricht. Hierbei handelt es sich um die Qualitätsfreigabe der Charge.“	
Nr.	**Fragen und Bezug**	**Kommentierung**
15-4	Gibt es zur (elektronischen) Chargenfreigabe klare Regelungen innerhalb des QMS?	Analog zur Regelung der Chargenfreigabe in Papierform müssen auch Regelungen für die elektronische Variante vorliegen. Diese Regelungen beinhalten detaillierte Verfahrensvorgaben zu dem Prozess der Chargenfreigabe und den technischen Voraussetzungen. Über das Rollenkonzept muss sichergestellt sein, dass nur gemeldete und von der Firma hierzu bestimmte sachkundige Personen in den dazu vorgesehenen Systemen die Freigabe und Zertifizierung durchführen können.
15-5	Wird durch die elektronische Unterschrift ein Workflow ausgelöst (z. B. Überführung in den verkaufsfähigen Bestand)?	Der Workflow und entsprechende Transaktionen müssen beschrieben und verifiziert/getestet sein.
15-6	Werden automatisierte Datenzusammenfassungen im Rahmen des Freigabeverfahrens verwendet?	Sofern individuelle Datenzusammenfassungen erzeugt werden, sind derartige Systeme vollständig zu validieren. Viele Produktionsanlagen (z. B. Tablettenpressen, Sterilisationstunnel) können Datenzusammenfassungen liefern. Wenn diese für das Freigabeverfahren genutzt werden, muss der Aggregationsprozess auch hierfür qualifiziert werden. Eine besondere Form der automatisierten Datenzusammenfassung ist die elektronische Chargenprüfung als ‚Review by exception‘.
15-7	Hat die sachkundige Person vor der Freigabeentscheidung Zugriff auf alle relevanten Daten?	Die Anforderungen des Kapitels 4 (englische Version) und Anhang 16 des EU-GMP-Leitfadens an die Freigabe sind auch im Falle elektronischer Systeme zu erfüllen.
16. Kontinuität des Geschäftsbetriebes (Business Continuity)		
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 erforderli-		

che 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.

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative sys-tem). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

Nr.	Anmerkungen
16-1	Kritische Prozesse sind zu identifizieren und aufzulisten.
16-2	Mögliche Ausfallszenarien (→ Abhilfemöglichkeiten in Klammern angegeben) sind z. B.: • Ausfall von Komponenten, z. B. Drucker oder Waage (Bereithalten von Ersatzgeräten) • Ausfall des Gesamtsystems oder von Teilen desselben durch Naturkatastrophen, z. B. Stromausfall, Überflutung (→ Notstromaggregat) • Systemabsturz (→ lokale Datenpuffer) • Hackerattacken, Eindringen von Viren oder Schadsoftware (→Erarbeitung und Umsetzung eines IT-Sicherheitskonzepts, regelmäßige Datensicherung) • Ausfall des Dienstleisters (→ alternativer Dienstleister)
16-3	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.

Nr.	Fragen	Kommentierung
16-4	Gibt es einen regelmäßig aktualisierten 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 alternativ aufgezeichneter Daten und ggf. das Nachpflegen dieser Daten in das CS

		• 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.
16-5	Gibt es ein Meldeverfahren und was beinhaltet es?	Ein Meldeverfahren sollte implementiert sein. Dieses beinhaltet: • 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 • Meldeverpflichtung der verfügbaren Bestände von gelisteten Arzneimitteln nach § 52 b Abs. 3f AMG • KRITIS Meldeverpflichtung an das BSI
16-6	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.
16-7	Wurde die Auswirkungen des Zwischenfalls auf die Vollständigkeit und Integrität der Daten untersucht?	Der Zeitpunkt des letzten verwendbaren Back-Ups sollte bestimmt werden können. Sofern Zwischenfälle von Spezialisten forensisch untersucht wurden, lassen sich aus den Erkenntnissen gegebenenfalls der Zeitpunkt sowie die betroffenen Daten und Systeme ermitteln, die den Anforderungen an die Vollständigkeit und Integrität der Daten nicht mehr entsprechen. Im Umkehrschluss erlaubt die Untersuchung auch festzustellen, welche Daten-

		sätze/Back-Ups unverändert nutzbar sind und welche Systemkonfiguration zur Wiederherstellung verwendet werden kann.
16-8	Welchen Einfluss haben Datenverluste auf die laufende Produktion und die im Markt befindlichen Chargen?	Liegt ein Datenverlust vor muss geprüft werden, • welche Daten verloren gegangen sind, • welche Daten wiedererzeugt werden können (Analysendaten), • welche Auswirkung die fehlenden Daten für die Beurteilung der Produktqualität haben, • was der Verlust der Daten für die Sicherheit und Versorgung der Patientinnen/Patienten bedeutet.
16-9	Wie erfolgt der Umgang mit Daten, die nach Systemausfall oder anderen Fehlern wiedergewonnen werden konnten?	Die Daten sollten auf Richtigkeit, Integrität und Vollständigkeit überprüft sowie mögliche Fehler identifiziert werden.
16-10	Sofern externe Dienstleister betroffen sind, sind die Informationswege im SLA festgelegt? Wurde das Desastermanagement des Dienstleisters im Rahmen der Qualifizierung bewertet?	Das SLA sollte eindeutig festlegen, wer über Zwischenfälle und korrektive Maßnahmen im Rahmen des Desastermanagements informiert wird. Im Rahmen der Lieferantenqualifizierung sollte die Geeignetheit des Desastermanagements bewertet werden, ggf. sollte ein zweiter Dienstleister oder eine ‚on-premise'-Lösung als Alternative zur Verfügung stehen.

17. Archivierung (Archiving)

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.

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Nr.	Anmerkungen
17-1	Bei diesem Kapitel geht es um die Archivierung elektronischer Daten. Die Archivierung ist unabhängig von der Datensicherungsstrategie zu betrachten. Grundsätzlich ist die Archivierung die Langzeitspeicherung von Daten in einem nicht-proprietären Format durchzuführen. Nichtsdestotrotz ist es auch Usus, dass

	die Langzeitverfügbarkeit durch Back-Up-Systeme sichergestellt wird. Dies ist unabhängig von der Archivierung zu betrachten. Vorteil der Archivierung ist die Verfügbarkeit der Daten unabhängig von der Applikation und ggf. der zugehörigen Hardware (z. B. Laborgerät). Nachteil ist der Verlust der Möglichkeit, Daten zu reprozessieren. Ein weiterer Vorteil ist die Entlastung des Produktivsystems. Die Daten stehen somit im Produktivsystem nicht mehr direkt zur Verfügung. Vorteil der Sicherstellung der Langzeitverfügbarkeit durch Back-Up-Systeme ist die Möglichkeit der Reprozessierung der Daten über den gesamten Zeitraum. Nachteil ist, dass Daten während der Langzeitspeicherung ggf. mehrfach migriert werden müssen. Darüber hinaus besteht die Möglichkeit, auch Papierdokumente elektronisch zu archivieren. Voraussetzung hierfür ist ein validierter Scan-Prozess und die Unveränderbarkeit des Scans durch ‚Integritätssicherung' gemäß BSI. Zum ersetzenden Scannen hat das BSI Mindeststandards beschrieben (BSI Technische Richtlinie 03138). Gemäß AMG und AMWHV besteht die Möglichkeit, Papierdokumente durch elektronische Aufzeichnungen zu ersetzen. Ob andere Rechtsnormen (z. B. Gültigkeit geleisteter Unterschriften auf Papier) betroffen sind, wird an dieser Stelle nicht bewertet.	
Nr.	**Fragen und Bezug**	**Kommentierung**
17-2	Werden Daten archiviert, wenn ja wo und wie?	siehe Nr. 17-1
17-3	Welche Tests werden durchgeführt, um die Verfügbarkeit der Daten sicherzustellen?	Datenträger sind nur begrenzt haltbar, so z. B. DVDs, CDs, Flash-Drives, Hard-Drives. Leider gibt es keine verbindlichen Daten über die Haltbarkeit elektronischer Datenträger. Das Unternehmen sollte allerdings intern eine Festlegung getroffen haben, nach welcher Zeit die Lesbarkeit archivierter Daten geprüft werden soll. Insbesondere bei Aufbewahrungszeiträumen, die das übliche Maß von sechs Jahren überschreiten (Zulassungsdokumentation, klinische Prüfung, Blut, Validierungschargen usw.) ist damit zu rechnen, dass die Daten archiviert 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.

17-4	Werden geeignete Datenträger verwendet und 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.
17-5	Wie wird die Datenintegrität archivierter Daten sichergestellt?	Es muss vorzugsweise technisch sichergestellt sein, dass archivierte Daten nicht mehr verändert werden können. Dieses kann durch die Verschlüsselung der Daten erreicht werden. Sofern dieses technisch nicht sichergestellt ist, muss zusätzlich zur Plausibilitätskontrolle (z. B. die Anzahl der Datensätze) in definierten Abständen eine Stichprobe geprüft werden (DIN/ISO 2859, Teil 1). Sofern im Rahmen der Archivierung das Medium gewechselt wird, sind zusätzliche Maßnahmen (z. B. Qualifizierung, Migration) erforderlich.
17-6	Welche Anforderungen gelten für die elektronische Archivierung von Papierdokumenten?	Sollen papierbasierte Dokumente einem Scan-Prozess unterzogen und als elektronische Dateien archiviert werden, so sind die entsprechenden Geräte zu qualifizieren und die Prozesse zu validieren. Es sollte eine periodische Überprüfung des Scan-Prozesses stattfinden. Es müssen Festlegungen hinsichtlich einer kontinuierlichen Überprüfung bzw. repräsentativen Stichprobe getroffen werden, um die Qualität des Scanprozesses sicherzustellen. Die gescannten Dokumente sollten indiziert werden. Es sollten nur bekannte Datenformate verwendet werden, z. B. PDF/A. Vor der Vernichtung papierbasierter Dokumente muss sichergestellt sein, dass der Scan ein rechtssicheres Dokument darstellt, insbesondere hinsichtlich der Unterschriften.
17-7	Können Daten in einer anderen Einrichtung als die des Erlaubnisinhabers archiviert werden?	Die Daten können mit Zustimmung der zuständigen Behörde bei einer externen Einrichtung innerhalb der EU archiviert werden. Es gelten die GMP-Vorgaben hinsichtlich Dienstleisterqualifizierung, Durchführung von Audits, u. a. Die archivierten Daten müssen innerhalb einer angemessenen Zeit der zuständigen Behörde zugänglich gemacht werden können (siehe Votum V11002).

3 Definitionen und Abkürzungen

Die unterstrichenen Begriffe sind dem Glossar zu Anhang 11 des EU-GMP-Leitfadens entnommen.
Weitere Definitionen und Abkürzungen siehe Glossar auf der ZLG-Seite.

- **Akzeptanzkriterien**

  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 und um den Kunden in die Lage zu versetzen, das System zu akzeptieren oder abzulehnen (siehe auch Fabrik-Akzeptanztest und Standort-Akzeptanztest)

- **ALCOA**

  engl.: attributable, legible, contemporaneous, original und accurate

  Prinzip zum Erreichen von Datenintegrität: Daten müssen zuzuordnen und lesbar sowie aktuell sein, als Originalaufzeichnung vorliegen und fehlerfrei sein.

- **Anforderung**

  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**

  Die Langzeitspeicherung von Daten in einem - in der Regel – nicht proprietären Format.

- **Audit Trail**

  Systemseitiger Kontrollmechanismus, der es ermöglicht, Veränderungen und Löschungen zu dokumentieren

- **Back-Up**

  siehe Datensicherung

- **BSI**

  Bundesamt für Sicherheit in der Informationstechnik

- **CDS**

  engl.: chromatography data systems

- **Code Review**

  Mit dem Review werden Arbeitsergebnisse der Softwareentwicklung manuell geprüft. Der 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. Es sind auch Softwaretools zum Codereview verfügbar, um diesen automatisiert durchzuführen.

- **COTS**

  engl.: commercial-off-the-shelf software

  siehe kommerziell erhältliche Standardsoftware

- **CS**

  computergestütztes System

- **CSP**

  engl.: cloud service provider

- **Datensicherung/Back-Up**

  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.

- **DEVOPs**

  DevOps ist ein Kofferwort aus den Begriffen ‚development' (englisch für Entwicklung) und ‚IT Operations' (englisch für IT-Betrieb). DevOps ist eine Sammlung unterschiedlicher technischer Methoden und eine Kultur zur Zusammenarbeit zwischen Softwareentwicklung und IT-Betrieb. DevOps soll durch gemeinsame Prozesse und Software-Werkzeuge eine effektivere und effizientere Zusammenarbeit der Bereiche Softwareentwicklung (Dev), Systemadministratoren (Ops), aber auch Qualitätssicherung und Nutzerschaft ermöglichen.

- **DMS**

  Dokumentenmanagementsystem

- **Dritter**

  nicht direkt vom Inhaber der Herstellungs- oder Einfuhrerlaubnis geführte Einrichtung

- **ELN**

  engl.: electronic lab notebook (analytisches elektronisches Laborjournal)

- **ERP**

  engl.: enterprise ressource planning

- **Fabrik-Akzeptanztest (FAT)**

  Akzeptanztest im Werk des Lieferanten, üblicherweise unter Einbeziehung des Kunden

  Gegensatz zu Standort-Akzeptanztest (engl.: factory acceptance test)

  siehe auch Akzeptanztest

- **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.

- **FMEA**

  engl.: Failure Mode and Effects Analysis

  Fehlermöglichkeits- und -Einflussanalyse

- **GAMP**

  engl.: Good Automated Manufacturing Practice

  Leitfaden zur Validierung automatisierter Systeme in der pharmazeutischen Herstellung

- **IAAS**

  engl.: infrastructure as a service

- **IDS**

  engl.: intrusion detection system

- **Integrität**

  Schutz vor unbefugter Änderung von Information

- **IPC**

  engl.: in-process control

- **ISMS**

  engl.: information security management system

- **ITIL**

  engl.: IT infrastructure library

  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

  engl.: COTS (commercial-off-the-shelf software)

- **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**

  computergestütztes System angepasst an einen spezifischen Geschäftsprozess

- **LAN**

  engl.: 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

- **LIMS**

  Labor-Informations- und Management-System

- **MES**

  engl.: manufacturing execution system (Fertigungsmanagementsystem).

- **Migration**

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

- **PAAS**

  engl.: platform as a service

- **PLS**

  Prozessleitsystem

- **PPS**

  engl.: production planning system (Fertigungsplanungssystem)

- **Prozesseigner**

  für den Geschäftsprozess verantwortliche Person

- **Quellcode**

  (1) Computerinstruktionen und Datendefinitionen, die in einer für den Assembler, Compiler oder für andere Programmcode-Übersetzer geeigneten Form dargestellt sind

  (2) menschenlesbare Version einer Instruktionsliste eines Programms, das einen Computer veranlasst, eine Aufgabe auszuführen

- **RAID**

  engl.: redundant array of independent disks

- **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.

- **Review**

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

- **RLT-Anlagen**

  raumlufttechnische Anlagen

- **RU**

  engl.: regulated user

- **SAAS**

  engl.: software as a service

- **Schnittstelle**

  definierter Übergang zwischen Datenübertragungseinrichtungen, Hardwarekomponenten oder logischen Softwareeinheiten

- **SLA**

  engl.: service-level-agreement

- **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.

- **SIP**

  engl.: sterilization in place

- **SPS**

  speicherprogrammierbare Steuerung

- **Spezifikation (IT)**

  Dokument, das die Anforderungen, den Entwurf, das Verhalten oder andere Charakteristika eines Systems oder einer Komponente vollständig, exakt und nachprüfbar beschreibt

- **SQL**

  engl.: structured query language

- **Standort-Akzeptanztest (SAT)**

  Akzeptanztest am Kunden-Standort, üblicherweise unter Einbeziehung des Lieferanten

  siehe auch Akzeptanztest; Gegensatz zu Fabrik-Akzeptanztest (engl.: site acceptance test)

- **Systemeigner**

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

- **TCP/IP**

  engl.: 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 fokussieren

  (2) Test, durchgeführt zur Beurteilung der Konformität eines Systems oder einer Komponente mit spezifischen funktionalen Anforderungen und korrespondierenden vorhergesagten Ergebnissen

  Synonym: Black-Box-Test, eingangs-/ausgangsbezogener Test

  Gegensatz dazu: struktureller Test

- **Test, strukturell**

  (1) Test, der alle internen Mechanismen (Strukturen) eines Systems oder einer Komponente mit einbezieht

  Typen: 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.

- **UAT**

  engl.: user acceptance test

- **VBA**

  engl.: visual basic for applications

- **Verifizierung**

  Bestätigung durch Bereitstellen eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

  wird teilweise an Stelle von IQ, OQ, PQ verwendet

- **WAN**

  engl.: wide area network (Weitverkehrsnetz)

  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.

4 Anlagen und Formulare

Anlage 1 – Softwarekategorien nach GAMP5®

5 Änderungsgrund

Anpassung an den Stand von Wissenschaft und Technik und derzeit geltende Regularien

6 Literaturhinweise

- Anhang 11 des EU-GMP-Leitfadens
- Schriften des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
  - IT-Grundschutz-Kompendium
  - Technische Richtlinie des BSI – BSI TR-02102 ‚Kryptographische Verfahren: Empfehlungen und Schlüssellängen‘
  - Technische Richtlinie des BSI – 03138 ‚Ersetzendes Scannen‘
  - IT-Grundsatz-Baustein INF.6: Datenträgerarchiv
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, BSI-KritisV)
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG)
- Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
- ISPE GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems (steht den Überwachungsbehörden in elektronischer Form über den Mitgliederbereich auf den PIC/S Seiten zur Verfügung)

Anlage 1 - Softwarekategorien nach GAMP® 5

- **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: Diese umfassen 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 GAMP® 5 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.